H 7625

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

35. Jahrgang 2018 Einzelpreis: 7 EUR 2/2018 – Juni 2018

5 Jahre Edward Snowden

ISSN 0938-3476

• Informatik und Gesellschaft • Netzpolitik.org • Polizeiaufgaben-Gesetz •

Mit Dossier: Cyberrüstung und zivile IT-Sicherheit

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: https://commons.wikimedia.org/wiki/Category:Edward_Snowden_in_art#/media/File:EdsnowdenHOPE.png

Inhalt

Ausgabe 2/2018

inhalt

Forum

Retrospektive

Lesen & Sehen

Rubriken

Schwerpunkt „Informatik und Gesellschaft"

Schwerpunkt „Netzpolitik.org"

FIfF e. V.

Editorial

Die Themen Datenschutz und Überwachung stehen auch bei dieser Ausgabe der *FIfF-Kommunikation* im Vordergrund. Fünf Jahre, nachdem Edward Snowden die umfassende Ausspähung durch Geheimdienste ans Licht der Öffentlichkeit gebracht hat, sind Fortschritte, aber auch Rückschritte für die digitalen Bürgerrechte zu verzeichnen. Über beides wird zu reden sein.

Seit wenigen Tagen ist für den Datenschutz in Europa die Verordnung 2016/679 anzuwenden, die *Datenschutz-Grundverordnung* (DSGVO). Mehrere Beiträge zum ersten Abschnitt dieser Ausgabe befassen sich mit Aspekten dieser Verordnung und mit dem Datenschutz allgemein.

Den Anfang macht *Stefan Strauß*: „Wachsende Identitätsschatten – wo endet die Privatsphäre", fragt er, und diskutiert kritisch die Grenzen das Datenschutzes angesichts stetig wachsender sozio-technischer Identifizierbarkeit.

Es folgen Beiträge unserer Beiratsmitglieder *Alexander Roßnagel* und *Marie-Theres Tinnefeld*. Roßnagel setzt sich mit der Frage auseinander, was die mit hohen Erwartungen und großen Hoffnungen begleitete Datenschutz-Grundverordnung für den Datenschutz bewirkt, und kommt zu einem ernüchternden Ergebnis: Sie führe „weder zu einem einheitlichen Datenschutzrecht in Europa noch zu Datenschutzregelungen, die den modernen Herausforderungen gerecht werden." Tinnefeld analysiert die Datenschutz-Grundverordnung hinsichtlich der rechtswirksamen Einwilligungserklärung Betroffener – einer der wichtigsten Rechtsgrundlagen für die Verarbeitung personenbezogener Daten – im Kontext der zunehmend europäisch geprägten Menschenrechte.

Rainer Rehak behandelt in seinem Beitrag „(Meta-) Daten im Zeichen der Sicherheit?" die Auswertung und Nutzung dieser Daten, die die Handlungen von Menschen in IT-Systemen zunehmend hinterlassen, für polizeiliche und geheimdienstliche Zwecke. Er fordert ein stärkeres Bewusstsein für Zusammenhänge und Konsequenzen dieser Auswertung. Im Anschluss daran diskutiert *Markus Reinisch* „Zahlengläubigkeit und positivistisches Grundverständnis von *Big Data*" und die gesellschaftlichen, politischen, ethischen und bildungstheoretischen Folgen. *Hans-Jörg Kreowski* schließt den Abschnitt der Ausgabe mit einer Diskussion des Informationsraums aus militärischer Sicht – dem Cyberkrieg – und weist auf die ernsthafte Bedrohung hin.

NETZPOLITIK.ORG

Der zweite Abschnitt dieser Ausgabe ist in Zusammenarbeit mit der Plattform für digitale Freiheitsrechte *netzpolitik.org* entstanden. Als Auftakt einer verstärkten Zusammenarbeit enthält er vier netzpolitische Beiträge:

- *Leo Thüer* interviewt *Max Schrems* zu Beschwerden gegen Datenkonzerne und die gerade gegründete NGO *noyb.eu – None of your Business*.
- *Alexander Fanta* setzt sich mit dem rechtlichen Graubereich auseinander, in den sich Polizeibehörden bei der Nutzung sozialer Medien wie Twitter begeben.
- *Constanze Kurz* schreibt über den geplanten EU-weiten Zwang zur Abgabe von biometrischen Daten für EU-weit vereinheitlichte Ausweisdokumente.
- Nochmals *Constanze Kurz* interviewt *Peter Schaar* zum Widerstand gegen den Wettlauf um die härtesten Polizeigesetze, deren Sicherheitsversprechen einer kritischen Prüfung nicht standhalten.

Wir freuen uns auf eine im beiderseitigen Sinn fruchtbare Zusammenarbeit mit *netzpolitik.org*.

Unsere Retrospektive widmen wir *Edward Snowden*. Seine ersten Veröffentlichungen jährten sich am 6. Juni 2018 zum fünften Mal. Aus diesem Anlass halten wir Rückschau auf die *NSA-Affäre*, drucken – ebenfalls aus *netzpolitik.org* – den damaligen Bericht über PRISM von *Andre Meister* und lassen anhand unserer damaligen Chronologie von *Sara Stadler* die Wochen nach den ersten Enthüllungen Revue passieren. Den Abschluss der Retrospektive bildet der damalige Beitrag von *Klaus Fuchs-Kittowski* zur notwendigen Solidarität mit den Whistleblowern.

Eine Reihe weiterer Ankündigungen und Stellungnahmen vervollständigen die Ausgabe. Stellvertretend seien genannt die Stellungnahme zum Bayerischen Polizeiaufgabengesetz von *Dagmar Boedicker*, unsere Ankündigung des Weizenbaum-Preises, den wir ab diesem Jahr anstatt des bisherigen FIfF-Studienpreises vergeben werden und unsere Stellungnahme zum konservativen und rechtspopulistischen „Neuen Hambacher Fest" das in seiner nationalen und rückwärtsgewandten Ausrichtung aus unserer Sicht einen Missbrauch des freiheitlichen Symbols von 1832 darstellt.

Im Dossier *Wachsendes Ungleichgewicht – Cyberrüstung und zivile IT-Sicherheit* stehen Cyber-Angriffe auf Behörden, Wirtschaft und Zivilgesellschaft im Mittelpunkt, die mittlerweile auch in Deutschland an der Tagesordnung sind. International wächst die Einsicht, dass dieser Bedrohung durch Rüstungskontrolle entgegengewirkt werden müsste, es fehlen aber Analysen der Cyber-Angreifer und ihrer materiellen und personellen Ressourcen. Die Daten zeigen, dass die Angreiferseite sehr viel stärker ausgerüstet wird als die IT-Sicherheitsverantwortlichen. Abzulesen ist eine massive Rüstungsspirale, die eine erhebliche Bedrohung der zivilen IT-Nutzung darstellt.

Für die nächste Ausgabe haben wir den Bericht von den BigBrotherAwards 2018 vorgesehen, die dieses Mal im Stadttheater Bielefeld stattfanden.

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

Stefan Hügel
für die Redaktion

Der Brief

Rechtspopulistische Agenda

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

politisches Hauptthema in diesen Tagen ist, wie wir mit Menschen umgehen, die bei uns Schutz suchen. Das zeigt sich in den allgegenwärtigen Talkshows – und den Debatten im Netz. Die radikalisierten sich erneut nach der Sendung *Die Islamdebatte: Wo endet die Toleranz?* in der Talk-Reihe *Menschen bei Maischberger*. Sie wurde nach der Verfilmung des umstrittenen Romans *Die Unterwerfung* von Michel Houellebecq gezeigt; die Debatte eskalierte in einer Weise, dass Forderungen nach einem Moratorium für Talkshows laut wurden. In *Zeit online* nahm Maischberger persönlich dazu Stellung. Aus ihrer Sicht werden leidenschaftliche Debatten heute allzu häufig als „Krawall" abgetan. Sie fordert auf, wieder mehr zu streiten.[1]

Auf den ersten Blick hat sie damit vielleicht sogar recht. Doch wer Titel und Umfeld seiner Sendung so wählt, dass ihre inhaltliche Ausrichtung bereits naheliegt, muss sich die Frage gefallen lassen, ob es wirklich um fairen politischen Streit geht. Dazu muss man nicht einmal Fremdenfeindlichkeit unterstellen. Die Produktion von Talk-Shows ist schließlich auch ein Geschäft und Flüchtlinge dafür derzeit offenbar ein lukratives Thema.

„Die so vehement geführten Dabatten", so Maischberger, „spiegeln sich natürlich auch in politischen Talkshows wider." Selbstverständlich. Doch die Sendungen setzen auch die politische Agenda.[2] Sich auf gesellschaftliche Debatten zu berufen, auf die man nur reagiere, verkennt diese Funktion von Medien und ist schlimmstenfalls verantwortungslos.

„Verantwortungslos" – das ist auch der erste Begriff, der mir angesichts der aktuellen Debatte innerhalb der Bundesregierung einfällt. Eine Sitzung des Bundestags musste mehrere Stunden unterbrochen werden, nachdem zwischen CSU und CDU ein heftiger Streit über die Zurückweisung von Flüchtlingen an der deutschen Grenze entbrannt ist.[3] [4] Auch hier ist der Streit um die Deutungshoheit voll im Gange – doch Begriffe wie „Asyltourismus" sind nicht mehr nur verantwortungslos, sie sind unmenschlich und unerträglich.

Insgesamt verfestigt sich der Eindruck, dass die AfD zunehmend die Debatte bestimmt. Inzwischen diskutieren wir über das Singen der Nationalhymne vor Fußballspielen.[5] Diskussionen, Shitstorms und Pfiffe löst das – zugegebenermaßen politisch unglückliche – Zusammentreffen der Spieler Mesut Özil und İlkay Gündoğan mit dem Türkischen Präsidenten Erdoğan aus. Heutzutage ist schon ein klares nationales Bekenntnis notwendig, wenn man für Deutschland Fußball spielen will – vor allem dann, wenn man keine „biodeutsche" Herkunft vorweisen kann. Das frühe Ausscheiden bei der diesjährigen Weltmeisterschaft mag man bedauern, auf das schwarz-rot-goldene Fahnenmeer kann ich persönlich gut verzichten.[6]

Wohltuend ist hier das Engagement des Präsidenten des Fußballvereins Eintracht Frankfurt, Peter Fischer, der für seine klare Haltung von der Stadt Marburg und der Humanistischen Union Marburg mit dem *Marburger Leuchtfeuer* geehrt wurde.[7]

Die AfD nutzte unter dem Beifall ihrer Claqueure auch den erschütternden Fall in Wiesbaden, wo ein 14-jähriges Mädchen getötet wurde. Mutmaßlicher Täter ist ein Mann, der in Deutschland um Asyl nachgesucht hatte –, die AfD instrumentalisierte die Tat zur Hetze gegen Flüchtlinge und Asylsuchende durch eine *Schweigeminute* im deutschen Bundestag. Als Claudia Roth als verantwortliche Sitzungsleiterin dies unterband, sah sie sich heftigen Anfeindungen ausgesetzt. Bundestagspräsident Wolfgang Schäuble – sonst nicht gerade ein Freund des FIfF – ist für seine besonnenen und bestimmten Worte dazu zu danken.

Eigentlich wollte ich über ganz andere Dinge schreiben: Die EU-Datenschutz-Grundverordnung ist seit 25. Mai 2018 verbindlich anzuwenden. Am 6. Juni 2018 ist es nun fünf Jahre her, dass Edward Snowden uns durch seine Enthüllungen die weltweite Überwachung der Telekommunikation bewusst gemacht hat. Und unseren Studienpreis werden wir künftig als Weizenbaum-Studienpreis verleihen, um damit einen Mann zu ehren, der sich in besonderer Weise um *Informatik und Gesellschaft* verdient gemacht hat. Verstörend, dass auch ich mir von der AfD die Agenda diktieren lasse – aber das ist diesmal wohl unvermeidbar. Zu den anderen Themen verweise ich auf die zahlreichen Beiträge in dieser Ausgabe.

Mit FIfFigen Grüßen
Stefan Hügel

Anmerkungen

1 *Sandra Maischberger (2018): Abschalten? Zeit online, https://www.zeit.de/2018/25/sandra-maischberger-talkshow-themen-fluechtlinge-populismus-demokratie/komplettansicht*

2 *Pointiert zum Agenda-Setting dieser Sendungen Walter van Rossum (2004): Meine Sonntage mit „Sabine Christiansen". Köln: Verlag Kiepenheuer & Witsch. In dem Band wird der damalige konservative Politiker Friedrich Merz mit den Worten zitiert: „… Diese Sendung bestimmt die politische Agenda in Deutschland mittlerweile mehr als der deutsche Bundestag. …" (S. 15)*

3 *Es geht vor allem um den „Masterplan Migration" von Heimatminister Seehofer und um die ca. 46.000 Flüchtlinge, die bereits in einem anderen Staat Asyl beantragt haben. Vgl. dazu auch https://blog.ard-hauptstadtstudio.de/zurueckweisung-von-fluechtlingen-um-wie-viele-leute-gehts/*

4 *Nachdem früher vor dem* rot-grünen *Chaos gewarnt wurde, jetzt also das* schwarz-schwarze *Chaos. Man fragt sich aber gelegentlich, ob ein solcher inszenierter Streit zwischen Schwesterparteien wirklich* echt *ist, oder ob lediglich ein Volkstheater zur Profilierung für die anstehenden Landtagswahlen aufgeführt wird. Bei der Ausweitung der staatlichen Parteienfinanzierung war man sich dann zumindest sehr schnell wieder einig.*

5 *Schaut man sich Fußballspiele der deutschen Männer-Nationalmannschaft aus den 1970er Jahren an, so stellt man fest: Da hat niemand gesungen. Skandal! Vielleicht sollten wir die Weltmeisterschaft 1974*

zurückgeben, wurde sie doch von einer Mannschaft erspielt, die das notwendige Bekenntnis zur deutschen Nation offenkundig vermissen ließ. Zur aktuellen Debatte siehe auch http://www.spiegel.de/sport/fussball/fussball-wm-2018-interview-ulrich-schmidt-denter-zu-nationalhymnen-a-1213054.html

6 *Das ist nicht so harmlos, wie manche glauben machen wollen: Nach Ansicht des Antisemitismusforschers Clemens Heni hat der Patriotismus des „Sommermärchens" von 2006 rechtspopulistischen Tendenzen den Boden bereitet: http://www.fr.de/kultur/antisemitismus-sommermaerchen-bereitete-der-afd-den-boden-a-1409276. Auch andere zweifeln mittlerweile am Bild des harmlosen Party-Patriotismus: http://www.sueddeutsche.de/politik/patriotismus-nationalismus-deutschland-1.4003006*

7 *http://hu-marburg.de/2018/06/13/preisbegruendung-der-jury-peter-fischer-beweist-mut-und-haltung-gegen-rassismus/*

Dagmar Boedicker

Unbestimmt! – Unverhältnismäßig! – Verfassungswidrig?

Zum Bayerischen Polizeiaufgaben-Gesetz

Innenminister Seehofer will das neue Bayerische Polizeiaufgaben-Gesetz (PAG[1]) zur Vorlage für solche Gesetze bundesweit machen – als Mustergesetz. *Das PAG passt gut ins Denken von Entscheidern, die seit 2001 ein Netz um* Gefährder *und Kriminelle ziehen wollen, um ihren Wählerinnen und Wählern eine Sicherheit vorzugaukeln, die es so nicht gibt. Es ist eine erneuerte Sicherheits-Architektur auf Länder-, Staats- und europäischer Ebene entstanden. Ein Netz, in dem die Demokratie als Beifang zappelt!*

Hilflose Demokratie

Freie Menschen brauchen Privatsphäre als einen Ort, in dem sie diskutieren, eigene Meinungen erproben und bilden können. Privat ist der Ort, zu dem nur diejenigen Zugang haben, denen wir das ausdrücklich erlauben. Zwar sind das viel zu oft große Konzerne wie Facebook, Google, Amazon und andere –, dem Staat erlauben wir diese Überwachung aber nur, wenn es gar nicht anders geht. Wenn also unsere Repräsentanten dem mit Gesetzen zugestimmt haben. Auch dann ist nicht auszuschließen, dass eine Gesellschaft als Ganzes aufhört, furchtlos Meinungen zu äußern und auszutauschen und ihre demokratischen Grundrechte in Anspruch zu nehmen. Wer sich beobachtet fühlt, ändert das eigene Verhalten, passt sich an, verzichtet auf Freiheiten und nimmt weniger oder gar nicht mehr an der aktiven Gestaltung des Gemeinwesens teil.

Damit muss Bayern jetzt schon und demnächst wohl die Bundesrepublik rechnen, wenn „Voraussetzungen für polizeiliche Befugnisse nicht genannt, sondern in Verweisungsirrgärten versteckt"[2] werden, wenn Regelungen und Begriffe unbestimmt sind und „den Rechtsanwendenden [werden] nicht genügend Hinweise für eine begrenzende Auslegung gegeben"[3] werden. Oder wenn Eingriffe mehrfach damit begründet werden, dass eine Person oder Sache „mutmaßlich in Zusammenhang mit der Gefahrenlage"[4] steht.

> *„Tatsächlich enthält die Rechtsprechung des BVerfG, anders als die Begründung an mehreren Stellen suggeriert (S. 54, 59, 62, 66), keine Rechtfertigung von Eingriffen ausschließlich auf der Grundlage von Mutmaßungen."*[5]

Wenn ein Gesetz die Rechte des Souveräns beschneidet, muss es *mindestens (!)* möglich sein, dass einerseits der Souverän (wir Bürgerinnen und Bürger also) weiß, was dieses Gesetz von ihr/ihm verlangt. Wir müssen verstehen, wie wir uns gesetzeskonform verhalten sollen. Dazu müssen wir das Gesetz begreifen, es muss transparent und eindeutig sein. Wir dürfen erwarten, dass es fair ist und unsere demokratische Freiheit nicht über Gebühr beschränkt, *erforderlich* und *verhältnismäßig,* nicht mehr als unbedingt notwendig. Das gilt auch für diejenigen, die gar nicht Bürger dieses Staats sind, sondern sich lediglich in ihm aufhalten. Auf der anderen Seite müssen auch die, die dieses Gesetz anwenden sollen, wissen, welche Rechte wir haben und welche Rechte sie uns gegenüber. Auch Gerichte, Geheimdienste oder die Polizei müssen das verstehen. Es mag sein, dass der Polizei nicht jedes Verhalten genehm ist. Das bedeutet aber nicht zwangsläufig, dass sie unerwünschtes Verhalten unterbinden darf. Sollte sie ihre Kompetenzen überschreiten, müssen wir uns wehren können. Dafür brauchen wir Rechtsmittel. Missbrauch muss möglichst verhindert und – sollte er doch geschehen sein – müssen wir entschädigt werden.

So nicht!

Bayern hat ein Problem. Es ist für eine Demokratie nicht gesund, wenn eine Regierungspartei (noch) mit absoluter Mehrheit herrscht. Natürlich möchte die CSU, dass das so bleibt. Und solange es so ist, kann sie es sich leisten, ein PAG auch dann durch den Landtag zu drücken, wenn Experten in ihren Stellungnahmen Teile als verfassungswidrig betrachten. Das hat sie erfolgreich schon im Juli 2017 gezeigt, als sie das Polizeiaufgaben-Gesetz[6] zuletzt änderte. Der Bayerische Innenminister entzieht sich inhaltlicher Kritik und wirft im Gegenangriff den Oppositionsparteien und den zahlreich protestierenden Bürgern vor, zu lügen. Die Debatte im Landtag anlässlich der hastigen zweiten und dritten Lesung am 15. Mai 2018 war ein unschönes Schauspiel und ließ die Arroganz der Macht spüren. Jetzt ist das PAG in Kraft.

Das hat die CSU-Mehrheit unter anderem beschlossen:

- Kontaktverbote, Aufenthaltsverbote, Aufenthaltsgebote (Art. 16 Abs. 2 S. 1) und Präventivgewahrsam (Art. 17):
  Dafür sind die Voraussetzungen stark abgesenkt. Präventivgewahrsam kann jetzt von bisher 14 Tagen auf drei Monate ausgeweitet und unbegrenzt häufig verlängert werden („Unendlichkeitshaft"). Beim Verstoß gegen eine elektronische Aufenthaltsüberwachung oder ein Aufenthaltsgebot genügt dafür die „drohende Gefahr". Wenn Menschen aber durch Anordnungen, wo sie sich aufzuhalten haben, oder gar durch „präventive Ingewahrsamnahme" über viele Mo-

nate ihre Arbeit und Wohnung verlieren, dann müssen sie sich etwas zu Schulden kommen lassen haben. Wenn nicht, dann muss der Staat dieses Unrecht gut machen!

- Telekommunikationsüberwachung (Art. 42), Online-Durchsuchung („Staatstrojaner", Art. 45), Datenlöschung und Datenmanipulation im Rahmen der Online-Durchsuchung (Art. 45 Abs. 1 S. 6), Durchsuchung von Datenspeichern und in der Cloud gespeicherten Daten (Art. 22 Abs. 2).

- Den Einsatz von Drohnen als Mittel unmittelbaren Zwangs (Art. 78 Abs. 3) zog die CSU mit ihrem Änderungsantrag vom 25. April zurück, in Reaktion auf „Bedenken in der Bevölkerung" [7]. Der Änderungsantrag formuliert „Diese unbemannten Luftfahrtsysteme dürfen nicht bewaffnet werden."[8]

- Zu Überwachungszwecken (Art. 47) sind unbemannte Luftfahrtsysteme sehr wohl vorgesehen, das heißt dann „zur Datenerhebung":
  Eine Drohne überwacht natürlich nicht nur einzelne Personen. Es ist ein flächendeckender Eingriff aus der Luft, meist so weit entfernt, dass Menschen es nicht einmal bemerken. Falls doch, wie sollen wir erkennen, ob es ein Fluggerät der Polizei ist, ob da ein Hobby-Pilot übt, der sich nicht um die Rechtslage schert, oder womöglich Schlimmeres? Der Bayerische Datenschutzbeauftragte fordert, dass der Drohneneinsatz als polizeiliche Maßnahme wahrnehmbar sein muss und die Drohne nicht durchs Fenster in unsere Wohnungen gucken darf.[9]

Das stellt das PAG nicht sicher. Wenn Unschuldige durch heimliches Eingreifen in ihre Privatsphäre, Spitzel aus dem Freundes- oder Bekanntenkreis, das Abschöpfen ihrer Kommunikation und lückenlose Rundumüberwachung gläsern werden und sich nackt und schutzlos fühlen, dann nimmt der Gesetzgeber ihnen ihre Würde. Das darf ein Rechtsstaat nicht!

- Postbeschlagnahme (Art. 35) und Einsatz von verdeckten Ermittlern und Vertrauenspersonen (Art. 37 und 38):
  Drei Werktage kann die Polizei uns ohne richterliche Anordnung beobachten. Falls sie die Maßnahme dann beendet, kann sie sie jederzeit wieder beginnen. Die Polizei darf auch Post beschlagnahmen und öffnen, sogar bei unseren Nachbarn, wenn die so freundlich sind, sie für uns anzunehmen. Dafür genügt die Vermutung, dass die Nachbarin etwas mit der Gefahrenlage zu tun haben könnte, wenn also: „bestimmte Tatsachen die begründete Annahme rechtfertigen, dass sie für eine Person [...] Postsendungen entgegennimmt oder weitergibt und sie daher mutmaßlich in Zusammenhang mit der Gefahrenlage steht…".

Der Datenschutzbeauftragte fordert, dass „tatsächliche Anhaltspunkte" diese Annahme stützen müssen.[10] Wieso steht das nicht so im Gesetz? Das gilt auch für die Telekommunikations-Überwachung (TKÜ) von Kontaktpersonen, von denen wir alle – nicht nur die zwei Milliarden Facebook-NutzerInnen – eine große Menge haben. Auch hier genügt für die Polizei die bloße Vermutung, dass sie „in Zusammenhang mit der Gefahrenlage stehen".

- Erweiterung der DNA-Analyse (Art. 14 und 32):
  Das Bayerische Innenministerium behauptet, dieses Gesetz stärke den Datenschutz, obwohl bei ganz besonders schutzwürdigen wie biometrischen oder DNA-Daten entscheidende Fehler gemacht wurden. Aus solchen Daten lässt sich viel mehr erkennen als nur die Identität eines Menschen, sie bleiben ihr/ihm bis zum Tod und lassen sich nicht anonymisieren. Sie erlauben Aussagen über die seelische oder gesundheitliche Disposition, gleichzeitig sind diese Aussagen nur vage Prognosen, nicht objektiv eindeutig. Wir hinterlassen DNA überall und Verwandte lassen sich daraus ermitteln.[11]

In den USA suchten Ermittler in der Datenbank eines kommerziellen Dienstleisters und fanden dort die DNA von Verwandten eines Täters, dessen DNA sie am Tatort entdeckt hatten, und schließlich den mutmaßlichen Täter. Die Methode war entwickelt worden, um die Leichen unbekannter Verbrechensopfer identifizieren und ihren Angehörigen die sterblichen Reste übergeben zu können. Sie ist noch aufwendig und teuer und hat bisher zu falschen Beschuldigungen geführt.[12] Es braucht nicht viel Fantasie, um sich auszumalen, welchen Schreck der Anruf einer Sicherheitsbehörde bei ahnungslosen Verwandten auslösen kann.

Seitdem die Bayerische Regierung den von ihr kaum so erwarteten Protest erlebt (schließlich hatte im letzten Sommer kein Hahn nach dem PAG gekräht), wirft sie dem Bündnis noPAG angebliche Nähe zu Verfassungsfeinden vor, unterstellt ihm Falschinformation und zitiert recht fantasielos immer wieder dieselben eigenen Argumente, beispielsweise in ihren *Fragen und Antworten (FAQ)*.[13] So seien die neuen Befugnisse unbedingt erforderlich, bedürften aber auch immer einer richterlichen Anordnung. Das stimmt nicht, es gibt Ausnahmen, wie Art. 33 Abs. 4 (Bild- und Tonaufnahmen in Wohnungen), Art. 36 Abs. 2 (Besondere Mittel der Datenerhebung). Außerdem müssten die verdeckt Beobachteten anschließend informiert werden. Auch das ist nicht richtig: Ganz davon abgesehen, dass Betroffene verdeckter Überwachung höchst selten erfahren, wenn sie betroffen waren, moniert der Bayerische Landesbeauftragte für den Datenschutz, Thomas Petri, einen neuen Ausnahmetatbestand (Art. 31 Abs. 4 Satz 4), wonach die Benachrichtigung unterbleiben kann.

Außerdem stehe „Sicherheitsverwahrten" ein Verteidiger zu. Das stimmt nicht. Sie haben Anspruch auf einen *Beistand*, das ist nicht etwa ein (Pflicht-)Verteidiger.

Es wäre auch anders gegangen

Es bleibt der hässliche Eindruck, dass Sicherheitspolitiker wann immer möglich maximale Überwachung und Repression in ihren Gesetzen fordern, wohl wissend, dass Klagen gegen diese Angriffe auf den Rechtsstaat nicht alle Fehler im gesamten Machwerk korrigieren werden. Der eine oder andere Artikel ist nicht verfassungsgemäß? – Kein Problem, wird geändert, es sind noch genügend Übergriffe in unsere Privatsphäre und Verstöße gegen die Unschuldsvermutung möglich.

Wieso beschäftigt der legislative Apparat Gutachter, wenn viele Befunde dann nicht ins Gesetz finden? Allein das Gutachten des Bayerischen Landesbeauftragten für den Datenschutz ist mehr als 80 Seiten lang, er kommt zu höchst bedenklichen Schlüssen. Wo wurden sie im Gesetzentwurf berücksichtigt? Nicht nur das Grundgesetz, auch die europäische Grundrechte-Charta und die Menschenrechts-Konvention verlangen, dass Einschränkungen

unserer Privatsphäre und Handlungsfreiheit Bedingungen erfüllen. In einem Rechtsstaat müssen sie *geeignet, erforderlich* und *verhältnismäßig* für den Schutz *bestimmter* Rechtsgüter sein. Der Schlüsselbegriff der „drohenden Gefahr" ist alles andere als das und ermöglicht viele der oben genannten Eingriffe. Hier soll die Polizistin oder der Polizist im Einsatz nämlich interpretieren, was all diese unbestimmten Begriffe in der jeweiligen Situation bedeuten:

> *„bedeutendes Rechtsgut – erhebliche Eigentumspositionen – konkrete Wahrscheinlichkeit – seiner Art nach konkretisiertes Geschehen – Vorbereitungshandlungen – in absehbarer Zeit – Angriffe von erheblicher Intensität oder Auswirkung"*.

Schon viel länger als seit 2001 kämpfen wir für unsere informationelle Selbstbestimmung. Immer wieder erleben wir, dass Politik (und Wirtschaft) der Versuchung nicht widerstehen können zu tun, was technisch möglich ist. Seit mindestens 10 Jahren könnte die Polizei mit *Quick Freeze*[14] bei schweren Straftaten ermitteln. Die deutsche Politik aber, gegen europäische Rechtsprechung, beharrt auf einer weit umfassenderen Vorratsdatenspeicherung. Profis in Prävention und Strafverfolgung beklagen ausufernde Datenströme, in denen sich kaum etwas finden lässt. Und nun setzt die Politik wieder auf die technische Karte, jetzt soll es wahrscheinlich die *Künstliche Intelligenz* richten. Technische Lösungen funktionieren nicht für soziale oder politische Probleme.

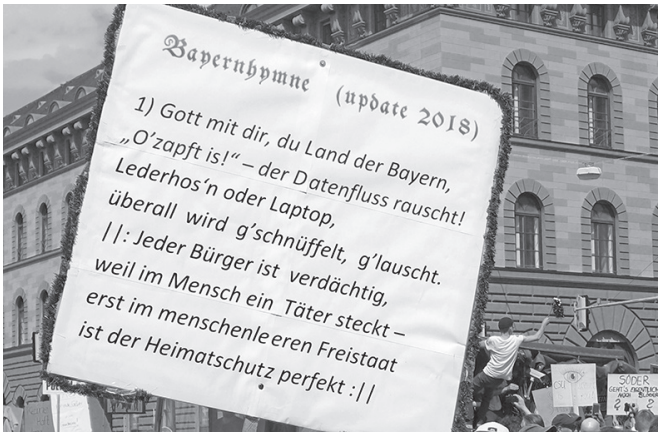
Unerwarteter Protest

Als wir in Bayern endlich aufgewacht sind – erst Monate nach der Einführung der drohenden Gefahr, war es schon zu spät, die zweite Reform des PAG zu verhindern. Dann sind wir aber rasch aktiv geworden. Ein Bündnis noPAG hat sich gegründet und innerhalb von nicht einmal zwei Monaten gab es am 10. Mai 2018 eine der größten und schönsten Demonstrationen für unseren Rechtsstaat und die Demokratie, die ich je erlebt habe. 30.000 Menschen sind nach Polizei-Angaben unterwegs gewesen, wahrscheinlich waren es sehr viel mehr. Die Fotos zu diesem Beitrag (siehe auch Seite 45 f.) zeigen die Assoziationen, die diese Menschen zum PAG haben. Positiv sind diese Assoziationen nicht!

Und wer ist schuld?

Anlässe für die Gesetzgebung waren – so die Begründung – europäische Vorgaben in der Richtlinie (EU) 2016/680 zum Datenschutz bei Polizei und Justiz vom 27. April 2016 sowie die Umsetzung befugniseinschränkender Rechtsprechung des Bundesverfassungsgerichts.

Ganz abgesehen davon, dass die Richtlinie (EU) 2016/680 bestimmte Regelungen im PAG sogar explizit ausschließt und das BVerfG bei seinem Urteil zum BKA-Gesetz ganz andere Intentionen hatte, möchte ich den Spieß umdrehen: Wer hat denn in den letzten Jahrzehnten Polizeistellen gestrichen? Wer hat der Polizei immer mehr Aufgaben zugeschoben, ohne ihr dafür die Ressourcen zu bewilligen? Wer ist für die Überstunden-Berge verantwortlich? Wer hat so getan, als sei die europäische Gesetzgebung eine unzulässige Einmischung in nationale Angelegenheiten? Wer hat den Staat für unfähig erklärt, die Daseinsvorsorge zu gewährleisten? Wer hat privaten *Sicherheits*-Dienstleistern das Feld überlassen?



Gott mit dir, du Land der Bayern

Hätte die Polizei noch Zeit für den Kontakt mit den Menschen auf den Straßen, dann könnte sie sich auf die wirklichen Bedrohungen konzentrieren und müsste nicht mit technischen Mitteln eine gewaltige Rasterfahndung bewältigen, durch deren Netze genau die schlüpfen, die wirklich gefährlich werden können. Statt dessen werden Polizisten jetzt Schulungen besuchen müssen, um eine missbräuchliche Anwendung des PAG zu verhindern. Und die CSU-Regierung hat weitere Pläne für sie: Sie sollen in die Schulen gehen und dort über das PAG informieren. Wieder müssen die Beamtinnen und Beamten ausbügeln, was Politik mit symbolischer Gesetzgebung anrichtet. Ein weiterer Schritt im Verlust des Vertrauens zwischen Exekutive und Bevölkerung.

Wie weiter?

Erweiterte Polizei-Befugnisse sind kein bayerisches Alleinstellungsmerkmal: Baden-Württemberg hat sie 2017 in seinem Polizei-Gesetz (PolG) ähnlich ausgedehnt, Bremen, NRW und Niedersachsen planen es, Sachsen und Mecklenburg-Vorpommern ebenfalls. Andere Länder schrauben an anderen Teilen ihrer *Sicherheits-Architektur,* wie Hessen am Gesetz zur Neuausrichtung des Verfassungsschutzes[15]. Dagegen regt sich Widerstand auf Länder- und Bundesebene, Beschwerden beim Bundes-Verfassungsgericht (BVerfG) sind geplant, die sich gegen die „drohende Gefahr" als Ermächtigungsgrundlage für eine heimliche Überwachung richten. Die Kräfte dafür sollten versammelt und koordiniert werden.

Dabei darf es aber nicht bleiben. Die europäische Rechtskultur ist nicht nur in Deutschland bedroht oder beschädigt. In Spanien

Dagmar Boedicker

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

versucht ein „Maulkorb-Gesetz“ seit 2015 die Empörten einzuschüchtern, in Frankreich ist der Ausnahmezustand zum ganz normalen Gesetz geworden, in Ungarn und Polen erfordert es großen Mut für Positionen einzustehen, die den Machthabern nicht passen. Von Demokratie-feindlichen Bewegungen und Parteien ist nichts Gutes zu erwarten. Auch in der EU sollten die Kräfte gebündelt werden, damit politischer Widerstand vom Recht bestätigt und nicht mit juristischen und polizeilichen Mitteln unterdrückt wird. Demokratie muss atmen! Sie braucht Beteiligung, Äußerung und Diskurs der Vielen, ob das den Herrschenden passt oder nicht. Wenn Staatsmacht die gewaltfreien Wege durch exzessive Überwachung unbescholtener Bürger unpassierbar macht, wird es böse enden. Falls nationale oder föderale Regierungen und Parlamente das nicht verstehen, muss es ihnen der EuGH oder der europäische Gerichtshof für Menschenrechte erklären.

Für die Fotos von der Demonstration (siehe auch Seite 45 f.) am 10. Mai bedanken wir uns bei Günther Gerstenberg, der diese unter CC BY-Lizenz zur Verfügung stellt.

Anmerkungen

1 *Gesetz zur Neuordnung des bayerischen Polizeirechts (PAG-Neuordnungsgesetz)*
2 *Stellungnahme RiBVerwG a.D. Prof. Dr. Kurt Graulich, S. 6*
3 *Stellungnahme des Netzwerks Datenschutzexpertise zum PAG, S. 6*
4 *PAG-Neuordnungsgesetz*
5 *Stellungnahme der Deutschen Vereinigung für Datenschutz e. V. (DVD) vom 6.4.2018, S. 4*
6 *Polizeiaufgabengesetz (PAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBl. S. 397, BayRS 2012-1-1-I), das zuletzt durch § 1 des Gesetzes vom 24. Juli 2017 (GVBl. S. 388) geändert worden ist (Gefährderüberwachungsgesetz)*
7 *Änderungsantrag vom 25.04.2018, Bayerischer Landtag Drucksache 17/21890*
8 *ebd.*
9 *Stellungnahme zum PAG-Neuordnungsgesetz des Bayerischen Landesbeauftragten für den Datenschutz, S. 48*
10 *Stellungnahme zum PAG-Neuordnungsgesetz des Bayerischen Landesbeauftragten für den Datenschutz, S. 31*
11 *Stellungnahme des Netzwerks Datenschutzexpertise zum PAG, S. 4*
12 *Tina Hesman Saey: New genetic sleuthing tools helped track down the Golden State Killer suspect. Science News. Washington, D.C.*
13 *Eine Gegendarstellung findet sich bis zum Erscheinen dieser FIfF-Kommunikation auf der Website des Bündnisses noPAG https://www.nopagby.de/*
14 *AK Vorrat zu „Quick Freeze Plus“: http://www.vorratsdatenspeicherung.de/images/ak-vorrat-stellungnahme_qf-e.pdf*
15 *Sachverständigenauskunft zum Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen – Drucksache 19/5412 https://www.fiff.de/presse/pressemitteilungen/fiff-stellungnahme-zum-trojanereinsatz-durch-den-hessischen-verfassungsschutz-fiff-lehnt-hessentrojaner-ab*

Dagmar Boedicker

Aus der Regionalgruppe München

Polizeiaufgaben-Gesetze in Bayern und anderswo

Bundesinnenminister Seehofer möchte das schärfste Polizeiaufgaben-Gesetz (PAG) Deutschlands zur Richtschnur für alle Bundesländer machen. So setzt sich der Sicherheitswahn nach dem September 2001 fort, Schily und Schäuble revisited. *Zumindest in Bayern, aber hoffentlich nicht nur dort, scheint das kleine kriegerische Bergvolk in all seiner Vielfalt etwas dagegen zu haben. Kurze Chronik des Widerstands:*

Nach zwei Vorbereitungstreffen fand sich am 11. April 2018 das *noPAG-Bündnis* gegen das Polizeiaufgaben-Gesetz zusammen, in dem inzwischen (Ende Mai) 96 Organisationen arbeiten und das eine Demonstration gestemmt hat, die so jung, bunt und beeindruckend ihresgleichen sucht. Nur wenig mehr als einen Monat hatte das Bündnis, um sie vorzubereiten. Es muss wohl das Maß voll sein, wenn alle Mitglieder, Nichtregierungs-Organisationen, Parteien und Vereine, Verbände und Gewerkschaften so konstruktiv zusammenarbeiten, ihre sicher oft unterschiedlichen Interessen zurückstellen und laut und deutlich *Nein!* sagen.

Am 10. Mai sind nach Polizeiangaben 30.000 Menschen in München auf die Straße gegangen. Wahrscheinlich waren es 40.000 oder sogar mehr, denn der Zug nahm einfach kein Ende. Die letzten TeilnehmerInnen verließen den Startpunkt Marienplatz erst, nachdem die Abschlusskundgebung auf den Odeonsplatz schon eineinhalb Stunden lief. Die Stimmung war dem Souverän angemessen:

> *Wir sind hier, wir sind laut, weil man uns die Freiheit klaut!*

Wer hätte gedacht, dass ganz normale BürgerInnen wie Fußballfans und Umweltschützer, Schüler und Lehrer, Antifa und Anwälte, Datenschützer und kirchliche Organisationen, Künstler und Flüchtlingshelfer, kurz: alle Betroffenen von diesem Angriff auf den Rechtsstaat und die Demokratie, mit Fantasie, Zeit und Energie eine solche Demonstration vorbereiten und verwirklichen? Die CSU wohl kaum, denn der Bayerische Innenminister Hermann hat bis zur bedauerlichen Verabschiedung des PAG im Landtag auf Spaltung des Bündnisses gesetzt. Er warf den Oppositionsparteien vor, sich nicht von Mitgliedern zu distanzieren, die „Lügen“ verbreiteten.

München war zwar der zentrale, keineswegs aber der einzige Fokus des Widerstands, auch andere bayerische Städte haben mit großen Kundgebungen protestiert. Bis diese *FIfF-Kommunikation* erscheint, werden sich auch aus anderen Bundesländern weitere Formen des Protests manifestiert haben: Verfassungsbeschwerden, offene Briefe, fantasievolle künstlerische Aktionen im realen und im Cyberspace, ...

FIfF e. V. war übrigens von Anfang an dabei.

Bündnis Brementrojaner – Pressemitteilung

Das Bremische Polizeigesetz soll verschärft werden: Das Bündnis Brementrojaner stellt sich dem entgegen. Kein weiterer Abbau von Grundrechten!

4. April 2018 – In Bremen treibt die rot-grüne Landesregierung im Eiltempo und ohne gesellschaftliche Debatte eine folgenschwere Änderung des Bremischen Polizeigesetzes voran. Der Senator für Inneres hat einen entsprechenden Gesetzentwurf am 15. Dezember 2017 vorgelegt. Er sieht gravierende rechtsstaatliche, grund- und datenschutzrechtliche Eingriffe vor.

Seit der ersten öffentlichen Debatte in der Innendeputation am 10. Januar 2018 steht der Entwurf des Innensenators in der öffentlichen Kritik. Inzwischen haben die rot-grünen Koalitionspartner den Entwurf intern überarbeitet; über das Ergebnis wird wahrscheinlich am 12. April 2018 in der Innendeputation abgestimmt. Auch nach möglichen Änderungen durch die rot-grüne Koalition wird unsere grundsätzliche Kritik an der Verschärfung des Bremischen Polizeigesetzes bestehen bleiben.

Denn die Konsequenzen sind:

- weitreichender Ausbau staatlicher Videoüberwachung im öffentlichen Raum,
- Einführung von „elektronischen Fußfesseln" zur lückenlosen Aufenthaltskontrolle mutmaßlicher „Gefährder" – also von Menschen, die nicht etwa Straftaten begangen haben, sondern denen solche aufgrund bestimmter Anhaltspunkte lediglich zugetraut werden,
- massive Ausweitung der polizeilichen Überwachung elektronischer Kommunikation mittels Computern und Smartphones, insbesondere durch heimlich eingeschleuste Schadsoftware („Staatstrojaner").

Das *Bündnis Brementrojaner* ist ein Zusammenschluss verschiedener zivilgesellschaftlicher und politischer Gruppen und Personen. Wir lehnen die geplante massive Überwachung und die damit einhergehenden gravierenden Grundrechtseingriffe entschieden ab. Die vorgeblich notwendigen Sicherheitsverschärfungen sind unverhältnismäßig und widersprechen rechtsstaatlichen Prinzipien.

Susanne Wendland, Mitglied der Bremischen Bürgerschaft (parteilos) und Sprecherin für das Bündnis: *„Es geht um unsere freiheitlich demokratische Grundordnung. Um unsere Freiheits- und Grundrechte, die angegriffen werden. Schlimmer noch: Sie werden ignoriert. Um uns vorzugaukeln, wir hätten die terroristische Gefahr im Griff. Sicherheitsfolklore nenne ich das, die zu nichts taugt. Deswegen lehnen wir als Bündnis die geplante Gesetzesverschärfung vollständig ab."*

Die geplante Erweiterung von Videoüberwachung ist nicht hinzunehmen. *„Bereits jetzt ist Videoüberwachung in Bremen weit verbreitet, obwohl ein entsprechender Nutzen nicht nachgewiesen ist"*, sagt Bündnissprecherin **Maike Schmidt-Grabia von Digitalcourage e. V. Bremen** *„Noch mehr Kameras werden unsere Freiheit weiter einschränken. Denn wer beobachtet wird, ist nicht frei."*

Mit dem Argument der Terrorismusabwehr sollen der Polizei weitreichende Grundrechtseingriffe auch in unser aller Privat- und Intimsphäre ermöglicht werden.

Rolf Gössner, Internationale Liga für Menschenrechte und Bündnissprecher: *„Der Bremer Gesetzentwurf reiht sich mit besonders eingriffsintensiven Polizeibefugnissen in eine bundesweite Entwicklung ein, mit der mühsam errungene Grund- und Freiheitsrechte abermals massiv eingeschränkt werden, um vermeintlich mehr Sicherheit zu erreichen. Insgesamt ein weiterer, verfassungsrechtlich hoch problematischer Schritt in Richtung präventiver Sicherheitsstaat."*

Eingeschränkt werden die Freiheitsrechte u. a. durch das heimliche Einschleusen von „Staatstrojanern" in Computer und Smartphones. Der Staatstrojaner zerstört das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen. Dazu sagt Bündnissprecher **Aaron Lye vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)**: *„Eingriffe in Rechnersysteme als Ermittlungsinstrument stellen strukturelle Gefahren für IT-Systeme und damit letztendlich für uns alle dar. Denn sie öffnen Missbrauch und gefährlichen Attacken Tür und Tor."*

Das *Bündnis Brementrojaner* verurteilt zudem die Art und Weise, wie der Gesetzentwurf möglichst lautlos durch das Gesetzgebungsverfahren gedrückt werden soll. Eine öffentliche parlamentarische Anhörung von Sachverständigen – wie etwa in Hessen – fand bisher nicht statt. **Susanne Wendland (MdBB)**: *„Es ist vollkommen unverständlich, dass eine rot-grüne Regierungskoalition solche tiefgreifenden Eingriffe in Grund- und Freiheitsrechte plant, ohne zuvor eine breite öffentliche Debatte in der Gesellschaft geführt zu haben."*

Das Bündnis Brementrojaner fordert die regierenden Parteien dazu auf, den laufenden Gesetzgebungsprozess für das Bremische Polizeigesetz abzubrechen.

Wer Freiheit für Sicherheit aufgibt, wird beides verlieren!

BündnispartnerInnen (in alphabetischer Reihenfolge):

- Chaos Computer Club Bremen e. V. (CCCHB)
- Digitalcourage e. V. – Ortsgruppe Bremen
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
- GRÜNE JUGEND Bremen
- Humanistische Union – Landesverband Bremen (HU)
- Internationale Liga für Menschenrechte e. V. (ILMR)
- Piratenpartei – Landesverband Bremen

- ver.di – Ortsverein Bremen
- Verein für Rechtshilfe im Justizvollzug des Landes Bremen e. V.
- Susanne Wendland, Mitglied der Bremischen Bürgerschaft (parteilos)
- Elke Bahl und Prof. Dr. Helmut Pollähne vom Kriminalpolitischen Arbeitskreis Bremen (kripak)

Unsere Website: *https://brementrojaner.de/*

Nach den Protesten wurde die Initiative durch die Grünen, die gemeinsam mit der SPD in Bremen regieren, zunächst gestoppt. Der weitere Fortgang des Gesetzgebungsverfahrens ist unklar.

BAfF – Berliner Allianz für Freiheitsrechte – Pressemitteilung

Berliner Allianz für Freiheitsrechte für die Sicherung grundgesetzlich garantierter Freiheit hat sich gegründet!

11. April 2018 – Am 11. April 2018 hat sich die Berliner Allianz für Freiheitsrechte gegen das von Thomas Heilmann, Heinz Buschkowsky und anderen angestrebte Volksbegehren gegründet. Die Berliner Allianz für Freiheitsrechte will, dass sich Parteien und Zivilgesellschaft gleichermaßen gegen den Ausbau von Videoüberwachung und für die Freiheitsrechte der Menschen einsetzen.

Max Althoff, Rechtsanwalt, erklärt dazu: „Die geplante massenhafte Videoüberwachung der Initiative mit dem irreführenden Namen ‚Aktionsbündnis für mehr Videoaufklärung und Datenschutz' stellt die Menschen unter Generalverdacht, schafft Misstrauen und verändert die Art, wie wir miteinander umgehen. Eine Ausweitung der Videoüberwachung oder gar eine Tonüberwachung im öffentlichen Raum lehnen wir daher ab. Videoüberwachung ist der Einstieg in ein umfassendes Überwachungssystem für mehr Kontrolle über jeden von uns."

Maximilian Blum, Sprecher der LAG Netzpolitik der Linken ergänzt: „Mit der vom Volksbegehren angestrebten ‚intelligenten Technik' der Videoüberwachung sollen mittels eines 'speziellen Algorithmus' ‚potentiell gefährliche Situationen' in ‚automatischer Früherkennung' identifiziert werden. Hieraus geht eindeutig hervor, dass es nicht nur um Täteraufklärung geht, sondern um die massenhafte Überwachung von Personen, denen ausgehend von entsprechenden Algorithmen ein mehr oder weniger großes Potential zur Begehung einer Straftat pauschal zugesprochen wird. Eine so umfassende Überwachungstechnologie schlägt schnell von einer Verhaltensanalyse in eine Verhaltenssteuerung um."

Aus Sicht der Berliner Allianz für Freiheitsrechte führt ein Ausbau der Videoüberwachung niemals zu mehr Sicherheit. „Sie kann nur ein rein subjektives Unsicherheitsgefühl beruhigen, führt letztendlich aber nur zur Verlagerung der Kriminalität an andere Orte", so Thilo Weichert vom Netzwerk Datenschutzexpertise. „Zielgerechter wäre es, wenn die Ursachen der Probleme analysiert würden und die Politik sich aktiv mit deren Beseitigung beschäftigte, anstatt weiter auf eine Politik der Verdrängung und Repression zu setzen."

Alexander Spies, der ehemalige Vorsitzende der Piratenfraktion im Abgeordnetenhaus, ergänzt: „Mit der Fokussierung auf Videoüberwachung machen sich die Initiatoren einen schlanken Fuß, führen die Menschen und ihre Sorgen in die Irre und verweigern tatsächliche Antworten auf sicherheitspolitische Fragestellungen. Damit setzt das Volksbegehren den Weg der Berliner CDU fort, den diese schon als Teil des Senats verfolgte: die reine Verschleppung der Probleme."

Auch das massenhafte Speichern von Daten stößt bei der Berliner Allianz für Freiheitsrechte auf erhebliche Kritik. Dazu Werner Hülsmann, stellvertretender Vorsitzender der Deutschen Vereinigung für Datenschutz: „Es ist bekannt, dass das massenhafte Speichern von Daten weitere Begehrlichkeiten weckt und immer auch die Gefahr birgt, dass diese abhanden kommen. Das Grundrecht auf Datenschutz und informationelle Selbstbestimmung kann bei Nutzung so einer Masseninfrastruktur nicht garantiert werden. Deshalb stellt ein Ausbau der Überwachung sogar ein erhöhtes Sicherheitsrisiko dar. Die gewonnenen Ton- und Videodaten werden aufgrund der riesigen Masse nur automatisch ausgewertet. Ob hier Ballspiele von Schlägereien unterschieden werden können, ist höchst fraglich. Ein direktes Eingreifen bei einer Gefahr findet nicht statt, weil Kameras niemals eingreifen und einer bedrängten Person helfen können. Das bringt kein Mehr an Sicherheit, und auch keine PolizistIn ist bei einer gefährlichen Situation tatsächlich vor Ort."

Auch rechtlich sei das Volksbegehren zweifelhaft. Louisa Hattendorff, Sprecherin der Grünen Jugend Berlin, führt aus: „Das Volksbegehren weckt erhebliche verfassungsrechtliche Bedenken. Es sollen auch massenhaft Tonaufnahmen erhoben und einen Monat gespeichert werden. Der Gesetzeswortlaut lässt jede Verhältnismäßigkeit vermissen. Es ist ein Treppenwitz der Geschichte, dass gerade ein ehemaliger Justizsenator so leichtfertig mit den Grenzen unseres Grundgesetzes und den Freiheiten der Menschen umgeht."

Rebecca Cotton sagt: „Wir wollen, dass der Schutz der Privatsphäre, welche sich in Verbindung mit dem einzigen nicht einschränkbaren Grundrecht, der Menschenwürde, aus der Verfassung ableitet (Art. 2 Abs.1 i. V. m. Art. 1 Abs. 1 GG), erhalten bleibt. Dieser Schutz darf nicht unter dem Deckmantel der Sicherheit der BürgerInnen zur Ausweitung der Macht und Informationshoheit des Staates ausgehöhlt werden."

Axel Bussmer von der Humanistischen Union ergänzt: „Aufgrund der zahlreichen, inzwischen von Fachleuten, der Berliner Beauftragten für Datenschutz und Informationsfreiheit, und Verbänden geäußerten verfassungsrechtlichen Bedenken fordern wir die Senatsverwaltung auf, das Gesetzesvorhaben dem Verfassungsgerichtshof des Landes Berlin zur rechtlichen Prüfung vorzulegen und keine Gespräche mit dem Überwachungsbündnis zu führen."

Stefan Strauß

Wachsende Identitätsschatten – wo endet Privatsphäre?

Zum Grundproblem sozio-technischer Identifizierbarkeit beim Datenschutz

Mit der Datenschutzgrundverordnung entsteht ein neues Europäisches Datenschutzregime, das einige Verbesserungen beim Schutz der Privatsphäre verspricht. Doch wie aussichtsreich ist wirksamerer Schutz der Privatsphäre im Zeitalter von Big Data und hochgradig vernetzten Technologien tatsächlich? Dieser Beitrag diskutiert kritisch die Grenzen des Datenschutzes aufgrund einer stetig wachsenden sozio-technischen Identifizierbarkeit und schlägt eine Typologie von Identitätsinformation als Beitrag zur systematischeren Erfassung datenschutzrelevanter Informationsprozesse vor, um dieses Grundproblem einzudämmen.

Wie weit trägt die Datenschutzgrundverordnung?

Die Datenschutzgrundverordnung (DSGVO) ist ein zentraler Meilenstein zur mittel- und langfristigen Stärkung des Datenschutzniveaus und eröffnet neue Handlungsspielräume. Neben deutlich erhöhtem Sanktionsrahmen sind vor allem zwei eng verzahnte Instrumente wesentlich: Datenschutz-Folgenabschätzungen (Privacy Impact Assessment – PIA) und Maßnahmen für Privacy-by-Design (PbD). Inwieweit sich Datenschutzstandards wirklich nachhaltig stärken lassen, ist jedoch noch weitgehend offen. Fortschreitende Digitalisierung und *Big-Data*-Paradigmen verleiten vielfach zu erweiterter Datennutzung und strapazieren das Ideal informationeller Selbstbestimmung (BVerfG 1983). Datenhandel und Profiling erfordern zwar im Sinne der DSGVO die Durchführung von PIA, sofern die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben kann (Art. 35 DSGVO). Ob Datensammelpraktiken damit deutlich eingrenzbar sind, wird sich zeigen, denn viele verschiedene Akteure agieren hier im rechtlichen Graubereich und erfassen große Datenmengen scheinbar beiläufig. Die jüngsten Vorfälle rund um *Facebook* und *Cambridge Analytica* verdeutlichen, wie umfang- und folgenreich diese Praktiken sein können (Davies 2018). Ohne breiten öffentlichen Diskurs wissen Betroffene davon meist gar nichts oder bleiben eher ratlos zurück. Konsequentes Nichtnutzen von Anwendungen oder Verweigern der Zustimmung zur Datenverarbeitung sind schwierig und digitale Informationsflüsse gerade bei vernetzten Verarbeitungskontexten de facto kaum kontrollierbar. Die DSGVO ist wichtig, aber alleine nicht ausreichend für Verbesserungen. Auch rechtskonforme Datenverarbeitung kann ethisch problematisch sein und tief in die Privatsphäre eindringen. Technische Trends von *smarten* Technologien, autonomen Fahrzeugen, dem *Internet der Dinge* usw. machen klar: Vernetzte Systeme bzw. Anwendungskontexte nehmen weiter zu und digitale Informationsflüsse lassen sich noch schwerer kontrollieren. Steigende Vernetzung bedeutet mehr Daten und damit mehr Möglichkeiten zur Verkettung und Aggregation unterschiedlicher Datenbestände. Es bleibt daher trotz DSGVO fraglich, inwieweit der wachsenden Komplexität digitaler Technologien bzw. sozio-technischer Systeme wirksam begegnet werden kann. Datenschutz-Analysen oder PIA sind meist kontextspezifisch und je nach Technologie unterschiedlich. Selbst Auffassungen über personenbezogene Daten können dabei variieren. Beispiel ist die in vielen Ländern unterschiedlich diskutierte Frage, inwieweit IP-Adressen als personenbezogen gelten. Ähnliches gilt für den Begriff *Metadaten* oder die unscharfe Abgrenzbarkeit zwischen direkt und indirekt personenbezogenen Daten. Zunehmend automatisierte Datenverarbeitung und technisch generierte Informationen verwischen die Grenzen. Noch fehlen gemeinsame Standards, das ist eine grundsätzliche Hürde für ein höheres Datenschutzniveau.

Öffentliche wie private Institutionen haben zwar wichtigen Handlungsspielraum bei der Umsetzung der DSGVO, doch mit offenen Fragen, was auf Kosten der Wirksamkeit von PIA und

PbD abseits rechtlicher Vorgaben gehen kann. PIA und PbD setzen detailliertes Wissen über Art und Struktur personenbezogener Daten sowie die verarbeitenden Informationssysteme voraus. Der je nach Anwendungsbereich mitunter hohe Komplexitätsgrad kann die Wirksamkeit von Datenschutz-Maßnahmen auch bei Rechtskonformität enorm beeinträchtigen. Mittelfristig ist mit unterschiedlichen Vorgehensmodellen und Handlungsabläufen zur DSGVO-Umsetzung zu rechnen, beispielsweise beim gebotenen Datenverarbeitungs-Verzeichnis, der PbD-Implementierung oder der konkreten Durchführung von PIA. Hier besteht Wildwuchsgefahr, die in der Praxis zu variierenden Datenschutzstandards auch in Europa führen könnte.

Sozio-technische Identifizierbarkeit als Kernproblem des Datenschutzes

Abseits rechtlicher Normen hängt die Wirksamkeit von Datenschutz-Maßnahmen wesentlich vom technischen und konzeptionellen Verständnis über jene Mechanismen ab, die auf die Privatsphäre einwirken. In der digital vernetzten Gesellschaft ist aber zusehends schwieriger fassbar, *was* unter personenbezogenen Daten eigentlich zu verstehen ist. *Big Data* ist symptomatisch für die verschwimmende Grenze zwischen personenbezogenen und nicht-personenbezogenen Daten (Strauß 2018). Wege aus dieser Misere erfordern neue Perspektiven auf bestehende Datenschutz-Konzepte, um den Anforderungen der digitalen Welt besser gerecht werden zu können. Wesentlich ist dabei, dass Identifikation der zentrale Mechanismus bei der personenbezogenen Datenverarbeitung ist: Die Möglichkeiten, eine Person zu identifizieren, sind ausschlaggebend für das Ausmaß der Auswirkungen auf die Privatsphäre dieser Person. Identifizierbarkeit ist das primäre Risiko für die Privatsphäre, das weitere Risiken nach sich ziehen kann (Strauß 2017). Das klingt zunächst trivial, meint Datenschutz doch seit jeher Informationen über identifizierte oder identifizierbare Personen[1]. Technische Standards verwenden zudem meist den (u. a. in den USA gängigen) Begriff der „personally identifiable information" (PII)[2]. In der Praxis werden diese Begriffe aber oft sehr unterschiedlich breit oder eng ausgelegt, was zu Problemen führen kann.[3] Das gleiche gilt für personenbezogene Daten, die je nach nationaler Gesetzgebung variabel interpretierbar sind. Erschwerend kommt hinzu, dass persönliche Identität selbst nicht nur statische, sondern auch dynamische Züge aufweist. Paul Ricoeur unterscheidet zwei Wesenszüge von Identität: Zum einen ist Identität etwas fortwährend Beständiges *(idem* bzw. *Gleichheit)* (Ricoeur 1992). Dementsprechend kann Identität durch gleichbleibende Attribute repräsentiert werden und wird dadurch unterscheidbar von anderen Entitäten. Zum anderen ist Identität aber auch dynamisch und in permanenter Entwicklung *(ipse* bzw. *Selbstheit).* In Summe lässt sich Identität daher als dialektisches Konzept aus Gleichheit und Selbstheit bzw. statischen und dynamischen Komponenten begreifen (Strauß 2017). Das ist insofern relevant, als digitale Technologien veränderte und noch dynamischere Formen der Identifikation hervorbringen können. Digitale Information ist an sich bereits dynamisch. Mit Verarbeitung von digitalen Informationen, die auf die Identität einer Person verweisen, wird auch die Identifizierbarkeit einer Person selbst zur variablen Größe. Als Konsequenz hängt die Wirksamkeit von Maßnahmen wie PbD erheblich vom jeweiligen Begriffsverständnis über personenbezogene Daten oder Identitätsinformation ab. Versteht man Identität nur als unveränderbares, statisches Konzept, das aus klar definierten Attributen besteht wie typischerweise Name, Geburtsdatum und -Ort usw., eindeutigen Personenkennzeichen oder biometrischen Merkmalen, bleiben dynamischere Attribute, die ebenso zur Identifikation nutzbar sind (Datenspuren, Quasi-Identifikatoren, technische IDs, Fingerprinting-Techniken usw.) außen vor. Gerade Profiling und ähnliche Praktiken machen aber starken Gebrauch von relativ dynamischen Identitätsattributen als vermeintlichen Nebenprodukten der Nutzung digitaler Technologien. Hier wird die Problematik wachsender digitaler „Identitätsschatten" (Strauß 2017) sichtbar. Die vorherrschende Standard-Einstellung in sozio-technischen Systemen im Sinne einer *Identifiability-by-Default* begünstigt diese Problematik. Technologien begünstigen durch mangelnde oder eingeschränkte Datenschutz- und Sicherheitskonzepte Identifizierbarkeit häufig eher als sie zu verhindern. Bei der Nutzung technischer Anwendungen werden oft zusätzliche Identifikatoren erzeugt, die Rückschlüsse auf einzelne Personen erlauben. So besteht ein inhärenter Konflikt zwischen Privacy-by-Design und Identifiability-by-Default (ebd.). Zu enge oder unpräzise Auffassungen von personenbezogenen Daten erschweren wirksamen Schutz.

Rechtlich gelten neben Namen primär Personenkennzeichen, Identifikationsnummern etc. sowie spezifische Personen-Merkmale als personenbezogene Daten. Das betrifft zwar grundsätzlich auch technische Identifikatoren. In der Praxis ist aber oft unklar, inwieweit technische Information als personenbezogen gilt oder nicht: Sind es etwa *nur* IP-Adressen oder auch andere Kennungen, Metadaten etc.? Unabhängig von der rechtlichen Beurteilung ist eine Präzisierung sinnvoll – gerade aufgrund wachsender Identitätsschatten. Bei jeder Nutzung digitaler Technologien entstehen viele Möglichkeiten zur indirekten bzw. impliziten Identifikation. Mittels Aggregation verschiedener Daten können Quasi-Identifikatoren erzeugt werden, wodurch eine Person auch ohne Zutun oder Wissen identifizierbar wird (ebd.). Gängiges Beispiel ist das Erstellen digitaler Fingerabdrücke *(Fingerprinting)* durch bloße Nutzung einer Technologie zur Verfolgung von Internet-NutzerInnen und das Erzeugen entsprechender Benutzer-Profile (Gierow 2017). Die dazu genutzten Informationen sind oft keine personenbezogenen Daten im engeren Sinn, die Auswirkungen für die Privatsphäre aber dennoch erheblich. Es bedarf daher eines tieferen Verständnisses von Identifizierbarkeit und Identitätsinformation in sozio-technischen Systemen, um datenschutzrelevante Verarbeitungsvorgänge genauer zu erfassen, Datenschutz-Folgeabschätzungen systematischer durchzuführen sowie PbD-Konzepte wirksamer zu gestalten. Denn im Kern geht es um das Erkennen und Schützen von Identitätsinformation, direkter wie indirekter.

Vier Dimensionen von Identifizierbarkeit

Ein wirksames Konzept von Identitätsinformation statt personenbezogener Daten ist relevant, weil es Personenbezug einbezieht und zugleich hilft, technisch generierte Daten mit möglichem Personenbezug nicht zu vernachlässigen. Identifizierbarkeit ist Grundvoraussetzung für Identifikation und ermöglicht Information zu verarbeiten, die direkt oder indirekt auf die Identität einer Person verweist. Identifizierbarkeit setzt grundsätzlich die Verfügbarkeit von Identitätsinformation vor-

aus (Strauß 2017). Die Crux ist hierbei, genauer zu spezifizieren, was unter Identitätsinformation zu verstehen ist, die im zeitlichen Verlauf eher zu- als abnimmt[4]. Streng genommen sind vollständige Aufzählungen aufgrund des dynamischen Charakters von Identität und digitaler Information zum Scheitern verurteilt. Um das Ausmaß von Identifizierbarkeit dennoch besser fassen zu können, schlage ich eine Typologie von Identitätsinformation vor, die von vier grundlegenden, aufeinander aufbauenden Dimensionen ausgeht (Abbildung 1): Substanzielle, räumlich-zeitliche, relationale und interaktionale Identitätsinformation.

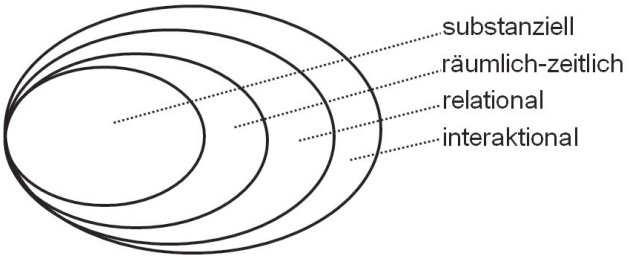


Abbildung 1: Vier Dimensionen von Identitätsinformation

Diese vier Dimensionen erlauben es Identitätsinformation genauer zu spezifizieren. Sie leiten sich aus einer systemtheoretischen Perspektive ab: Ein sozio-technisches System besteht nicht nur aus der Summe seiner Elemente, sondern auch aus den Beziehungen (Relationen) zwischen diesen Elementen innerhalb und außerhalb des Systems (seiner Umwelt) in unterschiedlichen räumlich-zeitlichen Kontexten. Auf ähnliche Weise lässt sich eine Person als systemische Entität begreifen, die über substanzielle Merkmale verfügt, Relationen bzw. Beziehungen zu anderen hat, und mit ihrer Umwelt und anderen Entitäten in unterschiedlichen räumlich-zeitlichen Kontexten interagiert. Diese Informationstypen sind maßgebliche Bestandteile der informationellen Identitäts-Repräsentation. Ausmaß und Zusammenspiel von Informationen entlang dieser Dimensionen haben daher Auswirkungen auf die Identifizierbarkeit der Person. Das gilt auch für die zur Informationsverarbeitung verwendeten Technologien, denn auch eine Technologie hat eine Art substanziellen Kern, wird in räumlich-zeitlichen Kontexten eingesetzt, hat meist interne und externe Relationen zu anderen technischen Komponenten und interagiert mit diesen. Die Beschaffenheit eines sozio-technischen Systems, das Identitätsinformation verarbeitet, kann daher Auswirkungen auf die Qualität dieser Information haben. Gerade digitale Technologien bestehen meist aus vielen miteinander vernetzten Komponenten (bzw. Teilsystemen). Die Identifizierbarkeit und damit der Schutz der Privatsphäre der Person hängen daher wesentlich von der Beschaffenheit und Konfiguration jener sozio-technischen Systeme ab, die ihre Identitätsinformation verarbeiten. Eine weitere Differenzierung zwischen personen-spezifischen (PII) und technologie-spezifischen Identitätsinformationen (TII) ist daher sinnvoll. Beide Typen können anhand der genannten vier Grunddimensionen beschrieben werden.

PII – Personen-spezifische Identitätsinformation

PII meint all jene Informationen, die direkt oder indirekt auf die Identität einer Person verweisen. Das deckt sich zunächst mit dem gängigen Verständnis von personenbezogenen Daten (im Sinne von DSGVO u. ISO), die in unterschiedlichen Formen häufig erhoben werden. Doch entlang der oben genannten Dimensionen entsteht ein differenzierteres Bild – PII lassen sich damit wie folgt zuordnen (Strauß 2017):

- Substanzielle PII (P1) meint wesentliche Identitätsmerkmale, also all jene Informationen, die sozusagen die *Substanz* der Identität einer Person beschreiben. Neben dem Namen als primären Identifikator sind das typischerweise wesentliche Merkmale über Aussehen und Beschaffenheit der Person wie Augen- und Haarfarbe, Größe, Gewicht, Geschlecht oder biometrische Merkmale wie Fingerprints, Gesichts-, Iris- oder auch Sprachmuster bis zur DNS.

- Räumlich-zeitliche PII (P2) meint all jene Information, die räumliche und/oder zeitliche Merkmale über die Person beschreibt. Geläufig sind v. a. Alter, Geburtsdatum und -Ort, Nationalität, Anschrift(en) privat/beruflich, Wohnort, Arbeitsplatz, Aufenthaltsort usw.

- Relationale PII (P3) umfasst alle Information über Beziehungen im engeren und weiteren Sinn. Typischerweise sind das etwa persönlicher Beziehungsstatus (verheiratet/ledig), Beschäftigungsstatus, Informationen über Arbeitgeber, Familie, Verwandte und Freunde usw.

- Interaktionale PII (P4) meint all jene Information, die bei Interaktionen der betroffenen Person mit anderen (Entitäten) entsteht wie persönliche Interessen, Aktivitäten, Verhalten, Meinungen usw. Darunter fallen auch sensible Informationen wie politische und religiöse Einstellungen, sexuelle Vorlieben etc.

Die genannten Beispiele können keine vollständige Auflistung bieten sondern sollen diese vier Grundtypen von Identitätsinformation näher erläutern. PII enthalten also vor allem Aspekte

Stefan Strauß

Foto: ITA/Peissl

Dr. **Stefan Strauß** ist promovierter Wirtschaftsinformatiker am Institut für Technikfolgen-Abschätzung (ITA) an der Österreichischen Akademie der Wissenschaften in Wien. Er forscht an der Schnittstelle zwischen Informatik und Gesellschaft, insbesondere zu Governance sozio-technischer Systeme, Privatsphäre, Sicherheit und Überwachung, digitaler Identität und Privacy Impact Assessment. Weitere Forschungsinteressen im Feld der Informations- und Computerethik.

wie: Was ist der substanzielle Kern der Identitätsinformation bzw. welche Informationen beschreiben primär die Identität einer Person? Welche Informationen beschreiben darüber hinaus räumlich-zeitliche Kontexte, Relationen und Interaktionen diese Person betreffend? Die informationelle Identität der Person lässt sich so als Satz von Informationen verstehen, der zum einen weitgehend invariante, substanzielle Identitätskriterien aufweist wie eben Name, Geburtsdatum, Geschlecht, biometrische Merkmale usw. Zum anderen gibt es aber eine Reihe weiterer Informationen, die auf die Identität der Person verweisen können. Diese Informationen sind vergleichsweise eher dynamischer Natur. Anhand der weiteren Typen (räumlich-zeitlich, relational, interaktional) lässt sich diese Dynamik systematischer fassen.

Alle PII-Typen sind auch mit technischen Mitteln abbildbar und werden meist dementsprechend verarbeitet. Allerdings kann sich dadurch die Beschaffenheit der Identitätsinformation selbst verändern. Bei Einsatz und Nutzung von Technologien werden meist weitere Informationen erzeugt, die das Ausmaß an Identifizierbarkeit der betroffenen Person erhöhen. Neben PII führe ich daher zusätzlich die Kategorie *Technologie-spezifische Identitätsinformation (TII)* ein.

TII – Technologie-spezifische Identitätsinformation

TII umfasst jede Information, die bei der Anwendung oder Nutzung einer Technologie entsteht und direkt oder indirekt auf die Identität einer Person verweist. Entlang der oben genannten Dimensionen lassen sich TII wie folgt zuordnen (Strauß 2017):

- Substanzielle TII (T1) meint Informationen technischen Ursprungs, die primär an der Verarbeitung von PII beteiligt sind. Typische Beispiele sind Identifikatoren wie Benutzernamen bzw. IDs (z. B. Benutzername eines Online-Dienstes wie Google, Facebook und Co., E-Mailadresse, Session IDs etc.) oder Kennungen von Geräten (z. B. IP-Adressen, MAC-Adresse, SIM Card IDs, IMEI usw.). Hier kann eine weitere Unterscheidung zwischen Anwendungs- und Geräte-spezifischen TII sinnvoll sein.

- Räumlich-zeitliche TII (T2) meint Information über den Nutzungskontext einer Technologie oder Anwendung. Typische Beispiele sind Zeitstempel, Zeitzone, Standortdaten (Geo-Lokalisierung), Login-Zeiten, -Dauer und ähnliche Informationen über technische Nutzer-Aktivitäten.

- Relationale TII (T3) sind all jene Informationen, die zusätzlich bei der Technologie-Nutzung anfallen, durch Relationen der primären Technologie oder Anwendung mit weiteren Komponenten. Gemeint sind hier vor allem Teil-Systeme der primären Technologie bzw. Anwendung. Das können Software-Komponenten wie Datenbanken, Software des Betriebssystems, Browser, Apps, Social Plugins und Logins usw. sein, aber auch einzelne verbaute Hardware-Komponenten, sogar Kameras, Mikrofone usw. Diese Teil-Systeme müssen nicht direkt von einer Person genutzt werden, um Identitätsinformationen zu verarbeiten oder zusätzliche zu erzeugen. Das können etwa verschiedene Metadaten sein. So verfügt eine Webcam über eine eigene ID, die mitunter Rückschlüsse auf die Nutzer ermöglicht. Ähnliches gilt für spezifische Kennungen von Software, etwa Webbrowsern. In diese Kategorie fallen auch Informationen über Hard- und Softwarekonfigurationen, die sich für die Erzeugung von Quasi-Identifikatoren und damit Fingerprinting-Technik eignen, wie spezifische Einstellungen, Webbrowser-History, bis hin zu Schriftgrößen und Bildschirmauflösung.

- Interaktionale TII (T4) meint Informationen, die bei der Nutzung bzw. Interaktion entstehen. Typischerweise sind das technisch erzeugte Benutzer-Inhalte, beispielsweise gesendete Nachrichten, Postings, Kommentare, *Likes,* sonstiges Text-, Bild- oder Ton-Material wie Fotos, Audio- und Videodateien, aber auch technische Information über Kontakte usw. Wie soziale Medien verdeutlichen, ist die Liste von Online-Inhalten hier nahezu beliebig erweiterbar. Auch Metadaten über die Interaktion sind hier gemeint, wie Orts- und Zeitstempel, Anzahl an Nachrichten und beteiligten Kommunikationspartnern, Interaktions- oder Gesprächsdauer etc. Sogar Hardware-Interaktion erzeugt Datenspuren wie Nutzungsmuster von Keyboard, Maus, Touchscreens usw., aus denen potenziell digitale Fingerprints generiert werden können.

Zusammenfassung und Fazit

Die fortschreitende digitale Transformation der Gesellschaft bringt immer gravierendere Herausforderungen für den Datenschutz. Die DSGVO eröffnet Potenzial für eine nachhaltige Stärkung des Schutzniveaus. Das erfordert aber auch ein tieferes Verständnis für jene sozio-technischen Mechanismen, die die Privatsphäre maßgeblich beeinträchtigen können. Das ist wesentlich für die Entwicklung längerfristig wirksamer Schutzkonzepte. Die vorgestellte Typologie kann einen wertvollen Beitrag zur systematischeren Analyse digitaler Informationsflüsse mit Datenschutz-Relevanz leisten. Solche Analysen sind wesentlich für PIA, die nicht nur ein rechtliches Erfordernis in bestimmten Fällen, sondern ein zentrales Instrument für Datenschutz-konforme Technikgestaltung und damit PbD darstellt. Die Typologie ist weitgehend Technologie-neutral und unterstützt bei der Erfassung von Informationen, die direkt oder indirekt auf die Identität einer Person verweisen und damit potenziell datenschutz- und sicherheitsrelevant sind. Die genannten Dimensionen bzw. Grundtypen sind in unterschiedlichem Ausmaß in jedem sozio-technischen System zu finden. Gerade TII verdeutlichen die Fülle technischer Identitätsinformationen und deren weitreichende Folgen für die Privatsphäre bei unkontrollierter Verarbeitung. Vor allem relationale und interaktionale TII können sich je nach analytischer Perspektive überlappen, was eine eindeutige Zuordnung teils erschwert. Trotzdem ist eine Differenzierung nützlich, um das Ausmaß der Identifizierbarkeit genauer zu erfassen. Auch sind nicht alle Arten von TII à priori datenschutzrelevant. Das hängt wesentlich vom konkreten Anwendungskontext ab und inwieweit die Informationen gezielt verarbeitet und gespeichert werden. Werden IP-Adressen oder technische Identifikatoren gar nicht erfasst, sind sie zumindest keine TII mit Datenschutzrelevanz in Bezug auf die konkrete Anwendung. Das gleiche gilt für Informationen für potenzielles Fingerprinting, über die Anwendungsbetreiber oft gar keine Kontrolle haben. Allerdings können diese Informationen sicherheitsrelevant sein, und Kenntnis darüber wichtig zur Verbesserung von Schutzmaßnahmen. Gerade sicherheitsbewusste Un-

ternehmen sollten ihre Informationsprozesse im Detail kennen, um diese wirksamer schützen zu können. TII als eigene Kategorie ermöglichen die Berücksichtigung jener Informationsarten, die implizit auf die Identität einer Person verweisen und daher besonders schwer kontrollierbar sind. Das trägt zur Datensparsamkeit, aber auch zum Erkennen von etwaigen Sicherheitslücken bei, was nicht nur den betroffenen Personen, sondern auch Technologie-Betreibern und Entwicklern zugutekommt.

Literatur

DSGVO – Datenschutzgrundverordnung – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG

Davies H (2018): Facebook told me it would act swiftly on data misuse – in 2015. The Guardian, March 26, https://www.theguardian.com/commentisfree/2018/mar/26/facebook-data-misuse-cambridge-analytica

BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil)

Strauß S (2017): Chasing shadows: the interplay of privacy and (digital) identification – toward an identifiability-based framework for privacy impact assessment. Dissertation, Fakultät für Informatik, Technische Universität Wien

McCallister E; Grance, T.; Scarfone, K. (2010): Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Recommendations of the National Institute of Standards and Technology (NIST), Special publication 800-122. U.S. Department of Commerce.

ISO – International Standards Organisation (2011): Information technology – Security techniques – Privacy framework. ISO/IEC 29100:2011(E). 1st edition 2011-12-15.

Schwartz PM.; Solove DJ (2011): The PII problem: privacy and a new concept of personally identifiable information. New York University Law Review (86): 1814-1894.

Ricoeur P (1992); Oneself as Another. (Translated by Kathleen Blamey). University of Chicago Press.

Gierow H (2017): Nutzer lassen sich über Browser hinweg tracken, Golem, 17. Januar, https://www.golem.de/news/fingerprinting-nutzer-lassen-sich-ueber-browser-hinweg-tracken-1701-125627.html

Hansen M, Pfitzmann A, Steinbrecher S (2008): Identity management throughout one's whole life. Information Security Technical Report 13(2008): 83-94.

Strauß S (2018) Big Data – within the tides of securitisation? In: A.R. Saetnan et al. (eds.): The Politics of Big Data – Big Data, Big Brother?, Routledge, 46-67

Anmerkungen

1 *vgl. Art. 4 DSGVO*
2 *McCallister et al. 2010; ISO 2011*
3 *vgl. z. B. Schwartz/Solove 2011*
4 *vgl. Hansen et al. 2008*

Alexander Roßnagel

Datenschutz-Grundverordnung – was bewirkt sie für den Datenschutz?

Die Datenschutz-Grundverordnung der Europäischen Union hat hohe Erwartungen geweckt und wird mit großen Hoffnungen erwartet. Der Beitrag untersucht, ob diese berechtigt sind und ob die Verordnung dazu beitragen kann, den Datenschutz tatsächlich zu verbessern. Das Ergebnis ist gemischt: Nüchtern betrachtet führt sie weder zu einem einheitlichen Datenschutzrecht in Europa noch zu Datenschutzregelungen, die den modernen Herausforderungen gerecht werden. Gewisse Hoffnungen sind jedoch berechtigt, dass sie den Vollzug des Datenschutzrechts verbessert.

1. Datenschutz-Grundverordnung – Hoffnungen und Erwartungen

Nach mehreren Jahren vorbereitender Diskussion und einem anschließenden Gesetzgebungsprozess von über vier Jahren ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO)[1] am 25. Mai 2016 in Kraft getreten. Sie gilt vom 25. Mai 2018 an mit all ihren Regelungen[2] in allen Mitgliedstaaten unmittelbar und wird Teil ihrer Rechtsordnung.

Die DSGVO sollte durch eine Verordnung über den Schutz der Privatsphäre in der elektronischen Kommunikation, abkürzend E-Privacy-VO genannt, bereichsspezifisch ergänzt werden. Diese Verordnung soll die Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG) von 2002 ablösen. Sie sollte ebenfalls am 25. Mai 2018 Geltung erlangen. Da sie aber bisher nur in Form eines Vorschlags der Kommission vom 10. Januar 2017[3] und einer Stellungnahme des Parlaments vom 24. Oktober 2017[4] vorliegt, ist mit ihrer Verabschiedung vor Ende 2018 nicht zu rechnen.[5]

Die DSGVO wurde mit großen Versprechen angekündigt[6], mit hohen Erwartungen versehen[7], mit tiefen Enttäuschungen aufgenommen[8] und durch viel Lobby-Arbeit beeinflusst.[9] Sie wird im Ergebnis sehr unterschiedlich bewertet. Sie wird – vor allem von den an ihrem Entstehen Beteiligten – als „Meilenstein" bezeichnet[10], als „Goldstandard" gepriesen[11] sowie als „Beginn einer neuen Zeitrechnung im Datenschutzrecht"[12] und als „festes Fundament für die anstehenden Herausforderungen der Digitalisierung" gefeiert.[13] Umgekehrt wird sie von anderen zu „einem der schlechtesten Gesetze des 21. Jahrhunderts" gekürt und für das Datenschutzrecht als „größte Katastrophe des 21. Jahrhunderts" bezeichnet.[14]

2. Datenschutz-Grundverordnung – ein weiterer Schritt in der Entwicklung des Datenschutzrechts

Das geltende Datenschutzrecht – auch die DSGVO – stammt konzeptionell aus den 1960er und 1970er Jahren. In dieser Zeit fand die Datenverarbeitung in Rechenzentren statt. Die Daten wurden in Formularen erfasst und per Hand eingegeben. Die Datenverarbeitung betraf nur einen kleinen Ausschnitt des Lebens und war – soweit die Daten bei der betroffenen Person erhoben worden waren – für diese weitgehend kontrollierbar. Wurde die Zweckbindung beachtet, wusste der Betroffene in der Regel, wo welche Daten über ihn verarbeitet wurden. Für diese erste Stufe der Datenverarbeitung sind die grundlegenden Schutzkonzepte des Datenschutzrechts entwickelt worden. Aus dieser Zeit stammen die Regelungen zur Zulässigkeit der Datenverwendung, die Individualisierung der Rechtsdurchsetzung durch Unterrichtung und Benachrichtigung der betroffenen Person, durch ihre Einwilligung und durch ihre Kontrolle in Form von Rechten auf Berichtigung und Löschung, die Anforderungen an Zweckbestimmung, Zweckbindung und Erforderlichkeit der Datenverarbeitung sowie die ergänzende Kontrolle durch Aufsichtsbehörden. Die Nutzung von PCs ab den 1980er Jahren hat die Datenschutzrisiken zwar deutlich erhöht, aber nicht auf eine neue qualitative Stufe gehoben.

Die zweite, qualitativ neue Entwicklungsstufe wurde mit der – weltweiten – Vernetzung der Rechner erreicht. Dadurch entstand ein eigener virtueller Sozialraum, in den nahezu alle Aktivitäten aus der körperlichen Welt übertragen wurden. Jede Handlung in diesem Cyberspace hinterlässt Datenspuren, die ausgewertet werden können und auch werden. Weder die Erhebung der Daten noch deren – letztlich weltweite – Verbreitung und Verwendung können von der betroffenen Person noch kontrolliert werden. Web 2.0 oder Cloud-Computing sind weitere Ausprägungen dieser Entwicklungsstufe. Für sie versuchten die in den 1990er Jahren erlassenen Multimedia-Datenschutzgesetze die Risiken in den Griff zu bekommen. Sie haben für die Internetdienste die Anforderungen an Transparenz, Zweckbindung und Erforderlichkeit verschärft und vor allem die neuen Prinzipien der Datensparsamkeit und des Datenschutzes durch Technik eingeführt. Diese normativen Vorgaben konnten allerdings nur im Wirkungsbereich des Nationalstaats zur Geltung gebracht werden. Die neue Datenverarbeitung betrifft das komplette Leben im virtuellen Sozialraum, je nach Nutzung des Internet einen großen oder kleinen Ausschnitt des täglichen Lebens. Diesen Risiken zu entgehen, würde voraussetzen, den virtuellen Sozialraum zu meiden – für viele keine realistische Alternative. Jedoch besteht zumindest grundsätzlich die Möglichkeit, bildlich gesprochen, den Stecker zu ziehen.

In einer weiteren, dritten Entwicklungsstufe gelangt die Datenverarbeitung in die körperliche Welt. Ubiquitous Computing mit seinen Ausprägungen wie z. B. Smart Cars, Smart Health, Smart Home, Smarten Assistenten, Robotern und sonstige Techniken des Internet der Dinge, die auf der Erfassung der Umgebung durch vielfältige Sensoren und auf der Lernfähigkeit der Systeme durch Künstliche Intelligenz aufbauen, führen zu einer allgegenwärtigen Verarbeitung personenbezogener Daten, die potenziell alle Lebensbereiche und diese potenziell vollständig erfasst. In dieser Welt wachsen Körperlichkeit und Virtualität zusammen. Informationen aus der virtuellen Welt werden in der körperlichen Welt verfügbar, Informationen aus der realen Welt in die virtuelle Welt integriert. Aus dieser Welt und der in ihr stattfindenden Datenverarbeitung gibt es aber keinen Ausweg mehr. Insofern verschärft sich das Problem des Datenschutzes radikal und seine Lösung wird existenziell. Für diese neuen Herausforderungen gibt es noch keine datenschutzrechtlichen Regelungen.

Und auch die alten Regelungen greifen nicht mehr. In einer Welt allgegenwärtiger Datenverarbeitung laufen die bekannten Anforderungen der Zweckbindung, der Erforderlichkeit, der Transparenz, der Einwilligung und der Betroffenenrechte ins Leere. Wenn die allgegenwärtige Rechnertechnik gerade im Hintergrund und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen soll, wird es niemand akzeptieren, wenn er täglich zur Durchsetzung des Transparenzprinzips tausendfach bei meist alltäglichen Verrichtungen Anzeigen, Unterrichtungen oder Hinweise zur Kenntnis nehmen müsste. Wenn die Techniksysteme kontextsensitiv und selbstlernend sein sollen, werden sie aus den vielfältigen Datenspuren, die der Nutzer bei seinen Alltagshandlungen hinterlässt, und seinen Präferenzen, die seinen Handlungen implizit entnommen werden können, entgegen jeder Zweckbindung im Interesse des Nutzers vielfältige und umfassende Profile erzeugen. Wenn die Nutzer auf die Datenspeicher der sie umgebenden Gegenstände zurückgreifen, um ihr eigenes löchriges Gedächtnis zu erweitern, läuft das Erforderlichkeitsprinzip in Leere. Für die Gedächtnisfunktion ist für sehr lange Zeit eine Datenspeicherung auf Vorrat erforderlich, weil niemand wissen kann, an was man sich irgendwann einmal erinnern möchte. Diese Beispiele zeigen: Die allgegenwärtige Datenverarbeitung verursacht nicht nur ein weiteres Vollzugs-, sondern ein grundlegendes Konzeptproblem. Sie stellt die zentralen Schutzkonzepte des Datenschutzrechts in Frage.[15]

Alle drei Entwicklungsstufen bestehen heute parallel und beeinflussen sich gegenseitig. Für jede besteht ein spezifischer Modernisierungsbedarf – für die erste Stufe etwa in der Umsetzung der Datenschutzprinzipien beim Aufbau großer Datenverarbeitungssysteme für staatliche oder private Zwecke. Die unterschiedliche Umsetzung der Datenschutzrichtlinie (DSRL) von 1995 hat zu verschiedenen Datenschutzniveaus geführt, die auch als Standortvorteil genutzt wurden (Stichwort: Irland). Noch immer hat das Datenschutzrecht mit einem großen Vollzugsdefizit zu kämpfen. Für die zweite Stufe besteht der Modernisierungsbedarf vor allem darin, dass global agierende Konzerne mit Suchalgorithmen, sozialen Netzwerken, Plattformen und modernen Kommunikationsmöglichkeiten unverzichtbare Internet-Infrastrukturen ausgebildet haben, die Monopolcharakter haben und deren Geschäftsmodell die massenhafte Verarbeitung personenbezogene Daten voraussetzt. Moderne Datenschutzregelungen müssen den Gefährdungen der informationellen Selbstbestimmung durch diese neuen Infrastrukturen in einer Weise entgegentreten, die der Abhängigkeit von ihnen gerecht wird. Für die dritte Stufe besteht der Modernisierungsbedarf vor allem darin, neue Schutzkonzepte für die informationelle Selbstbestimmung zu entwickeln, weil die bisherigen gegenüber den neuen Technikanwendungen leerlaufen. Die Zukunftsfähigkeit neuer Datenschutzregelungen muss daran gemessen werden, ob sie den Herausforderungen auf allen drei Entwicklungsstufen gerecht werden und neue Lösungen für die Gefährdungen der Grundrechtsverwirklichung bieten.

3. Zielsetzungen der Datenschutz-Grundverordnung

Die DSGVO erhebt den Anspruch, den genannten Anforderungen an den Datenschutz gerecht zu werden und die festgestellten Defizite zu beseitigen. Ausweislich ihrer Erwägungsgründe (EG) verfolgt sie drei große Zielsetzungen:

- Zum einen will sie das Datenschutzrecht **unionsweit vereinheitlichen** und einen soliden, „kohärenten und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union" schaffen (EG 3, 9 und 13).

- Zum anderen will sie einheitliche Vorgaben für **gleiche wirtschaftliche Bedingungen** in der Union bieten und damit den Binnenmarkt stärken (EG 5, 10, 13). „Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden" (EG 10).

- Schließlich stellt sie fest, dass „rasche technologische Entwicklungen und die Globalisierung … den Datenschutz vor neue Herausforderungen gestellt" haben (EG 6). Die Verordnung will den Datenschutz angesichts dieser Herausforderungen **modernisieren** und den Schutz der Grundrechte verbessern (EG 1, 2 und 4).

4. Wirkungen der Datenschutz-Grundverordnung

Um zu verstehen, warum die DSGVO diese Ziele weitgehend verfehlt, ist der Machtkampf um die Zukunft des europäischen Datenschutzrechts während der Entstehung der Verordnung zu berücksichtigen. Da nahezu alle Lebens-, Wirtschafts- und Verwaltungsbereiche davon abhängig sind, personenbezogene Daten zu verarbeiten, hat derjenige, der über die Fortentwicklung des Datenschutzes bestimmt, ein zentrales Instrument zur Gestaltung der digitalen Gesellschaft in Europa in der Hand. Daher entspann sich ein heftiger Kampf, wer mit welchen Kompetenzen künftig die Datenverarbeitung reguliert (4.1). Er wirkte sich auf die Kontroversen über die Inhalte der Verordnung aus (4.2 – 4.4), mit denen diese Entwicklung begonnen werden sollte.

4.1 Kompetenzen zur Steuerung der Zukunft

Seit einigen Jahren hat die Kommission ihre Strategie zur europäischen Integration verschärft. Sie wechselte von einer „Angleichung der Rechtsvorschriften" (Art. 114 Abs. 1 AEUV) durch die Mitgliedstaaten zur einer „Vereinheitlichung der Rechtsordnungen" durch den Unionsgesetzgeber. Als Instrument nutzt sie nicht mehr vorrangig die Richtlinie, sondern die Verordnung.[16] Während eine Richtlinie durch die Mitgliedstaaten umgesetzt werden muss und diese nur hinsichtlich ihrer Zielsetzungen bindet, gilt eine Verordnung in den Mitgliedstaaten unmittelbar. Verordnungen entziehen daher ganze Politikbereiche der nationalen Demokratie.[17]

In ihrem Entwurf vom 25. Januar 2012[18] schlug die Kommission eine sehr radikale Lösung für die notwendige kontinuierliche Modernisierung des Datenschutzrechts vor: Durch die **Wahl einer Verordnung** wollte sie die Mitgliedstaaten von der weiteren Gesetzgebung im Bereich des Datenschutzes ausschließen, durch viele unbestimmte und ausfüllungsbedürftige Vorgaben sowie inhaltsleere Generalklauseln wichtige Datenschutzregelungen offen halten und innerhalb der Union sich selbst die Kompetenz vorbehalten, sie auszufüllen und fortzuentwickeln. Zu diesem Zweck sah der Entwurf 26 Ermächtigungen vor, die Verordnung durch **delegierte Rechtsakte** nachträglich zu konkretisieren, und 23 Ermächtigungen, sie durch **Durchführungsrechtsakte** auszugestalten. Außerdem behielt sie sich das Recht vor, bei einer Meinungsverschiedenheit zwischen verschiedenen Aufsichtsbehörden am Ende verbindlich zu entscheiden. Dadurch hätte die Kommission die künftige Rechtsetzung im Datenschutzrecht bei sich zentralisiert und monopolisiert.[19]

Dieser Entwurf hätte zur Folge gehabt, dass die Datenschutzregelungen der **Mitgliedstaaten**, die gerade für öffentliche Stellen stark ausdifferenzierte bereichsspezifische Regelungen enthalten, aufgrund des umfassenden Regelungsanspruchs der Verordnung hinfällig geworden wären. Doch nicht nur für das bestehende Datenschutzrecht hätte der Entwurf gravierende Auswirkungen gehabt. Seine tiefgreifendste Folge wäre die Entmachtung der Mitgliedstaaten und die Ermächtigung der Kommission zur Fortentwicklung des Datenschutzrechts gewesen.

Auf den Angriff der Kommission auf Gewaltenteilung und Demokratie in der Union hat das Parlament nur beschränkt reagiert.[20] Im Machtkampf zwischen Union und Mitgliedstaaten hielt das Parlament am Rechtsinstrument einer **Verordnung** fest. Insofern trug es die Entmachtung der Mitgliedstaaten mit. Es gab jedoch der Kritik insofern nach, als es **Öffnungsklauseln für nationale Regelungen** vorsah. Dadurch aber gab das Parlament selbst die Zielsetzung eines einheitlichen europäischen Datenschutzrechts weitgehend auf.

Hinsichtlich der Gewaltenteilung innerhalb der Union reagierte das Parlament stärker. Es beließ der Kommission nur zehn Ermächtigungen und war bemüht, vieles in der Verordnung selbst zu regeln. Die normative Inhaltsleere der Regelungen versuchte es mit vielfältigen Präzisierungen und Erweiterungen auszugleichen, ohne jedoch ein eigenständiges Regelungskonzept zu entwickeln. In den entscheidenden Fragen kam auch das Parlament angesichts der Komplexität und Breite der Regelungsmaterien über abstrakte Regelungen selten hinaus.

Auch der Rat hat die Wahl einer **Verordnung**, die, soweit sie reicht, den Mitgliedstaaten den Datenschutz als Gegenstand ihrer Politik und Gesetzgebung nimmt, **akzeptiert**.[21] Nicht akzeptiert hat er aber die Machtkonzentration der Kommission und beließ ihr nur neun Ermächtigungen für nebensächliche Fragen. Der Rat strich auch viele Detaillierungen des Parlaments. Die Macht, über die Zukunft der digitalen Gesellschaft zu bestimmen, sollte zum großen Teil bei den Mitgliedstaaten bleiben – insbesondere, wenn es ihre eigenen Angelegenheiten und nicht den europäischen Binnenmarkt betrifft. Überall, wo die geringe Komplexität der Regelungen des Kommissionsentwurfs Detaillierungen forderten, wurden – statt der Kommission – die Mitgliedstaaten ermächtigt, bestehende eigene Regelungen beizubehalten oder neue zu erlassen.

Im „Trilog", in dem sich Vertreter des Rats und des Parlaments unter Vermittlung der Kommission auf eine gemeinsame, die

später verabschiedete Fassung einigten, blieben nur zwei Ermächtigungen der Kommission, **delegierte Rechtsakte** zu erlassen, und sieben Ermächtigungen für **Durchführungsrechtsakte** übrig. In Verhältnis der Union zu den Mitgliedstaaten konnte der Rat seine Ziele uneingeschränkt durchsetzen. Die mangelnde Komplexität der Verordnungsregelungen wird dadurch ausgeglichen, dass die **Mitgliedstaaten** ihre **bereichsspezifischen Datenschutzreglungen** beibehalten oder neue erlassen können. Der Machtkampf bewirkte aber auch, dass die drei expliziten Ziele der DSGVO weitgehend verloren gingen.

4.2 Ko-Regulierung statt Vereinheitlichung des Datenschutzrechts

Die DSGVO hat ein grundlegendes Problem, das durch den Machtkampf verstärkt und nicht beseitigt wurde: die hohe Diskrepanz zwischen der enormen Komplexität des Regelungsbedarfs einerseits sowie die Abstraktheit und damit Unterkomplexität ihrer Vorschriften andererseits. Sie will in 50 Artikeln des materiellen Datenschutzrechts die gleichen Probleme behandeln, für die im deutschen Datenschutzrecht Tausende von bereichsspezifischen Vorschriften bestehen. Wer Datenschutz regelt, verursacht Veränderungen in allen Gesellschaftsbereichen – vom Archivwesen bis zum Zeitungsverlag. Wer meint, die vielen und vielfältigen gesetzlichen Regelungen zum Datenschutz in den Mitgliedstaaten durch wenige generelle und abstrakte Regelungen ersetzen zu können, unterschätzt nicht nur diese Aufgabe gewaltig, sondern übersieht auch die negativen Auswirkungen, die dadurch entstehen, wenn er die Vielfalt und Differenzierung bestehender Regelungen beseitigt und dadurch gewaltige Lücken der Rechtsunsicherheit erzeugt.[22]

Durch diesen unterkomplexen Regelungsansatz muss die DSGVO ihr eigentliches Ziel, einen soliden, kohärenten, einheitlichen Rechtsrahmen für den Datenschutz in allen Mitgliedstaaten der Union zu bilden, verfehlen. Vollzugsfähig und rechtssicher sind die Regelungen der Verordnung nur, wenn sie präzisiert, konkretisiert und ergänzt werden. Dies ist überwiegend Aufgabe der Mitgliedstaaten.[23] Das wichtigste Ergebnis aus dem Machtkampf um die Verordnung sind die 70 Öffnungsklauseln, durch die die Union den Mitgliedstaaten explizit Regelungskompetenzen im Datenschutzrecht überträgt. Diese sind unterschiedlich ausgestaltet. Sie eröffnen den Mitgliedstaaten eigene Regelungsbereiche ohne spezifische Vorgaben – wie in Art. 88[24] für den Beschäftigtendatenschutz.[25] Sie ermächtigen aber auch die Mitgliedstaaten, „spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser" zu bestimmen. Die umfangreichsten Ermächtigungen dieser Art sind in Art. 6 Abs. 2 und 3 zu finden.[26] Danach kann jeder Mitgliedstaat für den gesamten Bereich der Datenverarbeitung in öffentlichen Stellen und in nicht öffentlichen Stellen, die zur Datenverarbeitung verpflichtet werden oder diese im öffentlichen Interesse vornehmen, eigene Regeln erlassen oder beibehalten.

Die Öffnungsklauseln verhindern eine unionsweite Vereinheitlichung des Datenschutzrechts. Dies widerspricht zwar den Wünschen und Hoffnungen, die viele mit der Verordnung verbunden haben. Mehr als dieses Nebeneinander von Unions- und nationalem Datenschutzrecht, das im günstigen Fall zu einer Ko-Regulierung führt, hat der Unionsgesetzgeber aber nicht gewollt.

Wie sehr im Ergebnis ein unionsweit einheitliches Datenschutzrecht verfehlt wird, kann in der Anpassung des deutschen Datenschutzrechts an die DSGVO besichtigt werden. Noch in der 18. Legislaturperiode hat der deutsche Gesetzgeber ergänzend zu ihr erste neue Datenschutzgesetze erlassen. Das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 vom 30. Juni 2017 [27] enthält in Art. 1 das neue Bundesdatenschutzgesetz (BDSG). Dieses tritt am 25. Mai 2018 in Kraft und wird das bisherige BDSG vollständig ersetzen.[28] Art. 2 bis 6 enthalten Anpassungen des BVerfSchG, des MAD-G, des BND-G, des SiÜG und des G10-G. Außerdem hat der Bundesgesetzgeber im Gesetz zur Änderung des Bundesversorgungsgesetzes vom 24. Juli 2017[29] durch Art. 17 Neuregelungen zum Datenschutzrecht in der AO und durch Art. 19 und 24 im SGB I und X getroffen.

Das in Kürze in den Gesetzgebungsprozess einzubringende Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 wird in etwa 140 Artikeln weitere Regelungen zum Datenschutz in Fachgesetzen des Bundes an die Verordnung anpassen. Auch die Länder haben Gesetzgebungsverfahren angestoßen, in denen ihre jeweiligen Landesdatenschutzgesetze sowie ihre bereichsspezifischen Datenschutzregelungen neu gefasst werden.

Der Regulierungsstil dieser nationalen Anpassungsgesetze ist identisch. Sie sind von der Zielsetzung geprägt, das bestehende materielle Datenschutzrecht zu erhalten und nur formelle Anpassungen vorzunehmen. Es entfällt jedoch kein einziges Datenschutzgesetz und auch kein Abschnitt zum Datenschutz in den Fachgesetzen.

Im Ergebnis verfehlt die DSGVO weitgehend ihr Ziel, das Datenschutzrecht in der Union zu vereinheitlichen. Für Rechtsanwender und Rechtsbetroffene ist die Gemengelage aus DSGVO sowie dem weitgehend unveränderten deutschen Datenschutzrecht schwer zu durchschauen und verursacht ein hohes Maß an Rechtsunsicherheit.

4.3 Kontinuität in den Mitgliedstaaten statt einheitlicher Datenschutzpraxis

Stärker kommt die DSGVO im Bereich der Wirtschaft zur Anwendung. Doch auch wenn in allen Mitgliedstaaten die gleichen Vorschriften gelten, führt dies nicht immer zu unionsweit einheitlichen Wettbewerbsbedingungen. Gerade ihre vielen abstrakten und unbestimmten Regelungen bedürfen in der Praxis der Präzisierung und Konkretisierung durch die Verantwortlichen, betroffenen Personen, nationalen Aufsichtsbehörden und Gerichte.

Es ist ein entscheidender Unterschied, ob eine Richtlinie fünf Erlaubnistatbestände als Ziele vorgibt, die eine bereichs- und problemspezifische Konkretisierung durch nationale Gesetze erfahren sollen, oder ob die gleichen fünf Erlaubnistatbestände in einer Verordnung unmittelbare Rechtsgeltung haben und die bestehenden ausdifferenzierten und risikobezogenen nationalen Regelungen ersetzen sollen. Die Auslegung der identischen abstrakten Begriffe wird in jedem Mitgliedstaat nach der jeweiligen Datenschutztradition und -kultur erfolgen. Insbesondere

die offene Abwägung berechtigter Interessen der Verantwortlichen mit den schutzwürdigen Interessen der betroffenen Person wird in jedem Mitgliedstaat unterschiedlich sein. Dies ist z. B. für die Videoüberwachung, für Werbung, Auskunfteien, Marktforschung, Scoring, Bonitätsauskünfte oder Internetangebote zu erwarten. Europäischer Datenschutz wird hinsichtlich der Zulässigkeit der Datenverarbeitung in jedem Mitgliedstaat praktisch einen anderen Inhalt haben. Dadurch entsteht kein einheitlich durchgesetztes und gelebtes Recht. Wettbewerbsgleichheit ist so nicht zu erreichen.[30]

Indem die Verordnung die Entscheidung über die Abwägung letztlich auf die Gerichte überträgt, entstehen aber noch viel unterschiedlichere Ergebnisse als unter der DSRL. Bisher waren die typisierten vom Gesetzgeber vorgenommenen Interessenabwägungen wenigstens für Deutschland einheitlich. Jetzt wird es möglich sein, dass sie für lange Zeit von Gerichtsbezirk zu Gerichtsbezirk unterschiedlich ausfallen. Zwar haben für die Anwendung der unbestimmten Rechtsbegriffe die Aufsichtsbehörden des Bundes, der Länder und aller Mitgliedstaaten einen bestimmenden Einfluss. Um diesen unionsweit zu vereinheitlichen, gibt es umständliche Koordinationsmechanismen.[31] Da aber die Beschlüsse des Europäischen Datenschutzausschusses nach Art. 65 DSGVO nur die Aufsichtsbehörden verpflichten und kein allgemeinverbindliches (Exekutiv-)Recht setzen,[32] unterliegen die divergierenden oder vereinheitlichten Versuche der Aufsichtsbehörden, die Verordnung zu interpretieren, der Überprüfung durch die örtlichen Gerichte. Diese können jeden vereinheitlichten Interpretationsversuch durch den Datenschutzausschuss konterkarieren. Eine Vereinheitlichung der Rechtsprechung ist allenfalls in einzelnen Fällen bezogen auf die jeweils enge Fallfrage nach jahrelangen Prozessen[33] durch den EuGH zu erwarten.

4.4 Keine inhaltliche Modernisierung des Datenschutzrechts

Die DSGVO führt für das materielle Datenschutzrecht die Grundkonzeption der Datenschutz-Richtlinie von 1995 fort. Sie enthält keinen grundlegenden innovativen Ansatz, weist jedoch einige sinnvolle Neuerungen auf: Angesichts der Globalisierung der Datenverarbeitung ist die Ausweitung ihres räumlichen Anwendungsbereichs hilfreich. Danach ist die Verordnung auch anwendbar, wenn ein Datenverarbeiter – egal wo – personenbezogene Daten von Personen verarbeitet, die sich in der Union aufhalten und der er entweder Waren oder Dienstleistungen anbietet oder die er durch seine Datenverarbeitung in ihrem Verhalten beobachtet.[34] Bisher unbekannt ist das Recht für betroffene Personen in Art. 20 DSGVO, ihre Daten, die sie einem Verantwortlichen bereitgestellt haben, auf einen anderen Datenverarbeiter zu übertragen. Innovativ sind auch die Anforderungen an den Datenschutz durch Systemgestaltung und Voreinstellungen in Art. 25 DSGVO[35] und die Datenschutz-Folgenabschätzung in Art. 35 DSGVO.[36]

Inhaltlich verursacht die Verordnung Defizite – auch gegenüber dem bisherigen Datenschutzniveau[37] – und verfehlt ihr Modernisierungsziel vor allem durch ihren spezifischen Ansatz der Technikneutralität.[38] Technikneutralität ist sinnvoll, wenn sie verhindern soll, dass rechtliche Vorschriften technische Weiterentwicklungen ausschließen.[39] In der DSGVO wird Technikneutralität aber ideologisch überhöht und im Sinne einer Risikoneutralität[40] genutzt: In keiner Regelung werden die spezifischen Grundrechtsrisiken z. B. von smarten Informationstechniken im Alltag, von Big Data, Cloud Computing oder datengetriebenen Geschäftsmodellen, Künstlicher Intelligenz und selbstlernenden Systemen angesprochen oder gar gelöst. Die gleichen Zulässigkeitsregeln, Zweckbegrenzungen oder Rechte der betroffenen Person gelten für die wenig riskante Kundenliste beim „Bäcker um die Ecke" ebenso wie für diese um Potenzen risikoreicheren Datenverarbeitungsformen. Insbesondere durch abstrakte Zulässigkeitsregelungen wie in Art. 6 Abs. 1 werden die spezifischen Grundrechtsrisiken verfehlt.[41] Damit wird die Verordnung keiner der identifizierten Herausforderungen der zweiten und dritten Entwicklungsstufe der Datenverarbeitung[42] auch nur im Ansatz gerecht.

Letztlich muss klar sein, welche Anforderungen an die Verarbeitungsvorgänge gestellt werden. Diese Zielsetzung darf einerseits nicht dazu führen, dass die Vorschriften an technische Detailmerkmale anknüpfen, so dass sie technische Weiterentwicklungen ausschließen. Andererseits dürfen technikunspezifische Regelungen nicht dazu führen, dass der demokratisch legitimierte und zur Regelung berufene Gesetzgeber sich nicht mit den besonderen Interessenlagen und Risiken sowie passenden Lösungen einer Technikanwendung auseinandersetzt. Technikbezogene Regelungen sind gerade in einem so technikgeprägten Bereich wie dem Datenschutz unabdingbar, sollen die rechtlichen Ziele erreicht werden. Daher müssen spezifische Technikfunktionen und die typischen Verarbeitungszwecke, ihre Risiken und Lösungsansätze interessengerecht und risikoadäquat geregelt werden. Nur so kann die notwendige Rechtssicherheit und Interessengerechtigkeit erreicht werden. Dass es im Unionsrecht sehr wohl möglich ist, sowohl technikneutrale als auch funktions- und risikobezogene Datenschutzvorgaben vorzusehen, zeigen etwa Art. 6 der eCall-VO (EU) 2015/758[43], der klare Datenschutzanforderungen an die Zulässigkeit des automatisierten Notrufs stellt, oder die Regelungen zur Datenverarbeitung in der elektronischen Kommunikation, zum Schutz von Endgeräten und zur Steuerung zulässiger Werbung in den Art. 6, 8 und 16 des Entwurfs einer E-Privacy-VO.[44]

Die deutschen Gesetzgeber haben bisher weder im neuen BDSG noch in den Entwürfen zu den neuen Landesdatenschutzgesetzen die innovativen Impulse der DSGVO aufgenommen noch de-

Alexander Roßnagel

Prof. Dr. **Alexander Roßnagel** ist Universitätsprofessor für öffentliches Recht, Leiter der *Projektgruppe verfassungsverträgliche Technikgestaltung (provet)* im Wissenschaftlichen Zentrum für *Informationstechnikgestaltung (ITeG)* und Sprecher des *Forum Privatheit*.

ren Risikoneutralität durch die risikobezogene Regelung moderner Herausforderungen überwunden. Sie haben die Öffnungsklauseln fast ausschließlich dazu benutzt, Möglichkeiten zur Verarbeitung personenbezogener Daten zu erweitern und Rechte der betroffenen Personen zu beschränken. Damit haben sie im Ergebnis das Datenschutzniveau in Deutschland sowohl gegenüber dem bisherigen BDSG als auch sogar gegenüber der DSGVO reduziert.[45]

5. Innovationen im Vollzug

Die Differenz zwischen Sollen und Sein ist im Datenschutzrecht besonders groß. Daher ist es vor allem relevant, wie die Rechtsdurchsetzung in der DSGVO geregelt ist. Hier dürfte die wirkliche Innovation der Verordnung zu finden sein.

Die Regelung der Unabhängigkeit, der Aufgaben und der Befugnisse der Aufsichtsbehörden sowie deren Zusammenarbeit in der Union umfasst insgesamt 26 Artikel. Die Verordnung hat die Aufgaben und die Befugnisse erheblich ausgeweitet. Wichtig ist vor allem, dass die Aufsichtsbehörde nach Art. 58 Abs. 2 unmittelbare Durchsetzungsbefugnisse hat und z. B. eine rechtswidrige Datenverarbeitung verbieten kann. Eine auffällige Veränderung bringt auch Art. 83, der für Verstöße gegen die Verordnung drastische Sanktionen ermöglicht. Wichtig ist ferner, dass die Aufsichtsbehörde nach Art. 83 Abs. 6 bei Nichtbefolgung ihrer Anweisung Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängen kann, je nachdem, welcher der Beträge höher ist.

Bei Vollzug der Verordnung entsteht allerdings ein Spannungsverhältnis zwischen der Sicherung der „völligen" Unabhängigkeit jeder einzelnen Aufsichtsbehörde in Art. 52 Abs. 1 und dem einheitlichen Vollzug der Verordnung in der Union. Wie der EuGH in drei Entscheidungen zur Stellung der Aufsichtsbehörde in Deutschland, in Österreich und in Ungarn festgestellt hat, darf niemand der unabhängigen Aufsichtsbehörde Weisungen erteilen. Genau dies aber erlaubt Art. 65 Abs. 6 dem Europäischen Datenschutzausschuss. Er kann Entscheidungen treffen, die die betreffende Aufsichtsbehörde binden. Diese ist insoweit nicht mehr unabhängig, sondern muss die Entscheidung der Mehrheit der anderen Aufsichtsbehörden im Ausschuss befolgen. Auch in Deutschland wird die einzelne Aufsichtsbehörde im „kleinen Kohärenzverfahren" nach § 18 BDSG-neu in ihrer Entscheidung von der Mehrheit der anderen Aufsichtsbehörden abhängig. Ein einheitlicher Vollzug in der Union wird wohl ohne Koordination der Aufsichtsbehörden nicht zu erreichen sein und diese Koordination kann nur nach dem Mehrheitsprinzip erfolgen. Dennoch ist zu konstatieren, dass die Mehrheit die einzelne Aufsichtsbehörde zwingen kann und Art. 65 die in Art. 52 garantierte Unabhängigkeit „auf dem Altar" des einheitlichen Vollzugs „opfert".

Wichtig ist aber auch, dass die Zivilgesellschaft in den Vollzug eingebunden wird. Bürger und in ihrer Vertretung Datenschutzverbände können bei der Aufsichtsbehörde Beschwerde einlegen und gegen die Aufsichtsbehörde und gegen den Verantwortlichen Rechtsbehelfe einlegen, wenn sie der Meinung sind, dass gegen die Verordnung verstoßen wird. Haben sie dadurch einen Schaden erlitten, können sie auch Schadensersatz geltend machen.

Ob diese neuen Regelungen die Durchsetzung des Datenschutzrechts in der Wirklichkeit verbessern, hängt davon ab, wie sie in der Praxis angewendet werden. Dies setzt eine den neuen Aufgaben entsprechende Ausstattung der Aufsichtsbehörden voraus,[46] die derzeit noch fehlt. Daran wird der politische Wille zu besserem Datenschutz zu messen sein.[47] Die bisherigen Regelungen im BDSG und in den Landesdatenschutzgesetzen beschränken jedoch die Aufsicht im öffentlichen Bereich im Vergleich zur Verordnung.

6. Modernisierung des europäischen Datenschutzrechts

Die DSGVO hat weder zu einer Vereinheitlichung und Modernisierung des Datenschutzrechts geführt noch wird sie eine einheitliche Datenschutzpraxis in allen Mitgliedstaaten begründen. Statt einer Monopolisierung und Zentralisierung in der Weiterentwicklung des Datenschutzrechts hat sie eine sinnvolle Arbeitsteilung zwischen Union und Mitgliedstaaten eingerichtet. Nur so ist die notwendige Komplexität der Datenschutzregelungen angesichts einer gesellschaftsweiten Verarbeitung personenbezogener Daten zu erreichen. Die angeordnete Ko-Regulierung kann auch für die Suche nach einem modernen Datenschutzrecht eingesetzt werden: Angesichts der Vielfalt und Dynamik der zukünftigen, heute noch unbekannten Herausforderungen der Informationstechnik und ihrer Anwendungen für die Grundrechte kann auf der Ebene der Mitgliedstaaten mit unterschiedlichen Regelungskonzepten experimentiert werden. Deren Vielfalt kann dazu beitragen, dass sich in der Union ein lebendiger Datenschutz entwickelt. Statt einer Vereinheitlichung der Datenschutzpraxis ermöglichen unbestimmte Rechtsbegriffe und ihre situationsgerechte Konkretisierung, dass in den einzelnen Mitgliedstaaten Datenschutz den lokalen Bedingungen angepasst werden kann. Schließlich bieten die vielen Regelungsmöglichkeiten der Mitgliedstaaten Chancen für eine Modernisierung des Datenschutzrechts, indem dort versucht wird, durch risikoadäquate Regelungen einen ausreichenden Schutz der Grundrechte gegen künftige Herausforderungen zu gewährleisten. In den Evaluationen und Überarbeitungen der DSGVO gemäß Art. 97 kann dann das Bewährte unionsweit übernommen werden.

Der Beitrag erschien in vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftpolitik #211/212 (1/2018). Wir danken Redaktion und Autor für die freundliche Genehmigung zum Nachdruck.

Anmerkungen

1 *EU ABl. L 119 vom 4.5.2016, 1.*
2 *Zu den einzelnen Regelungen der DSGVO s. Schaar, vorgänge #211/212, 31-40 und Weichert, vorgänge #211/212, 5-16.*
3 *KOM(2017) 10 endg.*
4 *Europäisches Parlament, A8-0324/2017.*
5 *S. Roßnagel, MedienWirtschaft 1/2018, 32ff.*
6 *Mitteilung der Europäischen Kommission: Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg.; Justizkommissarin Reding, ZD 2012, 195.*

7 S. z. B. Schaar, DuD 2012, 154.
8 S. z. B. Berufsverband der Datenschutzbeauftragten Deutschlands (BvD), Positionspapier zum Entwurf der DSGVO vom 25.1.2012.
9 S. z. B. Albrecht, CR 2016, 97.
10 Albrecht, CR 2016, 97; BfDI Voßhoff nach heise-online, http://heise.de/-3179872 vom 21.4.2016.
11 Albrecht, CR 2016, 98.
12 Schantz, NJW 2016, 1841.
13 Albrecht, CR 2016, 97.
14 Hoeren, nach heise-online, http://heise.de/-3190299 vom 27.4.2016; ähnlich negativ Giesen, Euphorie ist kein Prinzip des Rechtsstaats, in: Stiftung Datenschutz (Hrsg.), Zukunft der informationellen Selbstbestimmung, 2016, 23 ff.
15 S. hierzu Roßnagel, Datenschutz in einem informatisierten Alltag, 2007.
16 So z. B. in der Mitteilung der Kommission „Eine Vision für den Binnenmarkt für Industrieprodukte" vom 22.1.2014, KOM(2014) 24 endg., 9.
17 S. hierzu auch Roßnagel, in: ders. (Hrsg.), Das neue Datenschutzrecht, 2018, § 1 Rn. 16 ff.
18 KOM(2012) 11 endg.
19 Nach dem Scheitern dieser Strategie werden beide Instrumente der Machtsteigerung vom Generalsekretär der Kommission, Selmayr, nachträglich als geniale Scheingefechte dargestellt, die nie ernst gemeint waren, sondern nur die Mitgliedstaaten zu entsprechenden Entscheidungen verleiten sollten – s. Selmayr/Ehmann, in: Ehmann/Selmayr, DSGVO, 2017, Einleitung Rn. 56.
20 EU-Parlament, P7_TA-PROV(2014)0212.
21 Rat der Europäischen Union, 9565/15.
22 S. näher Roßnagel/Geminn/Jandt/Richter, Datenschutzrecht 2016 – „Smart" genug für die Zukunft?, 2016, 176f.
23 S. hierzu näher Roßnagel (Fn. 17), § 1 Rn. 31 ff. und § 2 Rn. 1 ff.
24 Art. und EG ohne Gesetzesbezeichnung sind solche der DSGVO.
25 S. z. B. Maier, DuD 2017, 169; Roßnagel, DuD 2017, 292.
26 S. Roßnagel, in: Simitis/Hornung/Spiecker, DSGVO, 2018, Art. 6 Abs. 2 Rn. 1 ff. und Art. 6 Abs. 3 Rn. 1 ff.; Roßnagel (Anm. 17), § 2 Rn. 21 ff.; Schaller, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, 2018, § 7 Rn. 16f.
27 BGBl. I, 2097.
28 S. dazu Schaar, vorgänge #211/212, 31-40.
29 BGBl. I, 2541.
30 So aber Voßhoff, in: BfDI-Info 6: Datenschutz-Grundverordnung, 2016, 7.
31 S. Roßnagel, Datenschutzaufsicht nach der EU-Datenschutz-Grund–verordnung, 2017, 77 ff., 146 ff.
32 S. Roßnagel (Anm. 31), 151 ff.
33 Das Urteil zur Vorratsdatenspeicherung vom 8.4.2014 erfolgte über acht Jahre nach Erlass der Richtlinie zur Vorratsdatenspeicherung, das Urteil zu Safe Harbor vom 6.10.2015 erging über 15 Jahre nach der Entscheidung der Kommission zur Anerkennung des Safe-Harbor-Systems.
34 Diese Erweiterung sorgt auf dem europäischen Markt für Wettbewerbsgleichheit zwischen Anbietern in der Union und Anbietern außerhalb der Union und vereinfacht die Wahrnehmung von Betroffenenrechten.
35 Die Anforderung richtet sich jedoch an den verantwortlichen Technikanwender, statt an den Hersteller.
36 Die sich hoffentlich nicht in einem Formalismus erschöpfen wird.
37 Entgegen der Zusicherung der damaligen Justizkommissarin Reding, ZD 2012, 197.
38 S. EG 15; Reding, ZD 2012, 198.
39 S. grundsätzlich Roßnagel, Technikneutrale Regulierung: Möglichkeiten und Grenzen, in: Eifert/Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2009, 323 ff.
40 Der „Risikoansatz" der DSGVO – s. z. B. Albrecht, CR 2016, 94 – beschränkt sich darauf, bestimmte Pflichten des Verantwortlichen „entsprechend der Risiken von Datenverarbeitungsprozessen" zu reduzieren; s. kritisch Roßnagel, DuD 2016, 565, weil dieser Ansatz bewirkt, dass nur ein Bruchteil der Verantwortlichen und Auftragsverarbeiter diese Pflichten erfüllen muss.
41 S. näher Roßnagel, DuD 2016, 565.
42 S. Kap. 2.
43 EU ABl. L 123 vom 19.5.2015, 77.
44 S. hierzu Roßnagel, MedienWirtschaft 1/2018, 32ff.
45 S. dazu Schaar, vorgänge #211/212, 31-40.
46 Roßnagel (Anm. 31), 179 ff.
47 S. zum Datenschutz in der Koalitionsvereinbarung Forum Privatheit, Datenschutz stärken, Innovationen ermöglichen – Wie man den Koalitionsvertrag ausgestalten sollte, Policy Paper, 2018.

Marie-Theres Tinnefeld

Die selbstbestimmte Einwilligung – Bedeutung, Möglichkeiten und Grenzen

Menschenrechtliche Betrachtung

Die Einwilligungserklärung Betroffener ist nach wie vor eine der wichtigsten Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch öffentliche Stellen und durch Private (z. B. Online-Händler). Die EU-Datenschutz-Grundverordnung konkretisiert die Anforderungen an eine rechtswirksame Einwilligung. Der Beitrag von Marie-Theres Tinnefeld analysiert diese Bestimmungen im Kontext der zunehmend europäisch geprägten Menschenrechte.

Der wichtigste Schritt auf dem mühseligen Weg hin zur freien Selbstbestimmung des Menschen beginnt in Europa nach den traumatischen Unrechtserfahrungen am Ende des Zweiten Weltkrieges. Ohne dieses Ende im Jahre 1945 zur Stunde Null stilisieren zu wollen, so stellt jene Erfahrungsgeschichte doch eine Zäsur dar. Hier beginnt die Konstitution Europas – nicht nur Deutschlands – als ein eindeutiges anderes Europa, als ein Europa durch Menschenrechte (Schmale/Tinnefeld 2017: 343).

Gemeint ist eine veränderte Betrachtung des Individuums. Das europäische Recht spricht seitdem jedem Menschen wegen seiner Menschlichkeit eine unantastbare Würde zu, allein weil er lebt und unabhängig von der Frage, wie er lebt, welcher Herkunft oder welchen Geschlechts er ist, ob er alt oder jung, ob er krank oder gesund ist. Auch ein unheilbar Kranker oder „schwieriger" Mensch darf nicht entrechtet werden, wie dies unter den Nationalsozialisten der Fall war. Beispielhaft sei hier nur auf die

Geschichte des 1944 ermordeten Ernst Lossa im Dritten Reich verwiesen.[1] Die Rekonstruktion dieser Geschichte legt die Zielsetzungen der Nationalsozialisten offen, zu denen unter Mitwirkung von Ärzten, Anthropologen und Genetikern eine Politik gehörte, die auf „Rassenreinheit" setzte und zu Euthanasie und staatlich gelenkten Massenmorden führte.

Mit der Anerkennung der Gleichheit aller Menschen vor dem Gesetz im deutschen Grundgesetz (Art. 3 Abs. 1 GG) ist die Aufforderung verbunden, keinen Menschen zu entwürdigen oder verächtlich zu machen (Diskriminierungsverbot, Art. 3 Abs. 3 GG, und Gleichberechtigungsgebot, Art. 3 Abs. 2 S. 1 GG). Eine Rechtsvorstellung, die sich von der Menschenwürde her versteht, gewinnt nur einen übereinstimmenden Sinngehalt in „Gleichheit in der Freiheit" (Fries 1803: 33). Es ist daher grundlegend immer zu fragen, ob personenbezogene Unterschiede rechtlich überhaupt beeinflusst werden können und dürfen. Das Gleichheitsgebot entspricht der verfassungsrechtlichen Garantie von Menschenwürde und individueller Freiheit, die das Bundesverfassungsgericht in der digitalen Informationsgesellschaft immer wieder hervorgehoben hat.

Das Gericht hat schon frühzeitig auf grundrechtliche Schutzlücken reagiert, die durch die automatisierte Verarbeitung personenbezogener Daten in den siebziger Jahren des zwanzigsten Jahrhunderts entstanden sind, und aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m Art. 1 Abs. 1 GG) ein Grundrecht auf informationelle Selbstbestimmung bzw. ein Grundrecht auf Datenschutz geschöpft (BVerfGE 65, 1). Das „neue" Grundrecht basiert auf dem uralten Schutz von Privatheit und Intimität. Das Bundesverfassungsgericht hat den Sinn von Privatheit unter dem Aspekt der räumlichen Privatheit – hier der Wohnung – eindrücklich als Innenraum beschrieben, wo man „sich selbst besitzt" (BVerfGE 27, 1, 6). Der Schutz schließt heute vielfältige Formen des Raumes ein (Tinnefeld 2018: 44, 48 f.).Zu den notwendigen Bedingungen gleicher Freiheit ist zu sagen, dass der Einzelne auf geschützte, abgeschirmte Sphären des privaten Lebens angewiesen ist, die Hannah Arendt „die Dunkelheit des Verborgenen und Geborgenen" nennt (Arendt 1967: 50). Ohne unbeobachtete Freiräume und ohne Zeiten für ein intimes und privates Leben abseits vom „blendend unerbittlichen Licht, das aus der Öffentlichkeit strahlt", gäbe es keine Möglichkeit, eine individuelle Identität zu entwickeln und soziale Kontakte mit der Außenwelt zu knüpfen.

Das Recht auf Privatheit bedarf angesichts der subtilen neuen Technologien, des multifunktionalen Einsatzes von „Big Data" und „Data Analytics", einer Gewährleistung durch höhere datenschutzrechtliche Barrieren. Das Bundesverfassungsgericht betonte in seinem bahnbrechenden Volkszählungsurteil bereits im Jahre 1983: „Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt" (BVerfGE 65, 1, 41). Das heißt auch, dass die informationelle Selbstbestimmung nicht nur eine Grundbedingung für die „individuellen Entfaltungschancen des Einzelnen" ist, sondern auch für seine freien „Handlungs- und Mitwirkungsrechte in einem demokratischen Gemeinwesen" (BVerfGE 65, 1, 43).

Die Orientierung am Individuum als einem „autonomen Willens- und Handlungssubjekt" scheidet die Bereiche von Staatsmacht und Bürgerfreiheit (Denninger 1994: 9). Die eigene Person und ihre Privatheit kennzeichnen den Lebensbereich, in den der Staat nicht oder nur unter einer rechtfertigungsbedürftigen Ausnahme aufgrund eines Gesetzes oder/und der wirksamen Einwilligung einer betroffenen Person eingreifen darf. Das Vorrecht der betroffenen Person, grundsätzlich selbst über die Verwendung ihrer Daten im Wege der Einwilligung zu entscheiden, ist auch gegenüber Privaten von Bedeutung. Angesichts der Möglichkeiten der exzessiven globalen Verbreitung persönlicher Daten kann eine Einwilligung aber nur dann Wirkkraft entfalten, wenn sie an einen bestimmten Zweck gebunden wird. Nur dann kann die betroffene Person die Verarbeitungskonsequenzen überschauen. Dieses Rechtsverständnis entspricht dem supranationalen Unionsrecht.

Europäische Tonlage

Das Recht auf Privatheit (right to privacy) ist vor allem in der Europäischen Menschenrechtskonvention (Art. 8 EMRK) von 1950 verankert und umfasst heute auch das Recht auf Datenschutz. Dieses Recht findet seinen Vorläufer im Recht der Vereinten Nationen, das in der Allgemeinen Erklärung der Menschenrechte (Art. 12 AEMR) von 1948 festhält, dass das Private als „universelles Menschenrecht" zu schützen ist (Guradze 1956: 201 ff.). Das right to privacy wurde später im UN-Zivilpakt[2] von 1966 eigens verbrieft (Art. 17 IPbpR) und von allen Mitgliedern des Europarates unterzeichnet.

Das Recht auf Privatheit und Datenschutz hat Eingang in die EU-Grundrechtecharta gefunden. Die Charta ist zusammen mit dem Vertrag von Lissabon am 1. Dezember 2009 in Kraft getreten und besitzt den gleichen Rang wie diese, sie gehört also zum Primärrecht der Union. Die Charta hat das Menschenrecht auf Privatheit (Art. 7 GRCh) verankert und es explizit um ein Datenschutzgrundrecht (Art. 8 GRCh) ergänzt. Damit wird auf der Unionsebene das historische Menschenrechtsverständnis an den Lebensverhältnissen und -bedingungen im digitalen Zeitalter ausgerichtet: Art. 8 Abs. 2 S. 1 GRCh hält fest, dass personenbezogene Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlichen legitimen Grundlage verarbeitet werden [dürfen]." Das Grundrecht schreibt zudem ein Auskunfts- und Berichtigungsrecht der betroffenen Person über die sie betreffenden Daten fest (Art. 8 Abs. 2 S. 2 GRCh) und statuiert die Überwachung dieser Vorschriften durch eine unabhängige Stelle (Art. 8 Abs. 3 GRCh).

Die Auslegung des Menschen- und Grundrechts auf Privatheit und Datenschutz hat sich von nationalen Verfassungsgerichten auf die höchsten europäischen Gerichte verlagert: den Europäischen Gerichtshof für Menschenrechte (EGMR) in Straßburg und den Europäischen Gerichtshof (EuGH) in Luxemburg. Das Straßburger Gericht stärkt europarechtlich seit langem die Abwehr von unzulässigen oder unverhältnismäßigen staatlichen Informationszugriffen. In den letzten Jahren ist auch der EuGH zunehmend zu einer herausragenden Instanz in Fragen des Grundrechtsschutzes mit dem Schwerpunkt Datenschutz geworden, der gegenüber staatlichem und privatem Eingreifen Wirkkraft entfaltet.[3]

Voraussetzung einer freiwilligen Einwilligung ist eine umfassende Information (Jarass 2016: Art. 8 Rn. 9). Die betroffene Person ist über die jeweiligen Verwendungsabsichten und deren mögliche Konsequenzen zu informieren. Sie muss vor einer Zustimmung, etwa für die Datenverarbeitung bei einer Kreditvergabe durch die Bank, einer Behandlung durch den Arzt oder einer Videoüberwachung durch den Arbeitgeber so aufgeklärt werden, dass sie in der Lage ist, sich von der Bedeutung ihrer Erklärung ein Bild zu machen, um eine Einwilligung ggf. auch verweigern zu können.

Die Forderung nach Autonomie des Einzelnen macht es verständlich, dass im Datenschutzrecht die Einwilligung und ihre für die Datenverarbeitung konstitutive Funktion betont wird. Vor dem Hintergrund praktischer Erfahrungen mit der Einwilligung ist es allerdings fraglich, ob die vorausgesetzte autonome Entscheidung etwa im Bereich des Datenschutzes für Arbeitnehmer oder für Patienten nicht in erster Linie dazu dient, einseitige Regelungen im Interesse des Verantwortlichen für die Datenverarbeitung zu sanktionieren. Ist daher eine Reduktion der Legitimationswirkung der Einverständniserklärung in abhängigen Verhältnissen zugunsten von zwingenden gesetzlichen Vorgaben notwendig? Diese Frage stellt sich auch bei der Einwilligung von Kindern, Jugendlichen oder Schwerkranken. Sind sie einsichtsfähig? Es gibt nicht immer ein klares Ja oder Nein. Hier ist eine Rückbesinnung auf die primäre Funktion der Einwilligung im Datenschutzrecht notwendig. Eine letztlich die betroffene Person völlig übergehende Verarbeitung ihrer persönlichen Daten ist jedenfalls ohne eine Legitimationsgrundlage schrankenlos, so wie dies in der Zeit des Nazi-Regimes der Fall war.

Die Charta bindet die Legitimation der Datenverarbeitung an den „Grundsatz von Treu und Glauben mit Rücksicht auf die vereinbarte Zweckbindung". Anders ausgedrückt: Zweckentfremdungen sind nur zulässig, wenn sie gesetzlich vorgesehen sind oder mit Kenntnis der betroffenen Person und deren Einwilligung erfolgen. Mit der informationellen Selbstbestimmung wäre es unvereinbar, wenn der Zweckbindungsgrundsatz vom Verantwortlichen für die Datenverarbeitung ignoriert oder heruntergespielt würde.

Seit dem Volkszählungsurteil des BVerfG folgt aus der informationellen Selbstbestimmung, dass eine Verarbeitung personenbezogener Daten für die betroffene Person durch die Möglichkeiten von Kontrolle und Korrektur durchsichtig sein muss. Zu den flankierenden prozeduralen Schutzvorschriften gehört daher der Grundsatz der Transparenz sowie auch das Gebot unabhängiger Aufsichtsbehörden. Ziel ist es, die Autonomie des Einzelnen und somit seine Kommunikations- und Partizipationsfähigkeit zu sichern. Eben diese Fähigkeit ist auch erforderlich, um eine demokratische Gesellschaft zu erhalten.

Im Vertrag von Lissabon findet sich eine grundsätzlich umfassende Rechtsetzungskompetenz für das sekundäre Datenschutzrecht (Art. 16 AEUV). Der Unionsgesetzgeber hat auf dieser Grundlage die allgemeine Datenschutz-Grundverordnung (DSGVO) 2016 (VO (EU) 2016/679) verabschiedet. Sie gilt ab 25. Mai 2018 in allen EU-Mitgliedstaaten und löst die bis dahin geltende Datenschutz-Richtlinie (RL 95/46/EG) ab.

Unionsweite Verordnung

Im digitalen Zeitalter sind staatliche Aktivitäten für die betroffene Person ebenso gefährlich wie diejenigen von Privaten, etwa der Konzernriesen Google und Facebook. Die neuen Technologien werden im öffentlichen wie im nicht-öffentlichen Sektor mit dem stets gleichen Ziel angewendet, über die betroffene Person nicht nur alles zu erfahren, sondern auch alltägliche Prozesse durch Big Data und datenauswertende Algorithmen zu steuern. Die Verarbeitungsanlässe mögen im öffentlichen und privaten Bereich verschieden sein. Der Informationswert ist aber auch dann in beiden Bereichen von großem Interesse, wenn die Reaktionen verschieden ausfallen. Für beide gilt „Ordne so lange, bis du Dein Ziel erreicht hast" (Schirrmacher 2011: 191). Erst recht kommt es darauf an, dass die betroffene Person von jedem öffentlichen und nicht-öffentlichen Verantwortlichen für die Datenverarbeitung in verständlicher Form über ihre jeweils verarbeiteten Daten informiert wird und ggf. auch ein Beschwerderecht bei einer zuständigen Aufsichtsbehörde hat. Im Zeichen der digitalen vernetzten Datenverarbeitung ist allerdings eine getrennte Kompetenz der Aufsichtsbehörden nach den Kategorien öffentlicher bzw. nicht-öffentlicher Bereich unhaltbar.

Die DSGVO hat unmittelbare Geltung: Sie will in den Mitgliedstaaten ein gleichmäßig hohes Datenschutzniveau unionsweit gewährleisten und bezieht in ihrem Anwendungsbereich grundsätzlich öffentliche und nicht-öffentlich Verantwortliche ein. Grundvoraussetzungen einer wirksamen Einwilligung sind in der DSGVO in Übereinstimmung mit der Grundrechte-Charta geregelt.

Maßstäbe für die Einwilligung

Es stellt sich die Frage, ob ein selbstbestimmtes Entscheiden angesichts von Vorselektionen durch die digitale Auswertung enormer Datenmengen in der Praxis noch möglich ist. Der ehemalige Bundesverfassungsrichter und ausgewiesene Kenner riskanter Datenverarbeitung, Wolfgang Hoffmann-Riem, der federführend ein IT-Grundrecht[4] initiiert hat, beantwortet diese Frage positiv mit Blick auf die Reformen in der DSGVO (Hoffmann-Riem 2016: 646). Es gilt, die Maßstäbe der Einwilligung zu betrachten, die im Spiegel der Grundrechte-Charta und technischer Gefährdungslagen entstanden sind.

Unter der Verordnung kommt der Einwilligung als Erlaubnistatbestand für eine rechtmäßige Datenverarbeitung weiterhin eine zentrale Rolle zu.[5] Die Verordnung enthält eine Definition der freiwilligen Einwilligung (Art. 4 Nr. 11 DSGVO), die in Art. 7 Abs. 4 DSGVO sowie in den Erwägungsgründen (EG) ausdifferenziert wird. EG 43 macht die Freiheit in der Gleichheit zur Antriebsfeder bei der Beurteilung der Freiwilligkeit. Anders ausgedrückt: Es darf kein Ungleichgewicht zwischen der betroffenen Person und den Verantwortlichen in staatlichen oder privaten Lebensbereichen geben. Damit sich Machtungleichheiten etwa zwischen Arbeitgeber und Arbeitnehmer durch eine „fiktive" Einwilligung nicht verfestigen, kann diese durch eine geschärfte, ggf. auch nationale gesetzliche Regelung in angemessene Bahnen gelenkt werden. Bei einer informationellen Unterlegenheit kann keine freiwillige Entscheidung der betroffenen Person angenommen werden (Spindler 2012: F 99 f.). Sie steht auch nicht im Einklang mit dem Grundsatz von Treu und Glauben (Art. 5 Abs. 1 lit. a DSGVO).

Welche Person kann eine wirksame Einwilligung abgeben?

Voraussetzung ist, dass eine betroffene Person einwilligungsfähig ist. In diesem Kontext muss auch die Handlungskompetenz und Selbstverantwortlichkeit von solchen Personengruppen, die im Dritten Reich rechtlos gestellt waren (Erbkranke, Juden, „Asoziale" u. a.), nach dem Gleichheitsgrundsatz gesehen werden. Es gilt auch einen verantwortungsvollen Umgang mit den Möglichkeiten und Konsequenzen etwa genetischer Diagnostik zu suchen. In seinem 1970 erschienenen Buch „The Patient as Person" fordert Paul Ramsey eine nicht-paternalistische, nicht-direktive Arzt-Patient-Beziehung ein, in der die Entscheidungsfreiheit des Patienten geachtet wird.

Die Verordnung behandelt vor allem die Einwilligungsfähigkeit von Kindern (EG 65). Kinder bedürfen eines besonderen Schutzes, weil sie sich der langfristigen und weitreichenden Folgen ihres Handelns hinsichtlich der Verarbeitung ihrer Daten in der Regel (noch) weniger bewusst sind als Erwachsene (EG 38, 58, 65). Diese Einschätzung findet sich in mehreren Artikeln (Art. 6, 8, 12, 14 und 57) der DSGVO wieder. Die der Einwilligung vorausgehenden Hinweise sollen in einer verständlichen Sprache erfolgen (EG 58), die allerdings häufig in Online-Klauselwerken fehlt, die vielfach schon volljährige Personen nicht verstehen.

Die im deutschen Recht zu findende Unterscheidung von Kindern und Jugendlichen trifft die Verordnung zwar nicht. Sie sieht aber in Bezug auf „Dienste der Informationsgesellschaft" eine Regelgrenze von 16 Jahren vor. Bei Präventions- und Beratungsdiensten, die unmittelbar einem Kind angeboten werden, ist davon auszugehen (EG 38), dass eine Einwilligung des Trägers der elterlichen Verantwortung entbehrlich sein kann bzw. sein muss (Ernst 2017: 111). Die Verordnung legt allerdings eine absolute Untergrenze von 13 Jahren fest, die der Gesetzgeber in den Mitgliedstaaten auf keinen Fall unterschreiten darf.

Wann ist eine selbstbestimmte Einwilligung „freely given" und konkret?

In der Verordnung lautet durchgängig die Vorgabe: Es darf keinen Zwang bei der Abgabe einer Einwilligung geben, jede/r muss so handeln können, wie es ihr/ihm bis zur Todesstunde richtig erscheint (Borasio 2014:116 ff., Will 2018: 18).

Die Freiwilligkeit lässt sich an vielen Kriterien festmachen. Sie knüpft u. a. auch an das aus dem deutschen Recht bekannte Koppelungsverbot an. Danach darf die Erfüllung eines Vertrages nicht von der Verarbeitung personenbezogener Daten abhängig gemacht werden, „die für die Erfüllung eines Vertrages nicht erforderlich sind" (Art. 7 Abs. 4 DSGVO und EG 43). Beispielsweise kann die Koppelung einer Leistung, etwa die des Zugangs zu einem Telemediendienst, nicht mit einer Einwilligung in eine Datennutzung, die dafür nicht zwingend erforderlich ist, verbunden werden. Dies dürfte für die Mehrzahl der Online-Dienstleistungen gelten, die ihre Geschäftsmodelle auf dem Prinzip „Dienstleistungen gegen Daten" aufbauen.

Die Verordnung hält fest, dass die betroffene Person ihre Einwilligung nur „für einen oder mehrere bestimmte Zwecke" geben darf (Art. 6 Abs. 1 lit. a EG 32). Die autonome Zwecksetzung darf keinen pauschalen Charakter haben, darf nicht zur Bedeutungslosigkeit herabsinken. Auch mit Hilfe der Technik darf der Zweck eines Verwendungszusammenhangs nicht determiniert werden, etwa im präventiv-medizinischen Bereich. Je tiefer der Eingriff in das informationelle Selbstbestimmungsrecht ist, desto exakter muss der Zweck der Datennutzung oder -weitergabe angegeben werden, in die eingewilligt werden soll. Demnach ist auch eine Zweckänderung zu nicht kompatiblen Zwecken bei einer Weiterverarbeitung nur unter ganz bestimmten Voraussetzungen möglich (Art. 6 Abs. 4 DSGVO).

Was sind die Voraussetzungen für eine informierte und transparente Einwilligung?

Die betroffene Person muss ihre Einwilligung in „informierter Weise" (Art. 4 Nr. 11 DSGVO) abgeben. Ein „informed consent" liegt nur dann vor, wenn sie zumindest weiß, „wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen" (EG 42 S. 4).

Im Nachlass von Franz Kafka findet sich eine kurze Erzählung mit dem Titel „Zur Frage der Gesetze" (Kafka 2004), in dem der Autor davon spricht, wie quälend es sei, von Gesetzen beherrscht zu werden, die man nicht kennt. Deshalb sollte ein Gesetz jedem zugänglich sein und einfach, klar und verständlich formuliert und publiziert werden. Ähnliches gilt für eine selbstbestimmte Einwilligungserklärung, die Legitimationswirkung erzeugen kann. Die betroffene Person muss daher nicht nur wissen, wer nach der von ihr zu gebenden Einwilligung welche seiner Daten zu welchem Zweck verwenden darf, sondern auch, dass sie ihre Einwilligung für die Zukunft jederzeit widerrufen kann (Art. 7 Abs. 3 S. 1 DSGVO). Die Forderung betrifft insbesondere auch vorformulierte Einwilligungen in Allgemeinen Geschäftsbedingungen (AGB), die nicht nur hervorgehoben, sondern von anderen Sachverhalten klar unterschieden werden müssen (Art. 7 Abs. 2 S. 1 DSGVO). Von einer informierten Einwilligung kann nur gesprochen werden, wenn die Hinweise, die die erforderlichen Fragen erklären sollen, in einer verständlichen Sprache verfasst sind. Anders gesagt: Normen, die juristische Regeln für die Einwilligung und damit für das Zusammenleben der Menschen enthalten, sollten nicht in einer unverständlichen Rechtssprache vorgelegt werden. Wenn ein internationaler Konzern von deutschen Verbrauchern eine wirksame Einwilligung in die Nutzung ihrer Daten erwartet, dann sollte er die Datenschutzhinweise in deren Muttersprache formulieren. Er ist zudem verpflichtet, eine Widerrufsbelehrung anzufügen. Sie ist notwendig, um eine „faire und transparente" Verarbeitung zu gewährleisten (vgl. Art. 13 Abs. 2 lit. c).

In welcher Form ist die Abgabe einer Einwilligung zulässig?

Eine unmissverständliche Einwilligungserklärung (Art. 4 Nr. 11 DSGVO) ist grundsätzlich in jeder Form möglich, auch als elektronisch in Textform abgegebene Erklärung (EG 32). Ebenso ist die mündliche Einwilligung möglich, wegen der Beweislastverteilung aber weniger praktikabel (Art. 7 Abs. 1 DSGVO). Eine Einwilligung kann auch dann vorliegen, wenn die betroffene

Person per Mausklick „ich bin einverstanden“ erklärt (EG 32). Möglich ist auch eine aktive Auswahl technischer Einstellungen bei Diensten der Informationsgesellschaft (EG 31). Schweigen und Untätigkeit sind anders als etwa im römischen Recht keine Erklärung (EG 31). Dasselbe gilt für sogenannte Widerspruchslösungen. Bei einer vorformulierten „fingierten“ Einwilligung, die die betroffene Person etwa per Mail erreicht, muss sie bei Einwänden nicht widersprechen. Verzicht auf den Widerspruch ist keine eindeutige bestätigende Handlung. Gleiches gilt für Opt-out-Kästchen. Ihre Nichtbeachtung erzeugt keine Einwilligung.

Die Frage nach der Formwirksamkeit einer Einwilligung stellt sich auch im Medizinbereich (Buchner 2013: 340). Die Einwilligung des betroffenen Patienten in die ärztliche Verarbeitung seiner Daten muss zwar grundsätzlich nicht in Schriftform erfolgen. Stimmt der Patient damit aber auch wirksam der Weitergabe seiner Daten etwa an eine externe Abrechnungsstelle zu? Die freie Selbstbestimmung des Einzelnen würde bedeutungslos, wenn er sich bestimmten Angeboten und Entscheidungen nicht aktiv entziehen kann bzw. sich nicht dem Maß einer Anwendung zu entziehen weiß.

Ist eine wirksame Einwilligung in die Verarbeitung besonderer (sensitiver) Daten möglich?

Für die Verarbeitung besonderer Kategorien personenbezogener Daten enthält die Verordnung bereichsspezifische Verbote (Art. 9 Abs. 1 DSGVO). Es handelt sich jeweils um gebotene und nunmehr auch im Unionsrecht anerkannte informationelle Diskriminierungsverbote. Eine Einwilligung in die Verarbeitung von Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist nur dann wirksam, wenn die betroffene Person für einen oder für mehrere festgelegte Zwecke ausdrücklich eingewilligt hat (Art. 9 Abs. 2 lit. a DSGVO).

Diese Regelung kommt nicht zur Anwendung, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten das Verarbeitungsverbot durch die Einwilligung der betroffenen Person nicht aufgehoben werden kann (Art. 9 Abs. 2 lit. a DSGVO). Anders ausgedrückt: Die nationalen Gesetzgeber haben bei der Umsetzung der Einwilligungsbestimmung einen Gestaltungsspielraum. Sie können die Einwilligung in die Verarbeitung besonderer Datenkategorien ausschließen oder mit zusätzlichen Bedingungen versehen, etwa für genetische und biometrische sowie für Gesundheitsdaten (s. Art. 9 Abs. 4 DSGVO). Denn biometrische und genetische Daten (Art. 4 Nr. 13 und 14 DSGVO) zeichnen sich dadurch aus, dass sie eine eindeutige Identifikation der betroffenen Person ermöglichen.[6] Wenn Fingerabdrücke oder biometrische Daten zur Gesichtserkennung (EG 53 S. 3) verwendet werden oder Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) Rückschlüsse auf den Gesundheitszustand oder die sexuelle Orientierung einer Person zulassen, dann fallen sie unter die Kategorie und den Schutz sensitiver Daten (Art. 9 Abs. 1 DSGVO). Ausnahmen von dem allgemeinen Verbot der Verarbeitung etwa von Gesundheitsdaten für Forschungszwecke (Art. 9 Abs. 2 lit. j und i DSGVO) sollten speziell im mitgliedstaatlichen Recht oder bei ausdrücklicher Einwilligung der betroffenen Person und bei bestimmten Notwendigkeiten (EG 51) konkretisiert werden.

Perspektiven

Die allgemeine Datenschutz-Grundverordnung hat notwendige Bedingungen gleicher informationeller Selbstbestimmung in der Union geschaffen. Varianten des mitgliedstaatlichen Datenschutzrechts – so auch das am 25. Mai 2018 in Kraft tretende neue Bundesdatenschutzgesetz – dürfen nur in vorgesehenen Fällen von den Vorgaben des Unionsrechts abweichen.

Bei der Berlin-Brandenburgischen Akademie der Wissenschaften findet sich zu einem Projekt der Verständlichkeitsforschung des Rechts folgender Text: „Ein juristischer Text soll verständlich, aber zugleich unmissverständlich sein, zwei Eigenschaften, die leicht im Widerstreit stehen“.[7] Übertragen auf die Anforderungen an eine selbstbestimmte Einwilligung kann demnach betont werden: Das Gemeinte muss nicht nur im Gesetz stehen, sondern sich auch aus einer unmissverständlichen wirksamen Einwilligungserklärung ergeben – und zwar einfach und nicht verklausuliert. Das Recht muss für diejenigen verständlich sein, die nach ihm handeln und leben sollen. Diese Forderung gewinnt im Europäischen Kulturerbejahr 2018 für das Menschenrecht auf Privatheit und Datenschutz als Teil unseres Kulturerbes große Bedeutung: Im Jahre 2018 darf nach der Datenschutzgrund-

Marie-Theres Tinnefeld

Prof. Dr. **Marie-Theres Tinnefeld** ist Juristin und Publizistin, mit zahlreichen Konferenzen und Veröffentlichungen im In- und Ausland zum Thema *Informationsrecht und europäische Rechtskultur*. Sie ist Mitglied im Beirat des FIfF e. V.

Zuletzt ist von ihr erschienen: *Überleben in Freiräumen. 12 Denkstücke* 2018, Verlag Böhlau, Wien/Köln/ Weimar; und Tinnefeld, Marie-Theres/ Buchner, Benedikt/Petri, Thomas/ Hof, Hans-Joachim, *Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht*, 6. Auflage 2017, Verlag de Gruyter, Berlin/ Boston.

verordnung die selbstbestimmte Einwilligung einer betroffenen Person in den einzelnen EU-Mitgliedstaaten nicht mehr unterschiedlich stark oder gering gewährleistet werden.

Der Beitrag erschien in vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftpolitik #211/212 (1/2018). Wir danken Redaktion und Autorin für die freundliche Genehmigung zum Nachdruck.

Referenzen

Arendt, Hannah 1967: Vita activa oder vom Tätigen Leben, München

Buchner, Benedikt 2013: Outsourcing in der Arztpraxis – zwischen Datenschutz und Schweigepflicht, MedR (Zeitschrift für Medizinrecht) S. 337–342

Borasio, Gian Domenico 2014: selbst bestimmt sterben, München

Ernst, Stefan 2017: Die Einwilligung nach der Datenschutzgrundverordnung, ZD (Zeitschrift für Datenschutz), S. 110–114

Fries, Jakob Friedrich 1803: Philosophische Rechtslehre und Kritik aller positiven Gesetzgebung, Jena

Guradze, Heinz 1956: Der Stand der Menschenrechte im Völkerrecht, Göttingen

Hoffmann-Riem, Wolfgang 2016: Innovation und Recht – Recht und Innovation, Frankfurt a. Main

Jarass, Hans D. 2016: GRCh, Charta der Europäischen Grundrechte, Kommentar (3. Auflage), München

Kühling, Jürgen/Buchner, Benedikt 2017: Datenschutz-Grundverordnung, Kommentar, München

Kafka, Franz 2004: Zur Frage der Gesetze und andere Schriften aus dem Nachlass (Taschenbuchausgabe), Frankfurt a. Main

Ramsey, Robert 1970: The Patient as Person, Yale University Press, New Haven

Schirrmacher, Frank 2011: Payback. Warum wir im Informationsalter gezwungen sind zu tun, was wir nicht tun wollen, und wie wir die Kontrolle über unser Denken zurückgewinnen, München

Schmale, Wolfgang/Tinnefeld, Marie-Theres 2017: Europa durch Menschenrechte, in: Datenschutz und Datensicherheit (DuD) Heft 6, S. 343–47

Spindler, Gerold 2012: Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, Gutachten F zum 69. Deutschen Juristentag, F 1 ff.

Tinnefeld, Marie-Theres 2018: Überleben in Freiräumen. 12 Denk-Stücke, Wien/Köln/ Weimar

Tinnefeld et al. 2017: Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht (6. Auflage), Berlin, Boston

Will, Rosemarie 2018: Kein Ende des jahrzehntelangen Rechtsstreites zum Erwerb eines Medikaments zur Selbsttötung in: Grundrechte-Report 2018

Anmerkungen

1 *Mit der Perversion des „Euthanasie"-Systems am Beispiel der Ermordung von „geisteskranken" oder „schwierigen" Kindern durch Aushungern oder tödliche Spritzen von Nazi-Psychiatern befasst sich der Film „Nebel im August" (2016, Regie: Kai Wessel) nach dem gleichnamigen, 2008 erschienenen Buch, in dem Robert Domes das Leben und die Ermordung von Ernst Lossa darstellt, der zum fahrenden Volk der Jenischen gehörte, einer heterogenen Gruppe, die von den Nationalsozialisten als „Zigeuner" bezeichnet wurde.*

2 *Internationaler Pakt über bürgerliche und politische Rechte (IPbpR).*

3 *Tinnefeld, in Tinnefeld et al. 2017: Prolog S. XIX.*

4 *IT-Grundrecht = Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme; s. BVerfG, Urteil des Ersten Senats v. 27. Februar 2008 – 1 BvR 370/07 (=BVerfGE 120, 274 ff.).*

5 *Buchner/Kühling, in Kühling/Buchner 2017: Art. 7 Rn. 5 ff.*

6 *Tinnefeld, in Tinnefeld et al. 2017: 208 ff.*

7 *„Sprache des Rechts. Vermitteln, Verstehen, Verwechseln." Interdisziplinäre Arbeitsgruppe an der BBAW, http://www.bbaw.de/iag/ag_sprache/ueber.html.*

Rainer Rehak

(Meta-) Daten im Zeichen der Sicherheit?

Zum staatlichen Umgang mit vernetzten Datenbeständen

Mit der zunehmenden Digitalisierung hinterlassen die Handlungen von Menschen Metadaten in den jeweiligen Systemen. Sie werden für die kommerzielle Profilerstellung, aber auch für folgenschwere polizeiliche und geheimdienstliche Zwecke ausgewertet. Über diese technikgläubige Herangehensweise muss dringend diskutiert werden.

Seit ihrer Existenz sammeln und speichern staatliche Stellen Informationen über ihre BürgerInnen. Auch die damit eng verbundene Grenze zwischen als notwendig erachteter Verwaltung und weit darüber hinausgehenden Kontrollabsichten ist seit jeher Gegenstand gesellschaftlicher Diskussionen. Seit Jahrzehnten befinden wir uns nun im Prozess einer zunehmenden automatisierten Datenverarbeitung persönlicher, geschäftlicher sowie gesellschaftlicher Interaktionen – inzwischen lapidar *Digitalisierung* genannt. Informationen werden nicht mehr in dunklen Kellern in Form von papierenen Aktenmetern angelegt, aufbewahrt und mühsam manuell durchsucht, sondern können in vernetzen informationstechnischen Systemen erzeugt und verarbeitet werden. Volltextsuche, Mehrfachindexierung, Sortieren, Filtern und effizientes Speichern sind dabei nur noch Fingerübungen der Informatik, die in jedem Informatikbuch über Algorithmen nachzulesen sind.[1] Neuere Methoden drehen sich eher um das Finden von Korrelationen durch statistische Analysen oder das Entdecken ähnlicher Strukturen durch Muster(wieder)erkennung, beispielsweise mit *lernenden* künstlichen neuronalen Netzen (KNN) oder anderen heuristischen – und damit nicht-exakten – Ansätzen. Ist die Datengrundlage vergleichsweise groß und vielfältig, so fällt häufig der unscharfe, aber politisch und wirtschaftlich wirkmächtige Begriff *Big Data*. Wenn es darum geht, die Ergebnisse solcher Herangehensweisen zu interpretieren, stellen sich jedoch weitreichende Fragen: Was sagen beispielsweise Korrelationen über kausale Zusammenhänge aus?

Und was sind *ähnliche* Strukturen? Welche *Muster* können und sollen überhaupt erkannt werden?

Die „digitalisierte Gesellschaft"

Wenn wir über die *digitalisierte Gesellschaft* sprechen, so ist damit häufig gemeint, dass jegliche persönliche Informationsverarbeitung mittels Digitalcomputern geschieht. Wir reichen unsere Steuererklärung digital ein, tragen ein Mobiltelefon bei uns, nutzen digitale Plattformen zum Informationstausch und Warenkauf, verwenden E-Mails und Instant Messenger zur Kommunikation, haben unsere Backups in der ominösen *Cloud* und fragen den *Wahl-O-Mat* nach unseren Wahlpräferenzen. Doch ein Fokus allein auf die individuelle Nutzung greift zu kurz, denn permanent sind wir in staatlichen und wirtschaftlichen Prozessen von digitalen vernetzten Informationssystemen umgeben und Gegenstand ihrer Verarbeitung: von der Abwicklung des Flugverkehrs, den Rentenverwaltungssystemen oder dem zentralen Fahreignungsregister in Flensburg (früher Verkehrszentralregister) über die Polizeiverwaltungs-, Fahndungs- oder Fallbearbeitungssysteme bis hin zu Krankenkassen-Verwaltungsstrukturen, Mautsystemen, den Einwohnermelde- und Finanzämtern, der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa), Unternehmens- sowie Bankensystemen und schließlich dem *Internet der Dinge* oder den Sensorensystemen für das *autonome* Fahren.

Neben vielen interessanten Aspekten dieser allgemeinen Entwicklung, beispielsweise dass eine der weltweit größten Zimmervermietungen gar keine Zimmer besitzt (AirBnB) oder die weltweit größte Enzyklopädie von Freiwilligen befüllt und administriert wird (Wikipedia), gibt es spezielle Eigenschaften aktueller digitaler Systeme. Hier fallen nicht nur die direkt verarbeiteten Daten an wie beispielsweise die eigentlichen Kommunikationsinhalte, die abgegebene Steuererklärung, die Schlafrhythmusdaten von Fitness-Apps, die Rechnungen in PDF-Form, die *gekauften* (bzw. tatsächlich nur lizenzierten) E-Books und andere Medieninhalte, sondern auch eine ganze Menge der viel zitierten *Metadaten* an. Metadaten sind Daten, die die Umstände der Datenverarbeitung beschreiben, wie etwa BesitzerIn und Erstellungszeitpunkt eines Dokumentes, die involvierten Sender- und Empfängernummern eines Telefongesprächs bzw. Nachrichtenaustauschs, die aufgerufenen Unterseiten einer Webseite und deren Ansichtsdauer, der aktuell verbundene Funkmast von Mobiltelefonen, die IP-Adresse von WebseitenbesucherInnen oder die genauen Nutzungszeiten von Kommunikationsdiensten. Diese Metadaten entstehen zwar nicht notwendigerweise, aber die meisten Systeme sind so gebaut, dass nahezu alle Aktivitäten festgehalten – geloggt – werden. Dafür gibt es teilweise technische Gründe, eine effektivere Fehlersuche oder schnellere Angriffserkennung, aber es überwiegen tatsächlich eher kommerzielle Gründe, beispielsweise Abrechnungsprozesse oder die Möglichkeit einer detaillierten Benutzerprofilerstellung ebenso wie zum A/B-Testen von Alternativinhalten.

Das Konzept *Metadaten* ist zwar nicht neu, aber ein Eingangsstempel auf einem papierenen Brief lässt sich nicht so automatisiert und massenhaft auswerten wie die Digitalversion. Hinzu kommt der Umstand, dass mit den aktuellen Hardwarekosten und Softwaredesigns das Behalten und Speichern von Daten und Metadaten viel billiger und weniger aufwändig ist als das Löschen, weil Daten beispielsweise auch aufeinander verweisen und so auch in andere Kontexte hinein verknüpft sind.

Daten oder Metadaten

Gerade in der Politik wird immer noch oft die Ansicht vertreten, Metadaten seien weniger aussagekräftig und daher weniger schützenswert als Inhaltsdaten. Doch offenbaren beispielsweise Metadaten von Kommunikationsvorgängen – die sogenannten Verkehrsdaten – den kompletten sozialen Graphen. Der zeigt, wer von wo mit wem und wann kommuniziert. Daraus lässt sich direkt ableiten, welche Gruppen und Zusammenhänge es gibt und wer die zentralen, vernetzten Personen sind. Aus den Kommunikationszeiten wiederum lässt sich in der Regel auch die Art der Beziehung ablesen – beruflich oder privat, lose oder intim, stabil oder dynamisch. Anrufe bei Anwaltskanzleien für Arbeitsrecht, HIV-Hilfestellen, psychologischen Praxen, Escort-Services oder Familienplanungszentren brauchen kaum weitere Inhaltsdaten, um für sich bereits aussagekräftig zu sein. Darüber hinaus lassen sich Metadaten auch mit anderen Informationen verknüpfen, und so offenbaren die Ortsdaten nicht nur Essensgewohnheiten (in Verknüpfung mit Restaurant-Listen) oder Gesundheitszustand (Arzt- oder Krankenhausverzeichnisse), sondern auch komplette Verhaltensprofile.[2] Denn würden die Metadaten (hier konkret Orts- und Zeitangaben) einer hypothetischen Vorratsdatenspeicherung[3] beispielsweise mit Informationen zu angemeldeten Demonstrationen oder anderen politischen Aktionen verknüpft, so erhielte etwa eine Behörde komfortabel nahezu vollständige Anwesenheitslisten dieser Veranstaltungen. Metadaten sind also ebenso aussagekräftig wie Inhaltsdaten, sie müssen nur anders ausgewertet werden. Auch deswegen schützt Artikel 10 des Grundgesetzes nicht nur die Kommunikation, sondern auch deren Umstände, wie die zugehörigen Metadaten. Die digitalen Spuren all unserer Handlungen liegen also entweder direkt von uns produziert (beispielsweise Kommunikationsdaten) oder indirekt erzeugt (Kunden-, Steuer-, Maut-, Kranken- oder Rentendaten) vor. Einzig rechtliche Einhegungen sorgen dafür, dass nicht einfach alle Daten zusammengeführt werden, um ein umfassendes digitales Abbild der menschlichen Welt zu erschaffen.[4] Im Allgemeinen gilt im europäischen Datenschutzrecht daher ein sogenanntes Erhebungsverbot mit Erlaubnisvorbehalt für die Verarbeitung personenbezogener Daten, demzufolge grundsätzlich nichts gespeichert werden darf, es sei denn es gibt explizite Gründe für eine Erhebung, z. B. eine informierte Einwilligung.[5]

Polizeidateien

In Deutschland legen Polizeien eigene Datenbanken über Personen an, die sie als relevant erachten. Diese sogenannten *Dateien* benötigen je nach Bundesland manchmal eine Errichtungsanordnung, für den Bund jedoch immer.[6] Sie definieren den Zweck, den betroffenen Personenkreis, Datenquellen, Regeln der Datenübermittlung an andere Stellen oder Höchstspeicher- und Prüffristen. In Berlin muss beispielsweise bei jeder neuen *Datei* der Berliner Beauftragte für Datenschutz und Informationsfreiheit unterrichtet werden, in Hamburg nur dann, wenn die Errichtung mit „besonderen [...] Problemen" verbunden ist.[7]

Eine solche Regelung aber sorgt bisweilen für merkwürdige Situationen, wie in Hamburg im Jahre 2014, wo das dortige Landeskriminalamt (LKA) eine Transparenzgesetz-Anfrage bezüglich der Existenz einer Sportgewalt-Datei verneinte. Dies entsprach „bedauerlicherweise" schon neun Jahre lang nicht mehr der Wahrheit, wie sich später herausstellte.[8] Die verschiedenen Polizeien erstellen so also jeweils eigene Dateien mit jeweils eigenen Formaten, für die jeweils die eigenen Landesinnenressorts verantwortlich sind. Dieses Unorganisiertheit ist im Sinne der vertikalen Gewaltenteilung beabsichtigt und wirkt gewissermaßen machtbeschränkend.

Interessant wird es dann, wenn federführend durch das Bundesministerium des Innern (BMI) und praktisch ausgeführt vom Bundeskriminalamt (BKA) Dateien bundesweit angelegt werden, die *INPOL-Verbunddateien*. Auch sie sind zweckgebunden und sollen Angaben zu den als interessant angesehenen Personen enthalten. Befüllt bzw. verwendet werden diese rund 150 Verbunddateien aber von den Landes- und Bundesbehörden gemeinsam, teilweise auch von Geheimdiensten. Das Konzept der Verbunddateien ist immer wieder Gegenstand von Kritik.[9] In einem prominenten Fall ging es um Teilnehmende einer Anti-Atom-Demonstration, deren Namen vor zwei Jahren vom Verfassungsschutz – laut BMI zu Recht – in eine gemeinsam mit dem BKA genutzte Projektdatei aufgenommen worden sind, mit der Begründung, Kernkraftkritik sei ja Systemkritik.[10] Für das BKA war eine so willkürlich gefüllte Datei jedoch praktisch nutzlos.

Ein weiteres Beispiel war die „Zentraldatei politisch-motivierte Kriminalität, links" (PMK-links Z), die im Jahre 2012 durch den damaligen Bundesdatenschutzbeauftragten Peter Schaar analysiert wurde. Im Gegensatz zu gemeinsamen Verbunddateien kann bei Zentraldateien nur das BKA schreibend zugreifen, es muss also selbst die Einträge prüfen. Schaar hatte dabei so viele Rechtsverstöße festgestellt, dass das BKA ca. 90 Prozent der Einträge löschen musste.[11] Die absolute Mehrheit der gespeicherten Personen waren also illegal in staatlichen Datenbanken gelandet, von deren Existenz sie nichts wussten und deren Auswirkungen auf etwaige Zuverlässigkeits-Überprüfungen komplett unklar waren. Die Konsequenzen einer solchen Speicherungspraxis zeigen sich besonders im Falle einer Rasterfahndung[12], denn der Abgleich mit einer Datei, die fast ausschließlich fälschlich gespeicherte Personendaten enthält, kann für die Betroffenen verheerende Folgen haben – für die eigentlich Gesuchten wiederum ist eine solche Praxis sehr von Vorteil. Hier offenbart sich das generelle Problem gemeinsam genutzter Datenbestände: Informationen werden von einem Akteur in einem Kontext mit einer bestimmte Absicht erhoben und dann – dekontextualisiert – als Daten gespeichert. Mit der Nutzung durch andere Akteure werden sie dann – meist ganz anders – rekontextualisiert. Dass aber die Kontexte der Erhebung und die der Nutzung zusammenpassen, muss akribisch sichergestellt werden, insbesondere wenn es sich bei den Akteuren um staatliche Stellen mit großer und/oder verdeckter Wirkmacht handelt. Die Konsequenzen einer solchen unzureichender Datenhaltung sind auch kürzlich wieder prominent zutage getreten. Die verweigerten 32 Akkreditierungen für JournalistInnen beim G20-Gipfel in Hamburg lassen sich mehrheitlich[13] auf falsche, nicht-aktualisierte oder schlicht illegal gespeicherte Daten solcher Verbunddateien zurückführen. Dabei haben die wenigsten Opfer solcher Datenpraktiken das Glück, in diesen publikumswirksamen Berufsfeldern zu arbeiten.

Die Liste derartig überbordernder Datenbanknutzung und falscher Einträge lässt sich nach wie vor millionenfach fortsetzen, sodass in den Medien nun von der „Spitze des Eisbergs" gesprochen wird[14] und BKA-Präsident Holger Münch sich an Generalrevisionsforderungen abarbeiten muss[15], während seine Kolleginnen und Kollegen in guter Verfassungsschutzmanier die Beweise des eigenen organisationalen Fehlverhaltens vernichten.[16]

Existenz fragwürdig, Prozesse intransparent, Daten veraltet

Es zeichnet sich ab, dass die schlechte Performanz solcher Datenbanken nicht die Ausnahme sondern die Regel darstellt. Eine sinnvolle Nutzung wäre rein theoretisch nur möglich durch mehr Qualitätssicherungspersonal, detailliertere Dateneingangsprüfungen, strikte Eintragsverbote beispielsweise für Personen mit Freisprüchen, kontextbeschreibende Annotationen der Daten, sinngebende Verweise auf Akten, Verfahren oder Hintergründe und regelmäßige, aufwändige Datenpflege inklusive restriktiver Löschfristen. Denn Daten veralten, verändern sich, müssen korrigiert oder gelöscht werden. Sollte das jedoch mit den vorhandenen Mitteln gar nicht möglich sein, so müssen Nutzen und Erforderlichkeit solcher Dateien generell infrage gestellt werden. Bei einer ständig unterbesetzten Polizei, die schon jetzt viele konventionelle Spuren kaum verfolgen kann, sind derartig komplex zu betreibende, löchrige, veraltete, illegale Datenbestände sogar schädlich. „Ganz klar: Unnötig gespeicherte Daten schaffen nicht mehr, sondern weniger Sicherheit", befand überraschend auch Justizminister Heiko Maas (SPD) im Kontext des G20-Akkreditierungsdebakels.[17] Ebenso klagen BKA-interne Analysten über zu viele irrelevante Daten in den Verbunddateien; insbesondere dort, wo Geheimdienste mit im Boot sind, da diese immer auf mehr Informationen aus sind, unabhängig davon, ob sie sich sauber überprüfen lassen.[18]

Lange Zeit, so scheint es, war die Nutzung solcher Dateien politisch gewollt. Auch diese Entwicklung muss im Kontext der Vernetzung und Digitalisierung sowie ihrer hehren Verheißungen verstanden werden: Auch hier spielen Technikgläubigkeit und mechanistische Weltbilder eine wesentliche Rolle, denn oft herrscht bezüglich der Kriminalitäts- und Terrorbekämpfung die Vorstellung einer Suche nach der „Nadel im Heuhaufen", wofür ja zuerst der ganze Heuhaufen benötigt würde.[19] In Deutschland werden bislang keine Big-Data-Analysen auf Basis polizeilicher Dateien durchgeführt und Datenbestände mit verschiedenen Zwecken (etwa des Staatsschutzes, der Bekämpfung der Organisierten oder der Wirtschaftskriminalität) dürfen auch nicht verkettet werden. Trotzdem sehen viele Personen in politischen Führungspositionen eine verheißungsvolle Zukunft in der Abkehr vom restriktiven Datenschutz hin zum Datenreichtum als Lösungsansatz für wirtschaftliche, ökologische oder polizeiliche Aufgabenstellungen.[20] Dieser Denkweise sind Trennungsgebot, Verkettungsverbot bzw. Zweckbindung ein Dorn im Auge.

Wilde Erfahrungen mit (Meta-) Daten

Was mit den angesammelten Daten passiert, wenn es zu wenige der oben beschriebenen Beschränkungen gibt, sehen wir beispielsweise in China, wo gerade ein *Sozialkredit*-Punktestand aller BürgerInnen aufgebaut wird. In dieser Datenbank wird gespei-

chert, wer bei Rot über die Ampel geht, wer Rechnungen nicht bezahlt oder wer sich kritisch über die Regierung äußert.[21] Ein anderes Beispiel ist die die verhängnisvolle Metadatennutzung für Drohnentötungen des US-Militärs in Pakistan oder Jemen. Auch der deutsche Bundesnachrichtendienst (BND) hat dafür Kommunikations-Metadaten sowie Stammdaten wie zugehörige Namen und Adressen beigesteuert.[22] Für solche Drohnenangriffe werden dann konkret nicht bekannte Personen anvisiert, weil bestimmte Muster passen. Bei diesen „signature strikes"[23] werden Eigenschaften und Zusammenhänge definiert, etwa regelmäßige Aufenthalte an bestimmten Orten, Telefonanrufe oder ähnliche Bewegungsmuster, wie sie andere, bereits bekannte Personen aufweisen. Diese Art von Datenverknüpfung wird allein mit Metadaten möglich, mit tödlichen Folgen für die Getroffenen.

Es gibt jedoch auch ganz andere Verwendungen von Metadaten, die keine komplexen Modelle brauchen, wie etwa die geheime Sammlung von Kompromat gegen „Gefährder" durch den US-amerikanischen Geheimdienst NSA zeigt. In einem der Fälle wurden massenhaft völlig legale, aber sozial brisante Webseitenzugriffe auf Pornographiewebseiten auf Vorrat gespeichert. Die damit erlangten Erotikvorlieben der Nutzer sollten dann verwendet werden, um die Zielpersonen bei Bedarf zu erpressen. In anderen Fällen wurden einfach alle BesucherInnen von Webseiten wie WikiLeaks (Enthüllungsplattform), TheTorProjekt.org (Anonymisierungssoftware) oder PirateBay (File-Sharing-Seite) auf Vorrat dokumentiert, vermutlich für eine spätere noch zu definierende Verwendung.[24] Hier wird erkennbar, welche Wirkung Metadaten entfalten können. Ähnlich datengetriebene Herangehensweisen sind bei der „prädiktiven Polizeiarbeit" in Teilen der USA erkennbar, bei der jedem Menschen mittlerweile *Gefahrenbewertungen* zugewiesen werden. Dieser *Gefährder-Score* berechnet sich nach den Datenmodellen der Hersteller, die zum Schutz von Betriebsgeheimnissen leider nicht nachvollzogen werden können.[25] Nur soviel ist bislang bekannt: Persönliche Daten aus Social-Media-Plattformen spielen genauso eine Rolle wie – bemerkenswert – der Kontakt zu Gewaltopfern.[26]

Gerade in Bezug auf Kommunikationsdaten ist auch in Deutschland eine starke Tendenz zur Datenanhäufung und -nutzung erkennbar. Die Zahlen von ermittlungsbezogenen Funkzellenabfragen nach Strafprozessordnung (StPO) nehmen stark zu, wobei großflächig und regelmäßig auf die vorhandenen Metadaten der Vorratsdatenspeicherung zurückgegriffen wird[27], ebenso wie die Nutzung von metadatenerzeugenden *Stillen SMS*. Interessant in diesem Zusammenhang: Im Jahre 2015 wurde die Firma Rola Security – Anbieter für polizeiliche Fallbearbeitungssoftware mit Überwachungsschnittstellen – von der Telekom gekauft.[28] Damit konnte die Telekom in Bezug auf Telekommunikationsüberwachung alles bequem aus einer Hand liefern.

Bei allen Anwendungsfällen fällt auf, dass die Betroffenen keine oder nur geringe Einfluss- und Beschwerdemacht haben, weil die Aktivitäten geheim ablaufen, weil ein späterer Widerspruch sinnlos wäre oder alles zusammen.

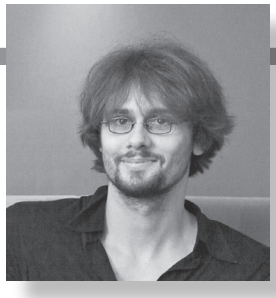
Big Data, künstliche Intelligenz und Technikgläubigkeit

Ganz allgemein gesprochen ist offensichtlich gerade staatlichen Akteuren weder bewusst, was automatisierte Datenauswertung kann bzw. nicht kann, noch was die Voraussetzungen dafür sind oder wie verheerend die Auswirkungen für die Betroffenen sein können.

Für die automatisierte Datenauswertung muss immer klar sein, was die gesuchten Zusammenhänge ausmacht, worin sie also genau bestehen. Mit den traditionellen informatischen Mitteln wie Suchen, Filtern, Sortieren sind immer auch formale Beschreibungen des Gesuchten notwendig. Es ist eben nicht möglich, Algorithmen auf eine Datensammlung anzusetzen und einfach nach *Terroristen* oder *Gefährdern* suchen zu lassen, denn wir haben bislang nicht einmal eine nicht-formale, allgemein anerkannte Definition von *Terrorismus* oder *Gefährderverhalten*. Wonach suchen wir also? Und gerade bei neuen Analyse- und Auswertungsmethoden mit bislang unklarer Wirkungsweise wie künstlichen neuralen Netzen muss genau abgewogen werden, was die Konsequenzen von Fehlanalysen sind, um den möglichen Nutzen damit abzugleichen.

Wenn beispielsweise der Google-Bilderkennungsalgorithmus ein Bild falsch klassifiziert, Amazon ein unpassendes Buch empfiehlt oder AlphaGo vielleicht auch einmal eine Partie verliert[29], ist die Konsequenz doch ungleich erträglicher als wenn fehlerhafte Rückfallvorhersagesoftware bei Gerichtsprozessen überwiegend Menschen dunkler Hautfarbe hinter Gitter bringt, JournalistInnen ihre Arbeit nicht mehr ausüben können, Menschen ihre politischen Aktivitäten einschränken, um keine verhängnisvollen Spuren mehr zu hinterlassen oder afghanische Bauersleute sterben, weil sie am falschen Ort Hochzeit gefeiert haben. Über diese Auswirkungen automatisierter Datenverarbeitung müssen wir dringend diskutieren, bevor wir eine Gesellschaft in – wenn auch manchmal nur ungewollt – ungerechte Technik gießen. Gerade auch Technikerinnen und Techniker müssen sich hier politisch zu Möglichkeiten und vor allem Grenzen von informationstechnischen Herangehensweisen äußern; oder um es sinngemäß mit dem Computerpionier und Gesellschaftskritiker Prof. Dr. Joseph Weizenbaum zu sagen: „Früher übergab man ein Problem dem Computer, wenn man es verstanden hatte. Heute ist es zunehmend anders herum." Diese Entwicklung gilt es zu stoppen.

Rainer Rehak



Rainer Rehak beschäftigt sich seit rund zehn Jahren mit dem Themenfeld *Informatik und Gesellschaft*. Er studierte Informatik und Philosophie in Berlin, Hong Kong und Peking. Während des Studiums arbeitete er am Lehrstuhl für I*nformatik in Bildung und Gesellschaft* von Wolfgang Coy. Aktuell promoviert er am Weizenbaum-Institut für die vernetzte Gesellschaft und lehrt in den Bereichen Datenschutz/Datensicherheit, sowie Informatik und Gesellschaft.

Dieser Text erschien zuvor in gekürzter Fassung in der Civil Liberties and Police (CILIP) 114 des Instituts für Bürgerrechte & öffentliche Sicherheit unter dem Titel „Die Datenschatten". Vielen Dank auch an Matthias Monroy und Heiner Busch für ihr wertvolles Feedback.

Anmerkungen

1 *Siehe z. B. Cormen, Leiserson und Rivest: Algorithmen – Eine Einführung, De Gruyter Oldenbourg, 2013*
2 *zeit.de v. 24.2.2011, http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz*
3 *Siehe die damaligen Pläne für das Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten.*
4 *Vergleiche dazu die Situation in China: Deutschlandfunk-Kultur, Weltzeit v. 5.9.2017, http://www.deutschlandfunkkultur.de/chinas-sozialkredit-system-auf-dem-weg-in-die-it-diktatur.979.de.html?dram%3Aarticle_id=395126*
5 *Siehe das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983, http://www.servat.unibe.ch/dfr/bv065001.html*
6 *Siehe § 34 BKA-Gesetz, § 490 Strafprozessordnung (StPO) oder § 49 ASOG Berlin*
7 *§ 26 Gesetz über die polizeiliche Datenverarbeitung Hamburg*
8 *Netzpolitik.org v. 17.1.2016, https://netzpolitik.org/2016/hamburger-polizei-fuehrt-geheime-datei-zur-sportgewalt-beluegt-buerger/*
9 *Zeit.de v. 24.9.2014, http://www.zeit.de/politik/deutschland/2014-09/bundeskriminalamt-daten-buerger-straftaeter*
10 *Deutschlandradio: Informationen am Morgen v. 2.9.2017, http://srv.deutschlandradio.de/themes/dradio/script/aod/index.html?audioMode=3&audioID=573924*
11 *Netzpolitik.org v. 14.4., 27.4 und 19.6.2015, https://netzpolitik.org/2015/bka-datenbank-bundesdatenschutzbeauftragter-fand-gravierenden-verstoss-gegen-datenschutzrechtliche-vorschriften/, https://netzpolitik.org/2015/innenministerium-bestaetigt-rechtswidrige-speicherung-linker-aktivistinnen/, https://netzpolitik.org/2015/nachhilfe-der-bundesdatenschutzbeauftragten-fuehrt-zu-90-schwund-in-polizeidatenbank-zu-linkem-aktivismus/*
12 *Beispielsweise § 98a StPO, § 47 ASOG (Berlin) oder § 28 BKAG*
13 *Tagesschau v. 3.10.2017, https://www.tagesschau.de/inland/g20-akkreditierungen-107.html*
14 *Tagesschau v. 30.08.2017, https://www.tagesschau.de/inland/gzwanzig-datenschuetzer-101.html*
15 *Tagesspiegel v. 1.9.2017, https://www.tagesspiegel.de/politik/kriminalitaetsdatenbanken-bka-praesident-wehrt-sich-gegen-speichervorwuerfe/20273314.html*
16 *Tagesschau v. 3.10.2017, https://www.tagesschau.de/inland/g20-akkreditierungen-107.html*
17 *Zeit.de v. 30.8.2017, http://www.zeit.de/gesellschaft/zeitgeschehen/2017-08/datenschutz-datenspeicherung-bka-heiko-maas-rechtswidrig-aufklaerung*
18 *Deutschlandradio, Informationen am Morgen v. 2.9.2017, http://srv.deutschlandradio.de/themes/dradio/script/aod/index.html?audioMode=3&audioID=573924*
19 *Guardian v. 10.10.2013, https://www.theguardian.com/commentisfree/2013/oct/10/double-danger-nsa-surveillance*
20 *Beschreibung der datengetriebenen Hoffnung in der Politik: Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Pressemitteilung v. 21.12.2016, https://www.fiff.de/presse/pressemitteilungen/digitalcharta-notwendige-politische-initiative-trotz-grober-fehler-fiff-sichert-mithilfe-zu*
21 *Deutschlandfunk-Kultur, Weltzeit v. 5.9.2017, http://www.deutschlandfunkkultur.de/chinas-sozialkredit-system-auf-dem-weg-in-die-it-diktatur.979.de.html?dram%3Aarticle_id=395126*
22 *zeit.de v. 15.10.2015, http://www.zeit.de/politik/2015-10/nsa-affaere-untersuchungsausschuss-metadaten-brandon-bryant-aussage/komplettansicht*
23 *zeit.de v. 16.10.2015, http://www.zeit.de/politik/ausland/2015-10/usa-drohnen-drohnenkrieg-rechtfertigung/komplettansicht*
24 *Netzpolitik.org v. 3.7.2014, https://netzpolitik.org/2014/nsa-ueberwacht-tor-infrastruktur-und-alle-nutzer-auch-betreiber-in-deutschland/ und Theintercept.com v. 18.2.2014, https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/*
25 *Siehe dazu auch die rassistische Rückfall-Vorhersagesoftware https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing*
26 *Netzpolitik.org v. 6.10.2017, https://netzpolitik.org/2017/pre-crime-ueber-menschen-die-ungewollt-teil-von-datenexperimenten-sind/*
27 *Netzpolitik.org v. 23.5.2017, https://netzpolitik.org/2017/funkzellenabfrage-letztes-jahr-landeten-handy-daten-aller-berliner-alle-elf-tage-bei-der-polizei/*
28 *sueddeutsche.de v. 6.7.2015, http://www.sueddeutsche.de/wirtschaft/angst-vor-ueberwachung-die-hilfssheriffs-der-telekom-1.2551588*
29 *heise.de v. 5.1.2017, https://www.heise.de/newsticker/meldung/Googles-KI-AlphaGo-gewinnt-und-gewinnt-3589295.html*

Markus Reinisch

Vermessen, berechnen und vorhersagen

Zahlengläubigkeit und positivistisches Grundverständnis von *Big Data*

Algorithmen *und* Deep Learning, kognitive Roboter, intelligente *Maschinen, vernetzte* Smart *Things (Internet der Dinge) sind nur einige der derzeit diskutierten Schlagworte, wenn es um die technische, insbesondere digitale Beschleunigung geht. Und es kommen laufend neue Schlagworte hinzu. Sie gehen einher mit der kontroversen Big-Data-Debatte, die nicht mehr nur in den Fachwissenschaften und Feuilletons geführt wird. Während Technologie-Euphoriker in Big Data und der zunehmenden* Datafizierung *von Lebensbereichen eine revolutionäre Art des Erkenntnisgewinns, von Vorhersagemethode und Effizienzsteigerung sehen, werden immer mehr kritische Stimmen laut. Vor allem solche, die sich gegen die fortschreitende Ausrichtung am Vermessen und damit am Quantitativen richten. Es wird heute in vielen Lebensbereichen eine unüberschaubare Menge an Daten erfasst, analysiert und tabellarisiert, um passgenaue Vorhersagen zu erreichen, beispielsweise für menschliches Verhalten. Hinter der Zahlengläubigkeit steckt jedoch eine positivistische Weltsicht, die alles auszuklammern scheint, was nicht mess- und formalisierbar ist. Dass dies nicht ohne gesellschaftliche, politische, ethische und bildungstheoretische Folgen bleiben wird, soll dieser Beitrag zeigen.*

Datafizierung und Zahlengläubigkeit: „… und dann funktionieren die Kontrollen."

„Was man nicht messen kann, kann man nicht managen", hieß es in der November-Ausgabe 2012 des Harvard-Business-Manager-Magazins. Nur kurze Zeit später prägten zwei Pioniere der Big-Data-Forschung, Viktor Mayer-Schönberger und Kenneth Cukier, den Begriff der Datafizierung, bei dem es darum geht, „ein Phänomen […] in ein Format zu bringen, sodass es zahlenmäßig erfasst und analysiert werden kann."[1] Mithilfe geeigneter Verfahren zur Erhebung großer Datenmengen und deren Auswertung sollen demnach immer mehr Lebensbereiche mathematisch vermessen und formalisiert werden. Dabei wird geflissentlich übersehen, „dass sich die Gesellschaft als Ganzes nicht allein mit mathematischen Methoden erfassen lässt."[2] Letztlich handelt es nicht nur um relativ wertfreie Bereiche wie den Wetterbericht, es soll auch das Verhalten von Menschen möglichst genau vorhergesagt werden, wenn man einmal genug Datenmaterial hat. Dass irgendwann auch abstrakte Phänomene wie Gefühle, Stimmungen und Kommunikation datafiziert werden können, daran lassen Mayer/Cukier keinen Zweifel: am Ende stehe „the datafication of everything".[3]

„Schluss mit dem subjektiven *Körpergefühl* – jetzt haben wir unsere Körperdaten", schrieb Dietrich Meyer-Ebrecht provokativ vor etwas mehr als zwei Jahren in dieser Zeitschrift.[4] Die Bedeutung des Zähl-, Mess- und Auswertbaren sowie die Software- und Zahlengläubigkeit sind seither enorm gewachsen. In einer auf Leistung und (Selbst-) Optimierung getrimmten Gesellschaft sind Technologien für das Messen hinsichtlich Selbstbeobachtung, -dokumentation, -bewertung wichtige Werkzeuge. Griffige englische Vokabeln wie *Lifelogging, Quantified Self* oder *Self-Tracking* stehen für die Erfassung von Daten rund um den eigenen Körper. Sie sind einerseits mediale Aspekte des „unternehmerischen Selbst" (Ulrich Bröckling) und stehen andererseits im größeren Kontext von Big Data. Es verwundert kaum, dass mit all diesen neoliberalen alltäglichen Datenpraktiken und der zunehmenden „problematischen Fetischisierung des Quantitativen"[5] die Überwachung und algorithmische Kontrolle über uns vorangetrieben wird. Die Diskussionen um *Digital Humanities* beispielsweise sind Ausdruck dieser Entwicklungen im Bereich der Geisteswissenschaften. Es ist auch die logische Fortentwicklung des *Web 2.0*. Was im *partizipativen Netz* mit der zunehmenden Preisgabe von relevanten Daten, der Personalisierung und Profilerstellung begann, erfährt in Big-Data-Anwendungen seine logische Fortsetzung. „Wir entblößen uns unbekümmert weiter", ist bei Yvonne Hofstetter zu lesen. Der renommierte Soziologe Zygmunt Bauman spricht vom selbstversichernden „Ich werde gesehen (beobachtet, bemerkt, erfasst), also bin ich." Die preisgegebenen Informationen über persönliche Verhaltensmuster werden dabei via Big-Data-Analyse zu Humankapital für Daten sammelnde Großkonzerne. Adrian Lobe bringt die Determinierbarkeit des Menschen in dieser Hinsicht auf den Punkt:

> *„Die Tech-Giganten sind von der Idee beseelt, den Menschen formbar zu machen wie ein Bauwerk. Der Informationskapitalismus ist eine Welt des In-den-Kopf-Eindringens geworden. Es geht darum, unsere Präferenzen so zu steuern, dass sie für ökonomische Ziele dienstbar gemacht werden können."*[6]

Oder, wie es Friedrich Kittler bereits 1995 im Gespräch mit Paul Virilio darlegte: „Wir werden alle kontrolliert auf unseren Maschinen", und wenn das große Geld im Spiel ist, „dann funktionieren die Kontrollen."

Korrelationen, Wahrscheinlichkeiten, Algorithmen, Positivismus – und die Ethik?

Bei *Big Data* wird nach Mustern gesucht: Algorithmen errechnen bislang unbekannte *Korrelationen* aus großen Datenmengen. Der Blick auf Ursache und Wirkung, das Arbeiten mit Theorien und Modellen habe demnach hingegen ausgedient, wie es der Chef des Technologie-Magazins *Wired,* Chris Anderson, 2008 bereits andeutete. Sein Text „Das Ende der Theorie. Die Datenschwemme macht wissenschaftliche Methoden obsolet", wurde vor allem von sozial- und kulturwissenschaftlicher Seite scharf kritisiert. Mit der Ausrichtung an Zahlen, quantitativen Auswertungen und probabilistischen Vorhersagen wird nicht mehr eine Theorie leitend, sondern Statistiken. Diese werden sodann übersichtlich visualisiert und suggerieren im Zuge von Big-Data-Analysen, die Welt würde objektiv, verlustfrei und damit verlässlich 1:1 abgebildet. Ein solcher Positivismus meint, eine Reduktion von Komplexität und Unsicherheiten durch eine Erhöhung von Wahrscheinlichkeit zu erreichen? Sich ausrichten am probabilistischen Wesen unserer Welt, wie es Mayer-Schönberger und Cukier als Big-Data-Grundsatz fordern? Mit welcher Begründung? Schließlich steckt dahinter eine Weltanschauung, die auch ethisch erklären müsste, warum Wahrscheinlichkeiten unsere Lebenswelten bestimmen sollten.

Die Forderungen, *selbstlernende* Algorithmen irgendwann mit den Fähigkeiten menschlicher Kognition gleichzusetzen und die Forschung an *Deep Learning* voranzubringen, scheinen im Big-Data-Diskurs eine größere Rolle zu spielen als medienethische Fragen wie zum Beispiel: Welche Institutionen, Behörden und Privatpersonen dürfen auf Ergebnisse von Big-Data-Analysen wann und in welchem Umfang zugreifen? Was wird in welchen Lebensbereichen damit entschieden sowie gesteuert, und wer sieht welche Erkenntnisse für wen als relevant an? Kann den Algorithmen im Spannungsverhältnis von Berechenbarkeit (*computability*) und Entscheidbarkeit (*decisionability*) eine autonome Handlungsbefugnis (*agency*) mit besonderen Kompetenzen zugesprochen werden (*Automated Decision Making*, ADM)? Lässt sich überhaupt eine Ethik programmieren? Und wenn ja, wie? Es scheint, als seien solche Fragen unbequem, zumal dadurch bei allen an Big Data Beteiligten mehr Transparenz gefordert würde. Eine Arbeitsgruppe des Ethikrats beschäftigt sich zwar seit 2015 mit diesem Thema, hat jedoch vorwiegend Gesundheitsdaten im Blick.

Gegeben oder gemacht?

Eine verkürzende, positivistische Sichtweise verkennt, dass Daten nie reine, neutrale Repräsentationen der Welt sein können, sondern in einem Prozess unter soziokulturellen Bedingungen stets erst *entstehen.* Sie sind epistemologisch als *Gemachtes, Hergestelltes* und nicht als *Gegebenes* zu verstehen. Schließlich sind die

„Verfahren der Datengewinnung, Datensammlung, Speicherung, Analyse und Verarbeitung immer schon und immer noch in ein vielschichtiges Netz epistemischer Vorannahmen, technischer Möglichkeitsbedingungen und materieller Limitierungen eingewoben".[7]

Eine wie auch immer postulierte Objektivität oder Neutralität von Daten, Algorithmen oder sonstigen Technologien kann es schlicht nicht geben. Die Vorstellung, „der konstruktive und deutende Eingriff finde erst ab dem Zeitpunkt der Auswertung und Interpretation statt"[8], hätte weitreichende Folgen, vor allem auch für Lern- und Bildungsprozesse und zeichnet derzeit verantwortlich für das positivistische Grundverständnis von Big Data. Die von den Technologie-Unternehmen oft vermittelte Vorstellung von *Rohdaten* oder *Rohöl* der Zukunft impliziert hingegen, dass die Daten unbearbeitet vorlägen, bevor sie weiterverarbeitet und häufig in andere Kontexte gebracht werden. Ansätze, die von einer reinen Gegebenheit der Daten ausgehen (wie etwa Mayer-Schönberger und Cukier), laufen „in ihrer positivistischen Tendenz Gefahr, (Medien-)Technologien als eigentliche Realität zu entwerfen, als fixierende Letztbegründung von Bedeutung und Wissen."[9]

Bequemlichkeit und die Verkürzung des Wissensbegriffs

Wir delegieren durch eine algorithmenbasierte Sicht immer mehr Entscheidungen, lassen uns Empfehlungen und Vorschläge unterbreiten („Kunden, die dies kauften, schauten auch nach…"). Es ist bequem, sich nicht nach Alternativen umsehen zu müssen, denn unsere Wünsche, Bedürfnisse und Neigungen sind durch entsprechende Empfehlungsalgorithmen bereits passend formuliert und durch *Targeting* an uns herangetragen worden. Dies führt auf lange Sicht jedoch zu einem „fortschreitende[n] Ablegen unserer Bereitschaft zu eigenständigen Entscheidungen".[10] Jeder große Technologie-Konzern weiß mit seiner ökonomischen Big-Data-Strategie gerade auch um Formen der Beeinflussbarkeit, hat die Rezipienten mit ihren Nutzungsgewohnheiten vermessen, um regelmäßig passgenaue Angebote unterbreiten zu können. Je mehr ich mich auf diese Angebote unreflektiert einlasse, desto eher riskiere ich auch, „meine Neugier zu verlieren, meine Lust zur Entdeckung von Unbekanntem, den Nervenkitzel vor dem Unerwarteten."[11] Besonders kritisch werden diese Entwicklungen, wenn wir es uns beim Zugang zu Wissen derart bequem machen: „Wozu soll ich das wissen? Ich habe doch Google!", ist immer wieder zu hören, nicht nur von Schülern. Das Gleichsetzen von *Googlen* mit *Wissen* oder *Wissenserwerb* ist die Folge einer positivistischen Auffassung, die durch den Big-Data-Ansatz nur weiter vorangetrieben wird. Denn die Vorstellung, unser Begriff von Wissen lasse sich auf die Kumulation von Daten und Informationen oder das Vorhandensein von Korrelationen reduzieren und Wirklichkeit sei die Summe der Daten und deren optimierter Analysen, dürfte nicht nur Bildungsforscher alarmieren. Der Aufbau von Wissen ist auch unter digitalen Vorzeichen mehr als nur das Beschaffen von Informationen oder Herauslösen von Korrelationen.

Wer meint, Suchmaschinen seien neutral und die ersten Treffer einer Suchanfrage seien gleichzusetzen mit Wissenszuwachs, macht es sich in vielfacher Hinsicht zu leicht. Zudem verkennt er den konstruktivistischen, selbst bestimmten und autonomen Prozess der Wissensgenerierung durch Nachprüfen, Vergleichen, intersubjektives Kommunizieren, Verwerfen, Deuten usw. Mit der positivistischen „Umstellung vom Subjektiven und Ambivalenten des Interpretierens auf das Mathematische algorithmischer Analyse"[12] scheint immer mehr der Fehlschluss verbunden, die durch Big Data errechneten Korrelationen seien mit Faktizität gleichzusetzen. Letztlich sind die Wenn-Dann-Gefüge eben kein Wissen, das sofort zur Anwendung bereit stünde, sondern zunächst nichts anderes als Informationen, mit denen Menschen oder Algorithmen in Form von Folge-Entscheidungen weiterarbeiten und anschlussfähiges Wissen generieren können. Es macht das vorherrschende utilitaristische Verständnis von Big Data aus, dass es sich dabei oft um kommerzielles Wissen als Teil neoliberaler Gewinnoptimierung handelt: Nützlich ist, was zu Geld gemacht werden kann.

Der zunehmende Druck auf die Gesellschaft

Abwechslung, das Unerwartete, Impulsivität, Verhaltensänderungen, Spontaneität, schlicht eine „Kreativität des Handelns" (Hans Joas) scheinen in Zeiten von Big Data nebensächlich zu sein oder lediglich als unerwünschtes *Rauschen* wahrgenommen zu werden. Es sind ja auch die Eigenschaften, die uns von Maschinen unterscheiden. Bei Big Data geht es darum, Probleme rein technisch *(Data-driven)* anzugehen und im Sinne der Algorithmen-Logik klar definierte, schnelle Lösungen anzuwenden. Das Ziel ist dabei meist ökonomisch ausgerichtet: die Wahrscheinlichkeit zu erhöhen, die Nutzer als Kunden zu gewinnen bzw. zu binden. Mit diesem *Solutionismus* werde allerdings, so meint etwa der Netzkritiker Evgeny Morozov, nicht eine neue Daten-Effizienz und -transparenz sichtbar, sondern eine neue Geisteshaltung, mit der erst neue Probleme geschaffen würden. Allein die technische Verfüg- und Anwendbarkeit von Lö-

Markus Reinisch

Markus Reinisch ist Lehrer an einer bayerischen Mittelschule. Er schreibt neben literaturdidaktischen Texten zu aktuellen medien-, gesellschafts- und bildungspolitischen Themen für verschiedene Zeitschriften. *markus.reinisch@gmx.de*

sungsalgorithmen setzt uns als Gesellschaft und als Bürger, die wir digitale Techniken nutzen, immer stärker unter Druck. Auf Big Data bezogen, heißt dies: die Algorithmen finden „im Big Data Mining immer mehr Wenn-Dann-Korrelationen und stellen […] die Gesellschaft unter den Handlungsdruck, bei unerwünschten *Dann*-Folgen auf der *Wenn*-Ebene einzugreifen."[13] Die Bergwerk-Metaphern des *Data Mining, Digging into Data* und *Data Tools,* von den großen Technologie-Konzernen wirksam in Szene gesetzt, verschärfen den Druck, denn sie verschleiern deren kommerziell ausgerichtete Datensammelwut. Stattdessen suggerieren sie, dass da Wertvolles und Wissenswertes lagere, es aber abgebaut werden müsse, wenn die Gesellschaft und der Einzelne davon einen Nutzen haben wollten, wovon stets ausgegangen wird. „Wenn du nicht mitmachst, entgeht dir etwas", wird es gerade auch durch die Dynamik und den Gruppendruck der *Sozialen Netzwerke* multipliziert. Der amerikanische Historiker Jerry Z. Muller macht in seinem Buch „The Tyranny of Metrics" (2018) auf diese Entwicklungen eindrucksvoll aufmerksam. Vor allem auch darauf, dass der freizügige Umgang mit Daten neue Maßstäbe zu setzen vermag, durch die Menschen schneller unter Druck gesetzt werden als die Debatte darüber vorankommt.

Vom Subjekt zum Datenbank-Objekt

Die Daten-Abbau-Metaphern tragen offensichtlich positivistische Züge, indem nahe gelegt wird, dass Daten „als faktisch vorfindliche Entitäten in der Welt bestehen und nur von entsprechenden Apparaturen ‚abgebaut' werden müssten".[14] Das *Graben* nach Informationen, also das Aufspüren von Mustern und Korrelationen nach bestimmten Vorgaben erinnert eher an die Suche nach der Nadel im Heuhaufen. Die Einzelnen verlieren immer mehr die Selbstbestimmung über ihren Informations- und Bildungsprozess und damit schwindet auch ihre Subjektivität, meist ohne dass sie es bemerken. Konnte in den Neunzigerjahren der Einzelne als neugieriges, weitgehend autonom handelndes Subjekt die Welt via Internet erkunden, so ist sie/er mittlerweile zum Objekt geworden, zu einem spannenden, erkundbaren Objekt für die großen Datensammler aus dem Silicon Valley. Die Subjektivität des Menschen sei, so der Medien- und Kulturwissenschaftler T. C. Bächle, „längst in eine Datenbanklogik übersetzt worden"[15], mit weitreichenden kulturellen Folgen. Dazu trug nicht zuletzt die Verabsolutierung des Messbaren bei. Zur Subjektivität gehören auch der individuelle Prozess des Aneignens von Wissen und die Autonomie, diesen Prozess jederzeit selbst steuern zu können. Big Data jedoch weist in eine andere Richtung, nämlich „hin zu einer positivistischen Denkökonomie, die es den Algorithmen überlässt, die Welt für die Menschen in digitale Datenpakete zu gliedern und neu anzuordnen".[16] Wir sind also vielfach lediglich am Reagieren, beispielsweise darauf, wie wir vermessen werden und Werte optimieren können (Self-Tracking). Agieren in Form von Durchdenken, Verstehen, Reflektieren und kritischen Äußerungen hingegen scheint in der zahlengläubigen Big-Data-Welt überflüssig geworden. Die Gefahr der *Filterblase,* 2012 von dem Netzaktivisten Eli Pariser beschrieben, entsteht, weil rasch Gleichgesinnte in den Kommunikationsräumen der sozialen Netzwerke gefunden werden können. Der Klick auf einen algorithmisch empfohlenen Link genügt und man navigiert von einer politisch rechten Seite zur nächsten. Wenn die Algorithmen das Widersprüchliche also bereits herausrechnen, bestehende Positionen ständig bestätigen und kritisches Nachfragen bzw. -denken ohnehin oftmals zu anstrengend scheint, ist Simanowskis Diagnose kaum zu widersprechen: „Der Vermessungsimpuls der Moderne wandelt sich […] zum Werkzeug eines Abschottungsnarzissmus."[17]

Zusammenfassung und Ausblick: Medienpädagogik und Medienkritik

Für den menschlichen Drang zum Vermessen, Berechnen und Vorhersagen ist in Big Data eine Technologie gefunden, die in etlichen Bereichen zum Einsatz kommen kann und wird. Gapski nennt Verteidigungs- und Finanzsektor, Konsumbereich, Versicherungswesen, politischen Wahlkampf, Strafverfolgung, Medizin, Katastrophenhilfe, Verkehrsplanung und Natur- sowie Geisteswissenschaften.[18] Dass es Vorteile geben und die Erkenntnisgewinnung vorangetrieben wird, steht nicht zur Debatte. Jedoch sollte dabei auch bewusst gemacht werden, dass die mit der Technologie implizierte veränderte „Sicht auf die Welt, die neupositivistische Handhabung von Datenbeständen"[18] nicht ohne soziale und kulturelle Folgen bleiben wird. Wenn bei Big Data für gesellschaftliche und individuelle Beschreibungen von der beschriebenen 1:1-Abbild-Beziehung ausgegangen wird, heißt das, man kann die Gesellschaft bzw. den Menschen verlustfrei und objektiv *in Daten übersetzen* als *digitales Double* oder *digitales Ich*, wenn man nur genügend „Datenpunkte" über sie bzw. ihn hat. Verhaltens- und Bewegungsmuster werden digital verdoppelt, um auf der Basis von errechneten Vorlieben Voraussagen zu wahrscheinlichen künftigen Gewohnheiten berechnen zu lassen. Hierin liegt das höchst verkürzende und positivistische Grundverständnis von Big Data, das sich zum Beispiel auch im Ausrufen einer vermeintlich neuen Wissenskultur durch die Macht wirtschaftlicher Großkonzerne zeigt. Es wird eine der Hauptaufgaben von Medienkritik, -pädagogik, -ethik sowie Informatik und auch Techniksoziologie sein, im Daten-Diskurs auf diese positivistische Sicht und die Deutungshoheit durch bestimmte Gruppen hinzuweisen. Dabei gilt es, „die vermeintliche Allmacht von Algorithmen als Mythos zu entlarven".[20]

Es wird darum gehen, nicht vor der Macht der Großkonzerne zu kapitulieren und der kulturpessimistischen Vorstellung eines „neuen Informationsproletariats" (Timo Daum) anzuhängen. Vielmehr sollen aufgeklärte, verantwortungsvolle, kritisch-reflektierte Mediennutzer im Mittelpunkt stehen, die um das Manipulationspotenzial nicht nur von Algorithmen und Big Data wissen, sondern auch *Fake News* als postfaktisch einordnen können. Mündige, digitale Techniken nutzende Bürger, die in ihrer (Medien-) Bildung nicht „vermessungsaffin und zahlengläubig an die Abbildung der Welt"[21] glauben, haben auch die prinzipielle Gemachtheit von Daten im Blick. Valentin Dander erläutert eine solche Form der Medienkritik für die medienpädagogische Praxis und verweist auf das im Kontext von Big Data viel zitierte „‚*Raw' Data* is an Oxymoron" von Lisa Gitelman und Virginia Jackson. Und „wenn die Medienpädagogik in ihren Überlegungen Daten nicht als solche selbstevidenten und irreduziblen Entitäten hinnehmen will, dann sollte nicht ihre unhinterfragbare ‚Gegebenheit', sondern die ‚Gemachtheit' von Daten den Ausgangspunkt für entsprechende Lernprozesse dar-

stellen."[22] So haben Medienpädagogik und verwandte Disziplinen früh anzusetzen bei all den Aufgaben, die schließlich zu wichtigen Fragen auf einer Meta-Ebene führen könnten: Worin liegt das Faszinosum von Big Data, dass wir viele der Dienste so unhinterfragt in Anspruch nehmen und uns nicht um ihre positivistisch-verkürzende Sichtweise kümmern? Warum lassen wir zu, dass durch die Zahlengläubigkeit Prozesse der Digitalisierung nicht nur die Rahmenbedingungen bilden, sondern oft den Kern in vielen Lebensbereichen? Und warum sind Vermessung, Berechnungen, Statistiken oft mehr wert als ästhetische Erziehung und real-sinnliche Erfahrungen?

Anmerkungen

1 *Mayer-Schönberger V, Cukier, K (2013): Big Data. Die Revolution, die unser Leben verändern wird. München, S. 78*
2 *Ortlieb CP (2010): Ökonomie ist eigentlich keine Wissenschaft. In FAZ vom 08.05.2010. Online unter: http://www.faz.net/aktuell/gesellschaft/oekonomie-ist-eigentlich-keine-wissenschaft-11418489.html (letzter Zugriff: 08.03.2018)*
3 *Mayer-Schönberger/Cukier, S. 94*
4 *Meyer-Ebrecht D (2016): Selbstbestimmt war gestern? Wenn wir das Entscheiden Maschinen überlassen. In: FIfF-Kommunikation 1/16, S. 12-15, S. 14*
5 *Burkhardt M (2015): Digitale Datenbanken. Eine Medientheorie im Zeitalter von Big Data. Bielefeld 2015, S. 341*
6 *Lobe A (2016): Wir laufen auf Autopilot. In: FAZ vom 27.02.2016. Online unter: http://www.faz.net/aktuell/feuilleton/kuenstliche-intelligenz-wir-laufen-auf-autopilot-14079287.html (letzter Zugriff: 31.01.18)*
7 *Borck C (2017): Big Data. Praktiken und Theorien der Datenverarbeitung im historischen Querschnitt. In: NTM – Zeitschrift für Geschichte der Wissenschaften, Technik und Medizin 4/2017, S. 399 – 405, S. 404*
8 *Dander V (2014): Von der ‚Macht der Daten' zur ‚Gemachtheit von Daten'. Praktische Datenkritik als Gegenstand der Medienpädagogik. In: Mediale Kontrolle unter Beobachtung 3.1/2014. Online unter: http://www.medialekontrolle.de/wp-content/uploads/2014/09/Dander-Valentin-2014-03-01.pdf (letzter Zugriff: 08.03.2018), S. 1-21, S. 2*
9 *Bächle TC (2016): Digitales Wissen, Daten, Überwachung zur Einführung. Hamburg 2016*
10 *Meyer-Ebrecht, S. 14*
11 *Ebd.*
12 *Simanowski R (2016): Data Love. Berlin 2016, S. 13*
13 *Ebd., 12 (Hervorhebung im Original)*
14 *Püschel F (2014): Big Data und die Rückkehr des Positivismus. Zum gesellschaftlichen Umgang mit Daten. In: Mediale Kontrolle unter Beobachtung 3.1/2014. Online unter: http://www.medialekontrolle.de/wp-content/uploads/2014/09/Pueschel-Florian-2014-03-01.pdf (letzter Zugriff: 16.01.2018), S. 1-23, S. 12*
15 *Bächle, S. 72*
16 *Püschel, S. 18*
17 *Simanowski, S. 80*
18 *Gapski H (2015): Big Data und Medienbildung – eine Einleitung. In: Ders. (Hg.): Big Data und die Medienbildung. Zwischen Kontrollverlust, Selbstverteidigung und Souveränität in der digitalen Welt. Marl, S. 9-18, S. 10ff.*
19 *Ebd., 13*
20 *Burckhardt, S. 302*
21 *Bächle, S. 142*
22 *Dander, S. 3*

Hans-Jörg Kreowski

Der Informationsraum aus militärischer Sicht

Dieser Artikel ist eine schriftliche Ausarbeitung eines Vortrags auf dem Kongress der Informationsstelle Militarisierung 2017 zum Thema Krieg im Informationsraum. Es geht um Cyberkrieg, was die etwas gängigere Bezeichnung für eine bedenkliche Entwicklung ist.

Während Albert Einstein zu einem denkbaren dritten Weltkrieg noch sagt: „I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones", legt sich Mandeep Singh Bhatia fest: *World War III: The Cyber War*[1]. Wenn auch die meisten anderen Fachleute und KommentatorInnen nicht soweit gehen, zeigt die enorme Resonanz des Themas Cyberkrieg in den Printmedien, dass hier eine neue ernsthafte Bedrohung heraufzieht (siehe Abbildung 1 mit diversen Titelbildern zum Cyberkrieg).

Das Thema hat mit *Zero Days: Hinter den Kulissen des Cyberkriegs* von Alex Gibney auch die Filmwelt erreicht. Der Dokumentarfilm wurde auf der Berlinale 2016 gezeigt. Mit Datum 19. August 2016 kann man recht reißerisch lesen[2]:

> *„Die Dokumentation von Alex Gibney fängt als Spurensuche über den Computervirus Stuxnet an. Und während IT-Sicherheitsexperten, Ex-NSA- und CIA-Chefs, ehemalige Mossad-Agenten und auch ein paar Whistleblower über das reden, worüber niemand reden darf, fällt der Satz, dass es sich gerade anfühle wie 1945, nachdem die USA zwei Atombomben über Japan gezündet haben: In dieser verwirrend coolen Spionage-Geschichte, die Sie permanent auf der Stuhlkante hält, geht es um mächtige neue Waffen, über deren Reglementierung man dringend reden muss, wenn die Welt nicht noch mehr im Chaos versinken soll."*

Stuxnet ist aber nur ein Beispiel. Die Liste gravierender Cyberattacken ist lang. So hieß es bei Heise Security am 27. Juni 2017: „Rückkehr von Petya – Kryptotrojaner legt weltweit Firmen und Behörden lahm", wobei Computersysteme verschlüsselt wurden mit dem Angebot, sie bei Zahlung von Lösegeld wieder zu entschlüsseln. So wurde am 15. Mai 2015 von SPIEGEL ONLINE gemeldet: „Sicherheitsalarm im Parlament: Cyberangriff auf den Bundestag", was bei n-tv die Überschrift „Cyber-Attacke löst Alarm aus: Beispielloser Angriff auf den Bundestag" erhielt. Die Beseitigung des erheblichen Schadens hat über 100 Millionen Euro gekostet. Weitere Beispiele liegen weiter zurück: eine Angriffsserie auf US-amerikanische Computersysteme von

Abbildung 1: Auswahl an Titelbildern zum Thema Cyberkrieg

Rüstungskonzernen, NASA und andere, die unter dem Namen Titan Rain bekannt wurde, die Denial-of-Service-Attacken auf estländische und georgische Regierungswebseiten, die tagelang außer Betrieb waren, die als Olympic Games bezeichnete und bisher vielleicht gravierendste Malwareattacke mit dem bereits angesprochenen Cyberwurm Stuxnet auf die nuklearen Wiederaufbereitungsanlagen des Irans, die dessen Atomwaffenprogramm um Monate zurückgeworfen hat. Die Entwicklung von Stuxnet hat nach Schätzungen von Fachleuten vielleicht bis zu einer Milliarde US-Dollar gekostet, zeigt aber, dass Cyberattacken zur Zerstörung technischer Anlagen führen können. Viele weitere Beispiele ähnlicher Art ließen sich anführen. Sie alle zeigen, dass sich Cyberangriffe mit Viren, Würmern, Trojanern und sonstiger Schadsoftware für Spionage, Propaganda und Informationsmanipulation verwenden lassen, dass man damit Service-Webseiten und Computersysteme insgesamt lahmlegen, infiltrieren und umfunktionieren kann, ja dass es sogar möglich ist, technische Geräte wie Kraftfahrzeuge, Flugzeuge bis hin zu ganzen Industrieanlagen fernzusteuern oder zu zerstören. Besonders bedroht sind kritische Infrastrukturen wie Energie- und Wasserversorgung, Krankenhäuser, Straßen-, Bahn- und Flugverkehr, Verwaltungseinrichtungen und militärische Einrichtungen. Je nach Ausmaß reichen die Konsequenzen von unbequem bis Elend und Tod.

Zum Begriff Cyberkrieg

An dieser Stelle möchte ich einen Versuch wagen, den Begriff Cyberkrieg wenigstens ansatzweise zu definieren als Kriegsführung mit Informations- und Kommunikationstechnik (IKT) wie Computer, Netzwerke, Software als Waffen und militärische Systeme aller Art, deren Entwicklung und Betrieb des Einsatzes von Informatikmethoden bedürfen. Dabei ist schon umstritten, ob das IKT-Steuerung von militärischen Systemen wie Raketen, Drohnen, Luftabwehr, Panzer etc. einschließt. Ich würde das bejahen, weil es sich um dieselben oder zumindest sehr ähnliche methodische und technologische Grundlagen aus der Informatik sowie der Informations- und Kommunikationstechnik handelt.

Der Begriff Cyberkrieg ist noch relativ jung. Vieles, was darunter subsumiert wird, wurde früher als Informationskrieg bezeichnet. Ute Bernhardt und Ingo Ruhmann geben im Dossier 74 *Information Warfare und Informationsgesellschaft – Zivile und sicherheitspolitische Kosten des Informationskriegs*, das als Beilage der Zeitschriften *Wissenschaft und Frieden* 1/2014 und *FIfF-Kommunikation* 1/2014 erschien, einen umfassenden Überblick. Sie sehen die Anfänge in der Entschlüsselung der Enigma-Chiffriermaschinen, die vom deutschen Militär im Zweiten Weltkrieg für die Verschlüsselung des Nachrichtenverkehrs eingesetzt wurden. Ein Team von Fachleuten um den berühmten britischen Mathematiker Alan Turing in Blechley Park hat das mit Hilfe von Vorläufern heutiger Computer geschafft, was nicht ohne Einfluss auf den Kriegsverlauf blieb.

Es führte bereits damals zur Gründung der National Security Agency (NSA) in den USA und des Government Communication Headquarters (GCHQ) in Großbritannien, die beide bis heute eine entscheidende Rolle als Cyberkriegführer spielen. Einen ersten Höhepunkt des *Information Warfare* war dann der Aufbau von C3I-Systemen (Control, Command, Communication, Intelligence) im Kalten Krieg in den USA, durch die die Kriegführungsebene auf Informations- und Kommunikationstechnik abgestützt wurde. Seitdem sind vor allem die Fähigkeiten dazugekommen, in generische Systeme durch Hacking gezielt einzudringen, sie zu manipulieren und sie zu zerstören.

Auf der begrifflichen Seite muss beachtet werden, dass alle Varianten wie Cyberkrieg, Informationskrieg, Krieg im Informationsraum oder Krieg im Cyber- und Informationsraum den gemeinten Sachverhalt nur sehr bedingt treffen. So ist *cyber*, das vom Altgriechischen *steuern und navigieren* stammt, zu eng und als Synonym für *Computer- und Internet-gestützt* zu nebulös. So ist *Information* zu statisch, und der *Informationsraum* ist überhaupt gar kein „Raum", sondern ein riesiges Netz aus Computern und computergesteuerten Geräten, Anlagen, Maschinen etc. Tatsächlich geht es um programmierte, von Algorithmen getriebene Kriegsführung. Ich verwende den Begriff Cyberkrieg dennoch auch weiterhin, weil er inzwischen so etabliert ist, dass mit jeder anderen Bezeichnung Verständnisschwierigkeiten entstehen könnten.

Weltweites Cyberwettrüsten

Dass das als Cyberkrieg bezeichnete Phänomen ernst genommen werden muss und eine eklatante neue Bedrohung darstellt, ergibt sich aus der Tatsache der weltweiten gigantischen Aufrüstung in diesem Bereich. Mehr als 100 Staaten haben Cyberkriegseinheiten gebildet, die zudem überwiegend offensiv ausgerichtet sind. Die USA betreibt mit der NSA und dem United States Cyber Command (USCYBERCOM) die größte Einheit. China hat die *Blaue Armee*, eine Hackereinheit, die offiziell rein defensiv ausgerichtet ist. Russland wird verdächtigt, wiederholt offensiv Cyberangriffe zu betreiben oder zu unterstützen, was allerdings wohl nicht wirklich bewiesen ist. Der Iran brüstet sich damit, die weltweit zweitgrößte Einheit zu haben. Israel hat die *Cyber Defense Taskforce*, Großbritannien die *Government Communication Headquarters* (GCHQ) und so weiter und so weiter.

Auch Deutschland steht da nicht zurück, auch wenn die Regierung erst spät auf die weltweite Entwicklung systematisch reagiert hat. Seit 2011 arbeitet der Nationale Cyber-Sicherheitsrat, der beim Beauftragten der Bundesregierung für Informationstechnik angegliedert ist. Im selben Jahr nahm das Nationale Cyberabwehrzentrum seine Arbeit auf, in dem die Cyberaktivitäten von Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesamt für Verfassungsschutz und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe koordiniert werden. Assoziierte Mitglieder sind das Bundeskriminalamt, der Bundesnachrichtendienst, die Bundespolizei, die Bundeswehr mit dem Militärischen Abschirmdienst sowie das Zollkriminalamt. Außerdem haben das BSI und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2012 die *Allianz für Cybersicherheit* geschmiedet. Die Strukturen dieser Einrichtungen sind allerdings eher intransparent und ihre Kontrolle ziemlich unklar. Die Bundeswehr steht nicht abseits. Seit 2016 baut sie einen Organisationsbereich *Cyber- und Informationsraum* (CIR) mit rund 13.500 Dienstposten auf. Das Kommando CIR, die Führungsebene des Bereichs, wurde am 5. April 2017 offiziell durch die Verteidigungsministerin in Dienst gestellt. Es bildet ein Dach über Abteilungen, die vorher über viele Bereiche der Bundeswehr verteilt waren; insbesondere sind ihm das Kommando Strategische Aufklärung, das Kommando Informationstechnik der Bundeswehr, ehemals Führungsunterstützungskommando der Bundeswehr, und das Zentrum für Geoinformationswesen der Bundeswehr unterstellt. Aufgaben wie die Erstellung von Lageplänen, Weiterentwicklung, Ausbildung, nationale und internationale Zusammenarbeit im Cyber- und Informationsraum sowie die Informationssicherheit in der Bundeswehr liegen damit in einer Hand. Soweit, so unspektakulär. Aber der Organisationsbereich CIR bringt auch einige äußerst bedenkliche Entwicklungen mit sich. So hat die Bundeswehr neben Heer, Marine und Luftwaffe eine weitere Teilstreitkraft gebildet, was auch weltweit betrachtet eine neue Qualität darstellt. Defensive und offensive Cyberkriegsfähigkeiten sollen massiv ausgebaut werden. Dazu führt die Bundeswehr eine millionenschwere Werbekampagne zur Personalgewinnung durch und hat an der Universität der Bundeswehr München einen Masterstudiengang IT-Sicherheit eröffnet, dessen personelle Ausstattung jede zivile Hochschuleinrichtung vor Neid erblassen lässt.

... aus militärischer Sicht

Cyberkrieg gilt als militärisch attraktiv, weil bei einem Angriff keine eigenen SoldatInnen direkt gefährdet sind, weil die Rückverfolgung schwierig und teilweise unmöglich ist, so dass der Angegriffene gar nicht weiß, wer angreift, weil der Angriff auf meist zivile Ziele den Gegner empfindlich schwächen kann, weil Cyberwaffen vergleichsweise billig zu haben sind. Die mangelhafte Rückverfolgung und Zuordnung von Cyberangriffen begünstigt Attacken auch unterhalb der Kriegsschwelle als „Nadelstiche" oder Versuchsballon. Die Vorteile gelten allerdings nur für die Angreifer, für die Angegriffenen verkehrt sich das in das Gegenteil. Aber auch die Vorteile sind eher scheinbar und in vielfältiger Hinsicht eigentlich Nachteile. Weil zum Beispiel Cyberwaffen relativ leicht zu beschaffen oder zu entwickeln sind, können viele Staaten und auch größere Terrorgruppen sich das leisten, so dass die eigene Gefährdung wächst. Zudem ist das Angreifen mit Cyberwaffen wesentlich einfacher als das Verteidigen, weil dafür die Instrumente bekannt sind und man nur ein paar gute Computer und ein Team von Hackern braucht, die wissen, wie man die unzähligen Schwachstellen und Sicherheitslücken für die Installation von Schadsoftware nutzen kann. Cyberabwehr dagegen ist bei massiven und komplexen Angriffen technisch viel schwieriger und nur unzureichend beherrscht.

Hans-Jörg Kreowski

Hans-Jörg Kreowski ist Professor (i. R.) für *Theoretische Informatik* an der Universität Bremen und Vorstandsmitglied des *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung in Wort und Schrift Stellung genommen.

Dennoch wird Cyberrüstung von Politik und Militär für nötig erachtet mit der Begründung, dass alle im Cyberbereich rüsten, so dass man selbst nicht abseits stehen kann. Die Konsequenz ist eine gigantische weltweite Cyberrüstungsspirale. An der drehen insbesondere die USA mit ungeheuren Geld- und Personalmitteln. In ihrer *Strategy for Operating in Cyberspace* wird das damit motiviert, dass die USA im Bereich Defensive schwach ist bei gleichzeitiger hoher Abhängigkeit von funktionierender Informationstechnik und hoher Verletzlichkeit durch Vernetzung, Zentralisierung, Standardisierung, Mobilität. Man findet dort eine weitgefasste Definition eines Cyber-Angriffs: Denial-of-Service-Attacken, Sabotage von militärischen und zivilen Systemen (insbesondere von kritischen Infrastrukturen), Manipulation von Informationen, Wirtschaftsspionage und Diebstahl geistigen Eigentums. Hacktivismus, Cybercrime und Cyberwarfare werden undifferenziert als Bedrohungen der nationalen Sicherheit angesehen. Die Eintrittsschwelle für Gegenangriffe wird in diesem Strategiepapier sehr niedrig angesetzt, wobei ausdrücklich konventionelle Gegenschläge vorgesehen sind. Auch wenn dieser Vorbehalt bisher wohl nicht zur Anwendung gekommen ist, klingt er doch ziemlich besorgniserregend. Was auch Deutschland und die anderen NATO-Partner der USA in diesem Zusammenhang betrifft, ist die Frage, ob die USA im Falle eines Cyberangriffs den Bündnisfall ausrufen und so die ganze NATO in einen (Cyber-)Krieg hineinziehen können.

An einer anderen Stelle beschäftigt sich die NATO bereits mit einem wichtigen Aspekt der Cyberkriegsführung. Zwischen 2009 und 2012 wurde von einer internationalen Gruppe mit rund 20 Fachleuten am *NATO Cooperative Cyber Defence Centre of Excellence* in Tallinn eine rechtlich nicht bindende Studie erarbeitet, wie sich das Kriegsvölkerrecht für den Kriegsfall (vor allem die Genfer Konventionen) auf Cyber-Konflikte und Cyberkrieg anwenden lässt. 2013 erschien Teil 1 des *Tallinn-Manuals* bei Cambridge University Press. Der Fokus des ersten Teils liegt auf den massivsten Cyber-Operationen, die während bewaffneter Konflikte durchgeführt werden oder das Verbot von Gewalteinsatz in internationalen Beziehungen verletzen. 95 Regeln zur Interpretation einzelner Bestimmungen des Kriegsvölkerrechts hinsichtlich Cyberkrieg sind aufgestellt worden. Inzwischen ist auch 2017 Teil 2 erschienen, in dem niederschwelligere Cyberangriffe behandelt werden.

Ohne auf die Details einzugehen, sei daran erinnert, dass die Genfer Konventionen von Kriegsparteien verlangen, Opfer, Wehrlose und Unbeteiligte zu schützen, wobei insbesondere Angriffe auf Zivilpersonen verboten sind. Außerdem sollen zivile Einrichtungen und Kulturgüter verschont werden. Schon allein daraus ergibt sich, dass die außerordentliche Bedrohung von zivilen Infrastrukturen durch die Cyberkriegsrüstung völkerrechtlich inakzeptabel ist. Darüber hinaus sei auch angemerkt, dass die Charta der Vereinten Nationen, der fast alle Staaten der Welt zugestimmt haben, Krieg verbietet. In der Präambel heißt es dazu: „... determined to save succeeding generations from the scourge of war ...“, und im Artikel 2 des ersten Kapitels steht: „... All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered ...“. Im Grundsatz ist also Cyberkrieg wie Krieg verboten.

Cyberpeace

Aus all diesen Fakten, Problemen, Vorkommnissen und allseitigen Bedrohungen wäre die einzig richtige Konsequenz Cyberabrüstung und ein Verbot von Cyberwaffen, zumindest den offensiven. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) führt seit einigen Jahren eine Cyberpeace-Kampagne durch, deren Ziel ein Gegenkonzept zum Cyberkrieg ist.

Angestrebt ist die Ächtung jeglicher Form von Cyberwaffen (zumindest von offensiven). Eine wesentliche Voraussetzung auf dem Weg dahin wäre ein demokratisch gestaltetes, demokratisch kontrolliertes und entmilitarisiertes Internet, das dem Frieden dient und nicht der Ausspähung sowie der Unterstützung militärischer Aktivitäten. Völlig utopisch ist das Ziel nicht, denn es gibt auf der Ebene de Vereinten Nationen ExpertInnen-Gespräche mit dem Ziel eines Cyberwaffen-Verbots oder wenigstens einer Regulierung. Aber auch auf nationaler Ebene lässt sich etwas tun. So könnte sich die Bundeswehr anders als momentan auf reine Cyberabwehr beschränken. So könnte gesetzlich geregelt werden, dass alle im zivilen und militärischen Bereich entdeckten Sicherheitslücken und Schwachstellen in IT-Systemen aufgedeckt und beseitigt werden müssen, statt sie für den eigenen offensiven Gebrauch zu erwerben, zu nutzen und geheim zu halten.

cyberpeace
eine Kampagne des FIfF

Mehr zum Thema Cyberpeace findet man auf der Webseite *https://cyberpeace.fiff.de*. Neben dem bereits genannten Dossier 74 der Zeitschrift Wissenschaft und Frieden möchte ich auf die Publikationen im Abschnitt *Referenzen* als weiterführende Literatur verweisen.

Referenzen

Hügel S, Kreowski HJ und Meyer-Ebrecht D (2017): Cyberwar and Cyberpeace. In: Handbook of Cyber-Democracy, Cyber-Development and Cyber-Defense, Springer, 25 Seiten.

Johnigk S, Kreowski HJ und Nothdurft K (2014): Cyberwar – Schimäre oder reale Bedrohung?, FIfF-Kommunikation 4/2014, Seiten 74-77.

Kreowski HJ and Meyer–Ebrecht D (2017): „Revolution in Military Affairs“. In: The Future Information Society, World Scientific Series in Information Studies, Band 8, Seiten 439-448.

Meyer-Ebrecht D (Hg.) (2015): Kriegführung im Cyberspace, Dossier 79 in Wissenschaft und Frieden 3/2015 und FIfF-Kommunikation 3/2015.

Ganz besonders möchte ich schließlich das 5-minütige Video von Alexander Lehmann: Cyberpeace statt Cyberwar, aus dem Jahre 2017 empfehlen, das mit Unterstützung des FIfF entstanden ist und sowohl sehr anschaulich in das Thema Cyberkrieg einführt als auch die Grundidee von Cyberpeace vermittelt (https://vimeo.com/216584485, https://www.youtube.com/watch?v=St955HBD-7k).

Anmerkungen

1 *Titel eines Artikels im International Journal of Cyber Warefare and Terrorism 1,3 (2011), 11 Seiten*

2 *https://www.stern.de/kultur/film/trailerpremiere-zero-days---der-krieg-tobt-im-computer-7015382.html*

Leo Thüer

Datenschutz à la „Friss oder Stirb“: Max Schrems reicht Beschwerde gegen Datenkonzerne ein

Laut Datenschutzgrundverordnung sollen wir selbst entscheiden können, ob und wem wir die Nutzung unserer Daten erlauben. Die vorherrschende Praxis der großen Datenkonzerne sieht aber anders aus. Wir sprechen mit Datenschutzaktivist Max Schrems über den politischen Kontext des Regelwerks und wie seine neue Organisation gegen Zwangszustimmungen vorgehen will.

Seit Freitag, 25. Mai 2018 ist die Datenschutzgrundverordnung[1] (DSGVO) europaweit wirksam und soll den Nutzerinnen und Nutzern eigentlich die freie Wahl lassen, ob und wem sie die Verarbeitung ihrer personenbezogenen Daten erlauben. Das erleben viele NutzerInnen in den letzten Tagen aber noch anders[2]. Den großen Datenkonzernen die Einwilligung in die Datenverarbeitung zu verweigern, bedeutet meist, deren Dienste nicht nutzen zu können. Max Schrems sprach mit uns darüber, wie er das ändern will.

Der Wiener Jurist und Datenschutzaktivist Max Schrems[3] wurde mit seiner Klage gegen Facebook[4] weltweit bekannt. Er erwirkte damals, dass der Europäische Gerichtshof das Safe-Harbor-Abkommen zu Fall[5] brachte. Sein neues Projekt „noyb – none of your business“[6] hat am 25. Mai die Arbeit aufgenommen und soll an diesen Erfolg anschließen. Ziel der Initiative ist es, die Lücke zwischen europäischen Datenschutzgesetzen und der unternehmerischen Praxis einiger Großkonzerne zu schließen.

DSGVO: Sammelklagen sollen für Klarheit sorgen

netzpolitik.org: *Hallo Max Schrems! Die Datenschutzgrundverordnung ist seit vergangenem Freitag europaweit wirksam. Wie hast du die Tage seitdem erlebt?*

Max Schrems: Eine Mischung aus Panik, skurrilen Reaktionen von Unternehmen und ebenso faszinierenden Versuchen der großen Player, einfach so weiterzumachen wie bisher und dabei zu behaupten, DSGVO-konform zu sein. Der DSGVO fehlt es an bestimmten Stellen an klaren Regelungen und das führt natürlich, so wie lange befürchtet, zu viel Rechtsunsicherheit. Hier läuft aber ein Spiel: Die Industrie-Lobbyisten haben erst dafür gesorgt, dass das Gesetz schwammig wird, mit Ideen wie einem „risikobasierten Ansatz“ statt klareren Grenzwerten. Damals mit dem Argument, dass wir „Flexibilität“ für kleine Unternehmen und Vereine brauchen. Genau diese „Flexibilität“ überfordert die Kleinen aber nun extrem, und das wird wiederum genutzt, um die gesamte Datenschutzgrundverordnung anzugreifen.

netzpolitik.org: *Inwiefern beeinflusst das neue Regelwerk Eure Arbeit?*

Max Schrems: Wir haben nun erstmals die Möglichkeit, auch entsprechende Strafen auszulösen, europaweit Verfahren bei den Behörden anzustoßen und auch gerichtlich vorzugehen. Leider haben wir in Österreich weiter nicht die Möglichkeit eine „Verbandsklage“ nach Artikel 80 Abs. 2 DSGVO einzubringen. Das kann sich aber auch noch ändern. Andernfalls kann man das eventuell auch über Deutschland machen. Machen wir eben einen „noyb – Germany e. V.“.

Der Wiener Datenschutzaktivist Max Schrems
All rights reserved europe-v-facebook.org

Auch Datenkonzerne müssen sich an Recht halten

netzpolitik.org: *Du hast ja mit deiner ersten Klage gegen Facebook ordentlich Öffentlichkeit bekommen und auch Erfolg gehabt – die Safe-Habour-Entscheidung wurde 2015 gekippt. In diesem Zusammenhang hast du den Verein „europe-v-facebook.org“ gegründet. Kommt Facebook in Sachen Datenschutz ein Sonderstatus zu, ist es quasi das größte Übel?*

Max Schrems: Es war reiner Zufall, dass ich mich damals mit Facebook beschäftigt habe. Ich glaube, es ist in einer juristischen Auseinandersetzung, wo es am Ende um Grundsatzfragen geht, notwendig, sich einen Fall rauszupicken, den man dann auch durchzieht – eher, als sich mit 100 Fällen zu verzetteln. Das ist für uns aber auch immer eine Frage der Finanzierung, also wie wir möglichst effektiv Spendengelder einsetzen. Noyb.eu hat hoffentlich bald die Kapazität, mehr Fälle zu betreiben. Wir werden aber immer repräsentative Einzelfälle betreiben und keine „Massen-Verklagungen“ machen. So viele Unternehmen, die wirklich wissentlich und absichtlich das Recht verletzten, gibt es dann auch gar nicht.

netzpolitik.org: *Ihr habt am vergangenen Freitag die ersten Beschwerden wegen „Zwangszustimmung" gegen Google, Instagram, WhatsApp und Facebook eingereicht. Wie läuft das jetzt genau ab und welchem Verfahren rechnest du die meisten Chancen zu?*

Max Schrems: Ja genau, wir haben drei Beschwerden zu Unternehmen der Facebook-Gruppe eingebracht. Diese werden wohl von der irischen Behörde gemeinsam mit den Behörden in Österreich, Hamburg und Belgien bearbeitet werden, da hier der Unternehmenssitz immer Irland ist. Wir warten hier mal auf die Stellungnahmen von Facebook und auf die nächsten Schritte im Verfahren. Spannend wird am Ende vor allem, ob es eine Strafe setzt und wie hoch diese ist.

Der Fall gegen Google zu Android läuft in Frankreich. Weil hier der Unternehmenssitz in den USA ist, kann die französische Behörde recht unabhängig entscheiden. Die Behörde hat auch schon Strafen gegen Google ausgesprochen.

Wenn man die Frage der Zwangszustimmung bei ein paar Unternehmen durchgefochten hat, dann gehe ich davon aus, dass sich auch alle anderen Unternehmen daran halten. Wenn nicht, können wir dann noch immer nachfassen. Wir werden über den Sommer vermutlich noch ein paar Beschwerden zu Fragen der Zustimmung einbringen. Gleichzeitig bereiten wir noch ein paar andere, komplexere Themen vor. Wir haben aber operational auch erst am 25. Mai gestartet und müssen daher noch viel interne Organisation machen. Wir ziehen zum Beispiel bald in ein dauerhaftes Büro um, brauchen eine dauerhafte Webseite oder wollen bald ein paar weitere Mitarbeiter einstellen.

Was ist dran an der DSGVO-Panik?

netzpolitik.org: *Die europäischen Datenschutzbehörden haben sich ja offen über fehlendes Personal und mangelhafte Kompetenzen beschwert. Wie schätzt du die Möglichkeiten der nationalen Datenschutzbehörden bei Euren Klagen ein?*

Max Schrems: Ich habe vor dem Verfahren weniger Angst. Wir haben die Sachen ja schon „servierfertig" vorgebracht, so dass hier die Arbeit der Behörden eher überschaubar ist. Das ist auch der Vorteil von Stellen wie noyb.eu – wenn Experten etwas einbringen, ist das auch für die Behörden einfacher zu bearbeiten. Das Problem wird eher der Instanzenzug sein. Wenn hier entsprechend entschieden wird, werden wohl die Unternehmen oder eben wir vor die Gerichte ziehen, und das kann auch bei den Behörden viel Geld und Zeit verschlingen.

netzpolitik.org: *Wie bewertest du die DSGVO-Debatte der vergangenen Wochen in Bezug auf die vorherrschende Frustration und den medialen Fokus auf Bußgelder für kleine und mittelgroße Unternehmen? Für wen gibt es Grund zur Panik und wer profitiert von der DSGVO?*

Max Schrems: Die eigentlichen Datenschutzrechte müssten natürlich für alle Unternehmen gelten. Ich war aber immer dafür, dass man die Pflichten zur Dokumentation und Administration massiv einschränkt, vor allem für kleine und mittelständische Unternehmen. Das könnte man etwa mit Klassen von Unternehmen machen, die man anhand der Zahl der Betroffenen – also beispielsweise ab 50.000, 100.000 oder 250.000 Betroffenen – definiert. Nur jene, die wirklich relevant genug sind, sollten dann auch alle Teile der DSGVO einhalten müssen. So macht man das ja auch bei anderen Gesetzen. Leider hat die Industrie stattdessen auf einen „risikobasierten Ansatz" gedrängt, der für alle Klassen von Unternehmen gleich ist. Die Großindustrie hat damit wohl gehofft, auch für die Multis etwas „Bewegungsspielraum" zu haben.

Die Bußgelder mit bis zu vier Prozent [des globalen Umsatzes der betroffenen Unternehmen] sind wichtig, weil es damit auch bei großen Konzernen eine ernsthafte Strafe gibt. Der Sockelbetrag von zwanzig Millionen Euro ist allerdings meiner Meinung nach viel zu hoch, weil dieser auch für ein Einpersonenunternehmen gilt. Hier hätten es wohl andere hohe Summen wie etwa 100.000 Euro auch getan.

Auch Meilensteine müssen reformiert werden

netzpolitik.org: *Die DSGVO ist im globalen Kontext ein Meilenstein für den Datenschutz. Allerdings ist sie keineswegs perfekt, hat Schlupflöcher und sollte nur der Anfang sein. Wie schätzt du die aktuelle politische Lage zum Datenschutz in Europa ein und was würdest du dir von der europäischen Politik wünschen?*

Max Schrems: Die DSGVO ist ein Meilenstein, aber sicher nicht das Ende am Weg zu einer sinnvollen Datenschutz-Regelung. Ich glaube, wir werden in ein paar Jahren eine „DSGVO 2"-Debatte haben. Das wäre eine Chance, Erfahrungen zu sammeln und das Gesetz klarer zu machen und Löcher zu stopfen.

In der Praxis würde das natürlich die Gefahr mit sich bringen, dass eine neue Debatte eher zum Gegenteil führt. Ich kann mir vorstellen, dass es entsprechend großen Widerstand geben wird, wenn die Debatte der letzten sieben Jahre nochmal geführt wer-

Leo Thüer

Leo Thüer hat Politikwissenschaft und Öffentliches Recht in Berlin studiert. Nach Zwischenstopps bei *La Quadrature du Net*, *Digitale Gesellschaft e. V.* und *Ligue des droits de l'homme* unterstützt er seit Mai die Redaktion von *netzpolitik.org* als Praktikant. Interesse an Netzneutralität, Plattformregulierung, Widerstand im Überwachungskapitalismus und mehr. Erreichbar unter *leo.thuer[ett]netzpolitik.org*. Ab und zu auf Twitter.

den soll. Nur weil die DSGVO nun gilt, ist das Thema Datenschutz nicht abgehakt. Ganz im Gegenteil, das zeigt der abstruse Widerstand der Industrie-Lobby gegen die aktuelle ePrivacy-Reform, die eigentlich gleichzeitig mit der DSGVO hätte in Kraft treten sollen.

netzpolitik.org: *Vielen Dank für das Gespräch!*

Quelle: https://netzpolitik.org/2018/datenschutz-a-la-friss-oder-stirb-max-schrems-reicht-beschwerde-gegen-datenkonzerne-ein/

Anmerkungen

1 *https://netzpolitik.org/tag/datenschutzgrundverordnung/*
2 *https://netzpolitik.org/2018/datenschutz-einmal-die-einwilligung-fuer-alles-bitte/*
3 *https://netzpolitik.org/tag/max-schrems/*
4 *https://netzpolitik.org/2018/schrems-gegen-facebook-eugh-wird-auch-privacy-shield-pruefen/*
5 *https://netzpolitik.org/2015/podcast-max-schrems-zum-ende-von-safe-harbor/*
6 *https://noyb.eu/?lang=de*

Alexander Fanta

Twitter und die Hauptstadtbullen: Darf die Polizei eigentlich Ironie?

Noch nie gab sich die Exekutive so cool wie heute: In sozialen Medien pfeffern die Beamten ihre Beiträge mit lockeren Sprüchen und ironischen Antworten. Dabei bewegen sich die Polizei-Influencer gelegentlich in einem rechtlichen und ethischen Graubereich.

Stella Schiffczyk / netzpolitik.org, CC BY-NC-SA 4.0

Auf dem Oktoberfest ist die Münchner Polizei so etwas wie die letzte Brandmauer gegen die Anarchie. Da gibt es Betrunkene, die in die Wiese pinkeln, Männer, die öffentlich masturbieren und ganze Gruppen von Lederhosenträgern, die sich wild raufen. Die Beamten nehmen die Sache mit Humor, schreiten ein, wo es nötig ist und verhelfen dem traditionellen Volksfest zum ordentlichen Ablauf. So zumindest versucht es die bayrische Polizei zu vermitteln, wenn sie unter dem Hashtag #WiesnWache von ihren Erlebnissen twittert.

Die Wiesenwache ist nur ein Beispiel für den neuen Kommunikationsstil der Polizei in den sozialen Medien. Lustig, frech und jugendlich wollen die Beamten wirken. Dabei treten sie bewusst unorthodox auf und nützen die Sprache der Internets für sich.

Die WiesnWache berichtet in lockerem Plauderton von ihren Erlebnissen und setzt dabei schon mal umgangssprachliche Kraftausdrücke ein.

Der lockere Stil sorgt für Beifall[1] und steigert die (ohnehin schon hohen) Beliebtheitswerte der Polizei[2]. Die mal mehr, mal weniger lustigen Äußerungen führen die Beamten aber auch in einen rechtlichen und moralischen Graubereich: Eigentlich sind die Gesetzeshüter in ihrer Kommunikation zur Neutralität und Sachlichkeit verpflichtet. Für Behörden war es bisher Tabu, sich über Menschen lustig zu machen, auch dann, wenn sie sich etwas zuschulden kommen lassen. Die Beamten müssen sich daher die Frage gefallen lassen: Darf die Polizei eigentlich Ironie?

„Mutti hat immer recht"

Auf Twitter wird das Gebot zur Aufklärung schnell in ein Gebot zur Schlagfertigkeit umgedeutet. Welche Strafe einem Jugendlichen beim Erwischtwerden mit ein bis fünf Gramm „Grass" drohe, fragte ein anonymer Nutzer 2016 die Frankfurter Polizei[3]. „Welches Buch", kalauerten die Beamten zurück.

Die Thüringer Polizei duzt unbekannte Twitter-Nutzer[4] bei pampigen Wortmeldungen, obwohl die Beamten damit laut einem Gutachten des Wissenschaftlichen Dienstes im Bundestag[5] in Gefahr laufen, eine Amtspflichtverletzung zu begehen, die zu Schadenersatzansprüchen führen kann. Auch wird recht salopp mit lästigen Zuschriften umgegangen: In einem Fall attestierten Thüringer Beamte einem Verbreiter von Verschwörungstheorien „Verdacht auf Belanglosigkeit"[6]. Einem Möchtegern-Rapper, der den Thüringer Beamten schreibt, seine Mutter drohe ihm Schläge an, wenn er weiter andere Frauen mit seiner Musik beleidigt, antwortet das Polizeikonto: „Mutti hat grundsätzlich immer recht"[7].

Von Bullen und Bürgern

Der flapsige Tonfall bleibt dabei den Beamten selbst vorbehalten. Zu Jahresanfang setzte die Berliner Polizei sich unter dem Hashtag #Hauptstadtbullen[8] in Szene. Polizeipräsident Klaus Kandt verteidigte[9] die kumpelhafte Sprache der eigenen Mitarbeiter in den sozialen Medien als Chance für die Rekrutierung: „Selbstverständlich darf die Polizei für sich werben. Alles andere wäre doch absurd." Das Recht auf saloppen Umgang gilt aber nicht für andere Twitter-Nutzer, hielten ihre Kollegen in Thüringen wenig später fest:

Mit ironischen Äußerungen riskiert die Polizei, direkt gegen ihre Verpflichtung zur wahrheitsgemäßen und korrekten Auskunft zu verstoßen. Der wissenschaftliche Dienst im Bundestag[10] betont, dass die Polizei auch über ihre Twitterkonten amtliche Auskünfte erteilt: Behörden sind also aufgrund ihrer Rechtsbindung verpflichtet, richtige Informationen zu geben und dürfen keine Unwahrheiten verbreiten.

Der heikle Umgang mit der Wahrheit

Das Gebot zu Sachlichkeit wird aber gelegentlich ignoriert, frei nach dem Motto: Lieber einen Freund verlieren, als auf eine Pointe zu verzichten. Die Satireseite Der Postillon verbreitete zuletzt[11], Notrufnummern würden ab 1. April kostenpflichtig werden. Ein Nutzer fragte daraufhin bei der Polizei Nordhessen nach:

Zwei Minuten später stellten die Beamten in einem weiteren Tweet klar, dass die Behauptung nicht ernstgemeint sei. Die Scherzbotschaft verbreitete sich in der Folgezeit in 46 Retweets und 539 Likes. Die Klarstellung erhielt 2 Likes. Am Tag darauf war bei den Verantwortlichen von tätiger Reue wenig zu merken:

Damit stellt die Polizei ihre eigene Professionalität in Frage. Egal wie weit hergeholt eine Aussage auch sein mag, ihre Verbreiter müssen auf offiziellen Kanälen davon ausgehen, dass sie ernstgenommen wird. Auf Twitter gelte der gleiche Anspruch wie für jegliche polizeiliche Öffentlichkeitsarbeit, sagt der Bochumer Kriminologe Tobias Singelnstein: „Über Tatverdächtige darf demnach nur äußerst zurückhaltend berichtet werden. Darüber hinaus sollte polizeiliche Öffentlichkeitsarbeit nicht nur sachlich richtig sein, sondern auch möglichst neutral, wertfrei und ausgewogen."

„Den Mechanismus bedienen"

Auf offizielle Anfrage hin sprechen Polizeiverantwortliche von einem Stilmittel. „Eine in angebrachten Momenten humorvolle Behörde schafft Bürgernähe und Bindung, die für eine dialogbasierte Kommunikation besonders in kritischen Situationen für beide Seiten immens wichtig ist", heißt es in einer Stellungnahme der Berliner Polizei an Netzpolitik.org.

Die Polizei München sieht in ihrem neuen Stil gar ein Gebot des Algorithmus. „Man kann sich täglich auf den Plattformen überzeugen, dass Social Media nur auf emotionaler Basis funktioniert", schreiben sie. Es sei daher notwendig, „in regelmäßigen, wohlausgewogenen Abständen bewusst diesen Mechanismus zu bedienen".

Alexander Fanta

Alexander Fanta ist seit Januar 2018 Journalist bei *Netzpolitik.org* und schreibt dort über die digitale Gesellschaft und ihre Feinde. 2017 beschäftigte er sich als Stipendiat am *Reuters-Institut* für Journalismusforschung in Oxford und bei der *NZZ* in Zürich mit Projekten zum Roboterjournalismus. Davor arbeitete Alexander für die österreichische Nachrichtenagentur APA.
Er ist unter *alexander.fanta ett Netzpolitik.org* und unter *@FantaAlexx* erreichbar.

Die Schwierigkeit der eigenen Arbeit auf Twitter ist der Polizei seit einiger Zeit bewusst, wie der in Frankfurt für Social Media zuständige Oberkommissar Andre Karsten im Vorjahr auf der re:publica deutlich machte[12]: „Da wäre es sehr schwierig, die nötige Ernsthaftigkeit zu vermitteln, wenn man die gesamte Woche zuvor nur Witze gemacht hat. Das ist schon ein krasser Drahtseilakt, der einem viel Fingerspitzengefühl abverlangt."

Humor ist eine Frage der Machtverhältnisse

Doch selbst mit viel Fingerspitzengefühl bleibt Humor eine Frage der Machtverhältnisse. Wer am längeren Ast sitzt, hat leicht lachen. Witzige Tweets mögen der Polizei höhere Beliebtheit und Zulauf bei der Rekrutierung verschaffen und vielleicht dabei helfen, öffentliches Bewusstsein für gesetzliche Normen zu schaffen. Aber was hat Humor generell mit dem gesetzlichen Auftrag der Polizei zu tun?

Öffentlich diskutiert worden ist die Frage, wie witzig die Polizei sein darf, bisher kaum. Sie wird damit aber nicht weniger relevant. Immer öfter sind nicht nur Polizeien in den sozialen Medien unterwegs, sondern auch einzelne Polizisten. Das führt den Kontakt zwischen Bürger und Polizei auf eine neue Ebene. Wenn einen erstmal der freundliche Beamte aus der Nachbarschaft über den digitalen Gartenzaun hinweg maßregelt, dann ändert sich bei so manchen womöglich die Einstellung zur twitternden Polizei.

Anmerkungen

1 *https://www.focus.de/digital/wiesnwache-oktoberfest-2017-die-witzigsten-tweets-der-wiesnwache_id_7631670.html*
2 *https://www.welt.de/politik/deutschland/article160905952/Das-Vertrauen-in-die-Polizei-ist-so-gross-wie-seit-20-Jahren-nicht.html*
3 *http://www.rp-online.de/digitales/gras-oder-grass-so-schlagfertig-antwortet-die-polizei-auf-twitter-aid-1.6127364*
4 *https://twitter.com/Polizei_Thuer/status/956837043308462080*
5 *http://meedia.de/2016/02/25/gutachten-zur-polizei-auf-twitter-wer-duzt-kann-schadensersatzansprueche-ausloesen/*
6 *https://twitter.com/Polizei_Thuer/status/963691011393323008*
7 *https://twitter.com/roli_994/status/957737541507174401*
8 *https://www.bz-berlin.de/berlin/hauptstadtbullen-naechster-fehltritt-des-social-media-teams-der-polizei*
9 *https://www.bz-berlin.de/berlin/polizei-auf-twitter-zu-kumpelhaft-polizeipraesident-bezieht-stellung*
10 *https://www.bundestag.de/blob/405538/c90e0606186c97afa-54b9694a865e026/wd-3-157-15-pdf-data.pdf*
11 *http://www.der-postillon.com/2016/02/ungeahntes-einnahmenpotenzial.html*
12 *http://www.spiegel.de/netzwelt/web/republica-2017-die-polizei-versucht-es-bei-twitter-und-co-mit-humor-a-1146147.html*

Quelle: https://netzpolitik.org/2018/twitter-und-die-hauptstadtbullen-darf-die-polizei-eigentlich-ironie/

Constanze Kurz

EU-weiter Zwang zur Abgabe von biometrischen Daten in Ausweisen

Innerhalb von zwei bis fünf Jahren sollen Papier-Ausweise ohne biometrische Daten in ganz Europa der Vergangenheit angehören. Das erklärte heute der EU-Innenkommissar Dimitris Avramopoulos: Digitale Gesichtsbilder und Fingerabdrücke sollen von allen Europäern ab zwölf Jahren eingesammelt werden.

Am Montag wurde bekannt, dass der EU-Innenkommissar Dimitris Avramopoulos für den heutigen Tag eine Pressekonferenz in Straßburg einberufen hatte, um neue Pläne zur biometrischen Erfassung aller Europäer zu erörtern. Das Schlagwort dazu ist im besten Neusprech „Sicherheitsunion", denn im Rahmen dieser Initiative wurde das Überwachungsvorhaben präsentiert. Gestern war bereits berichtet worden, dass der für Migration, Inneres und Bürgerschaft zuständige EU-Kommissar Avramopoulos eine halbe Milliarde Europäer dazu verpflichten will, ihre Fingerabdrücke abzugeben und digital in ihre Ausweise aufnehmen zu lassen. Für fast alle Bürger der EU-Mitgliedsstaaten besteht bereits eine Pflicht, einen Personalausweis zu besitzen.

Zu den Plänen der „Sicherheitsunion", die Avramopoulos, der Kommissar für die Sicherheitsunion Julian King und EU-Justizkommissarin Věra Jourová heute präsentierten[1] [2], gehören auch neue Regeln für Schusswaffen und Chemikalien, die für den Bombenbau verwendet werden können. Die Fingerabdruck-Biometrie gehört jedoch zum Teilbereich Fälschungssicherheit von Ausweisdokumenten („measures to prevent document fraud and the use of false identities"). Europol behauptete Anfang April beispielsweise, bei Terrorismus und Organisierter Kriminalität sei Dokumentenfälschung besonders bedeutsam. Belege dafür lieferte Europol allerdings nicht.[3]

EU-Innenkommissar Dimitris Avramopoulos
Quelle: Europäische Kommision

Deutsche Ausweisdokumente wird Europol wohl nicht gemeint haben, denn Zahlen der deutschen Bundesregierung[4] weisen in eine ganz andere Richtung: Demnach sind Personalausweise und Pässe von hoher Fälschungssicherheit und werden nur in sehr seltenen Fällen erfolgreich gefälscht. Weniger als einhundert Totalfälschungen innerhalb von sieben Jahren konnte die Bundespolizei ausmachen. Die Zahlen stammen aus der Zeit vor der Einführung der verpflichtenden Gesichtsbiometrie in hoheit-

lichen[5] Ausweisdokumenten, seitdem sollten die Fälschungen noch gesunken sein.

Die heute vorgestellten Pläne gehören zur „Sicherheitsunion", die von 2014 bis 2020 insgesamt 5,7 Milliarden Euro[6] verschlingen soll. Biometrische Vorhaben waren bereits Ende 2016 im Rahmen dieser „Sicherheitsunion"[7] vorgestellt worden: Avramopoulos kündigte damals für den Schengen-Raum die vermehrte Nutzung von Gesichtsbildern und Handabdrücken von Einreisenden an. Im letzten Jahr hatte der EU-Kommissar bei einem Besuch beim damaligen Innenminister Thomas de Maizière (CDU)[8] zusätzlich erklärt, europäische Informationssysteme, darunter auch das von 29 Staaten benutzte Schengener Informationssystem (SIS II) und die Fingerabdruckdatenbank Eurodac, besser verknüpfen zu wollen. Auch hier sind sensible Informationen betroffen, denn in den Informationssystemen sind auch biometrische Daten erfasst. Die heutige Ankündigung ist nun der nächste Schritt zu einer umfassenden Körperdatenerfassung aller europäischen Einwohner.

Biometrische Daten und Fingerabdrücke aller Europäer

Mit den neuen Plänen wolle man „Terroristen und Straftäter handlungsunfähig machen"[9] und gleichzeitig die „Sicherheit von Ausweisdokumenten" erhöhen und Dokumentenbetrug eindämmen.

Avramopoulos sagte in der Pressekonferenz, es solle in zwei Jahren in ganz Europa keine Papier-Ausweisdokumente mehr geben. Dass heute noch etwa neunzig Millionen EU-Bürger solche papiernen Ausweise benutzen, sei aus seiner Sicht nicht akzeptabel. In fünf Jahren soll jeder Europäer biometrische Daten und Fingerabdrücke auf elektronischen Ausweisdokumenten vorhalten.

Der Innenkommissar machte sich nicht die Mühe, zu erklären, wie die Abgabe der Fingerabdrücke aller Europäer die Sicherheit erhöhen könnte. Er begründete lediglich die eilige Umsetzung: „Terroristen ändern schnell die Strategie, wir wollen zeigen, dass wir schneller sind." Kein Krimineller solle sich mehr hinter einer *fake ID* (gefälschten Identität) verstecken können.

Er fügte noch an, dass die Mitgliedsstaaten keine einheitliche Ausweis-Produktion hätten, aber ein Nachweis der Identität notwendig sei. Man müsse die „Sicherheitspolitik rationalisieren". So reihte sich eine wenig aussagekräftige Phrase an die nächste. Auch der gleichzeitig veröffentlichte Bericht zur Umsetzung der „Sicherheitsunion"[10] enthält keine Zahlen dazu, wie viele Ausweis-Fälschungen es denn gibt und inwiefern die Biometrie bei der Fälschungssicherheit hilfreich sein könnte. Schließlich sind die digitalen Chips, auf denen die Biometriedaten gespeichert sind, mit Leichtigkeit zu deaktivieren. Die Ausweise bleiben dennoch gültig.

Auf die konkrete Nachfrage, ob denn ein Papier-Ausweis in Europa in zwei Jahren illegal wäre, gab Avramopoulos eine ausweichende Antwort: Italien benutze beispielsweise immer noch eine Papier-ID, das wolle er natürlich nicht verurteilen. Man wolle die papiernen Ausweise jedoch ersetzen. Die Mitgliedsstaaten müssten dem Inhaber einer ID-Karte vertrauen können. Dazu brauche man ein Minimum an „security features" (Sicherheitsmerkmalen). Dazu zählen offenbar aus Sicht des Innenkommissars auch biometrische Fingerabdrücke.

Avramopoulos schob eine Art versteckter Drohung hinterher: „Nur damit können wir Sicherheit und freien Personenverkehr gleichzeitig gewährleisten." Das könnte man so interpretieren, dass Mitgliedsstaaten, die sich den Vorschlägen verschließen, Einschränkungen in der Reisefreiheit für ihre Bürger hinnehmen müssten. Es solle eine „fünfjährige Auslaufperiode für vorherige Formate" geben, sagte der Kommissar. Das gelte für Karten, die nicht maschinenlesbar sind.

Folgende Maßnahmen zur Vereinheitlichung der europäischen Ausweisdokumente werden vorgeschlagen:

- **Verbindliche Einführung biometrischer Daten in Mitgliedstaaten, die Personalausweise ausgeben**: Die Personalausweise von EU-Bürgern (ab 12 Jahren) und die Aufenthaltstitel von Familienangehörigen aus Drittländern werden fortan biometrische Daten – Fingerabdrücke und Gesichtsbilder – enthalten, die auf einem Chip in der Karte gespeichert sind. Strengere Sicherheitsvorschriften werden regeln, wer auf die biometrischen Daten zugreifen kann.

- **Umsetzung eines ehrgeizigen Übergangsverfahrens**: Die neuen Regeln sehen vor, dass nicht konforme Ausweise relativ rasch aber schrittweise auslaufen, und zwar entweder mit Ablauf ihrer Gültigkeit oder spätestens innerhalb von fünf Jahren bzw. bei weniger sicheren (d. h. nicht maschinenlesbaren) Ausweisen innerhalb von zwei Jahren.

Constanze Kurz

Constanze Kurz ist promovierte Informatikerin, Autorin und Herausgeberin mehrerer Bücher[12], ihre Kolumne „Aus dem Maschinenraum"[13] erscheint im Feuilleton der FAZ. Sie ist Aktivistin[14] und ehrenamtlich Sprecherin[15] des Chaos Computer Clubs. Sie forschte an der Humboldt-Universität zu Berlin am Lehrstuhl „Informatik in Bildung und Gesellschaft" und war Sachverständige der Enquête-Kommission „Internet und digitale Gesellschaft" des Bundestags. Sie erhielt den Werner-Holtfort-Preis[16] für bürger- und menschenrechtliches Engagement[17], den Toleranz-Preis[18] für Zivilcourage und die Theodor-Heuss-Medaille für vorbildliches demokratisches Verhalten.

Avramopoulos wird am Donnerstag in Berlin erwartet. Ob er seinen heutigen[11] Aussagen noch etwas hinzuzufügen hat, bleibt abzuwarten.

Quelle: https://netzpolitik.org/2018/eu-weiter-zwang-zur-abgabe-von-biometrischen-daten-in-ausweisen/

Anmerkungen

1 *http://europa.eu/rapid/press-release_AGENDA-18-3379_en.htm*
2 *http://europa.eu/rapid/press-release_IP-18-3301_en.htm*
3 *https://twitter.com/Europol/status/981168214892716034*
4 *https://netzpolitik.org/2018/eu-kommission-plant-verpflichtende-fingerabdruecke-in-ausweisen/*
5 *https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03121/index_htm.html?nn=6615386*
6 *https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180417_security-union-a-europe-that-protects_en.pdf*
7 *http://www.statewatch.org/news/2016/dec/eu-com-sis-prel.pdf*
8 *https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2017/02/eu-kom-avramopoulos-zu-gast-im-bmi.html*
9 *http://europa.eu/rapid/press-release_IP-18-3301_de.htm*
10 *https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180317-progress-report-14-towards-effective-and-genuine-security-union_en.pdf, Seite 5*
11 *Der Artikel erschien am 17. April 2018.*
12 *http://gewissensbits.gi.de/constanze-kurz/*
13 *http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/*
14 *https://www.privacynotprism.org.uk/*
15 *https://www.youtube.com/watch?v=hj3gAsqrB18*
16 *https://de.wikipedia.org/wiki/Werner_Holtfort#Holtfort-Stiftung*
17 *https://media.ccc.de/search?q=Constanze+Kurz*
18 *http://www.ev-akademie-tutzing.de/toleranz-preis-fuer-christian-wulff-und-constanze-kurz/*

Constanze Kurz

Protest nicht nur in Bayern: Peter Schaar über den Widerstand gegen Polizeigesetze

Was uns als vermeintliche Verbesserung der Sicherheit verkauft wird, hält einer kritischen Prüfung oft nicht stand. Wir sprechen mit Peter Schaar über den Wettlauf um das härteste Polizeigesetz, die überfällige Protestwelle dagegen und warum in Bremen die Debatte um das Polizeigesetz anders verlief als in Bayern.

Der überraschend große Protest gegen das Polizeiaufgabengesetz in Bayern war Anlass für ein Gespräch mit Peter Schaar. Der ehemalige Bundesdatenschutzbeauftragte und Sachbuchautor hatte in seinem Buch „Trügerische Sicherheit“[1] analysiert, wie sich die Terrorangst auf grundlegende Bürger- und Freiheitsrechte auswirkt und wie intensive Grundrechtseingriffe durch die Große Koalition („GroKo“)[2] in der vergangenen Legislaturperiode damit gerechtfertigt wurden. Ob diese Gesetze tatsächlich für mehr Sicherheit sorgen, ist aber alles andere als bewiesen. Widerstand gegen diese Entwicklung regte sich in den letzten Jahren wenig, was sich nun zu ändern scheint: Anders als in Bayern wurde die Novellierung des Polizeigesetzes in Bremen nach Protesten vorerst gestoppt.

Wir sprachen mit Peter Schaar (Twitter: https://twitter.com/Peter_Schaar, Blog: https://www.eaid-berlin.de/?cat=34) über trügerische Sicherheit, Überwachung und symbolisches Handeln in der Politik. Schaar war für zwei Amtszeiten[3], also zehn Jahre, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und prägt bis heute öffentliche Debatten über Fragen der Privatsphäre. Er ist Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID)[4] in Berlin.

Die aktuellen Proteste: „Überfällig“

Constanze Kurz: *Herr Schaar, ich würde gern mit Ihnen über die aktuelle Stimmung in Sachen Datenschutz und Überwachung[5] reden. Wir haben das erste Mal seit der großen „Freiheit statt Angst“-Demo vor einigen Jahren wieder zehntausende Leute auf der Straße. Und Protest gibt es nicht nur in Bayern: In Bremen gab es wegen des bremischen Polizeigesetzes und des „Brementrojaners“ ebenfalls Widerstand. Wie bewerten Sie diese Stimmung, dass plötzlich wieder Protest aufkommt?*

Peter Schaar, Datenschützer und Buchautor.

Peter Schaar: Es ist überfällig, dass die Grundrechtseinschränkungen, die über die letzten Jahre scheibchenweise eingeführt worden sind, kritisiert werden. Wir sind an einen Punkt gelangt, wo sich Menschen fragen: Sind wir da nicht zu weit gegangen? Ist der Gesetzgeber wirklich auf dem richtigen Weg, wenn er immer mehr Überwachung erlaubt? Deshalb finde ich den Protest gut.

Das hängt auch damit zusammen, dass offensichtlich die bayerische Staatsregierung und die tragende CSU die Außenwirkung des neuen Gesetzes falsch kalkuliert haben. Man hat wohl vor, bestimmten populistischen Argumenten dadurch das Wasser abzugraben, dass man ihnen folgt und sie übernimmt.

Doch das klappt eben nicht mehr, und es ist offensichtlich eine hochgefährliche Strategie. Das haben sehr viele Menschen erkannt. Dagegen wenden sich mittlerweile selbst Vertreter der Polizei und der Polizeigewerkschaften. Das spätestens sollte eigentlich den Verantwortlichen zu denken geben, aber die bayerische Mehrheitspartei, die CSU, hat das Gesetz dennoch durchgezogen. Ich habe den Eindruck, das wird letztlich nicht dazu führen, dass sich damit die Wahlchancen und die Chancen auf eine neue absolute Mehrheit verbessern.

Im Wettlauf: „Wer macht das härteste Polizeigesetz?“

Constanze Kurz: *Es gab ja zuletzt noch eine stundenlange Landtagsdebatte in München. Die Argumentation der CSU gleicht dem, was Sie in Ihrem Buch „Trügerische Sicherheit“[6] herausgearbeitet hatten. Viele Argumente waren anekdotisch, man nimmt sich Einzelfälle, mit denen man Maßnahmen begründet, darunter auch solche, die gar nicht unbedingt ins Landespolizeirecht fallen. Die teilweise erfundenen Beispiele wirken aber oft sehr bedrückend, etwa ein Amoklauf unter Kindern, den ein CSU-Mann in der Landtagsdebatte anführte. Man zielt damit auf eine Emotion beim Zuhörer. Wie kann man dem argumentativ begegnen?*

Peter Schaar: Das Anekdotische ist im Grunde genommen ein Armutszeugnis für die Politik, wenn sie statistisch nachweisbare und nachvollziehbare Evidenz nicht liefert. Ich denke, man muss diese Beispiele trotzdem sehr genau prüfen, denn bei diesen Anekdoten ist ja vieles falsch. Kaum eine Maßnahme, die jetzt etwa in Bayern beschlossen worden ist, hätte irgendeine dieser Straftaten, die dort zur Begründung angeführt werden, verhindern können. Gerade wenn es um eine sehr schwerwiegende Gefährdung, wenn es um die Planung von schwersten Straftaten geht, sind schon diese Planungen strafbar. Insofern greifen hier auch schon die entsprechenden Befugnisse, die in der Strafprozessordnung enthalten sind. Dafür braucht es kein verschärftes Polizeirecht.

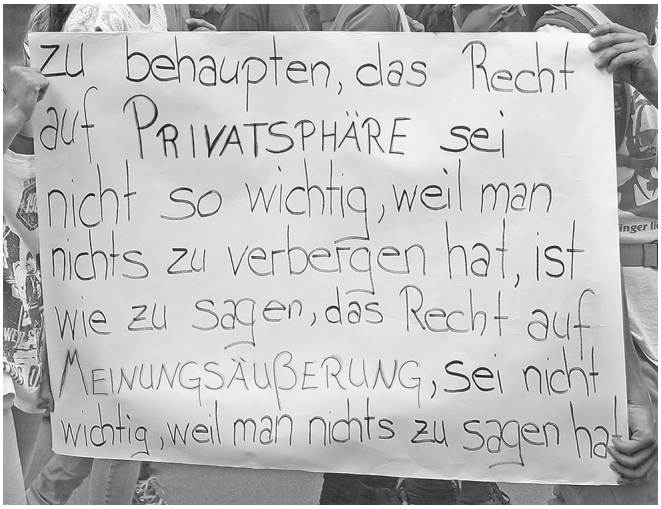
Es ist so, dass sich Bayern praktisch parallel zu dem, was auf Bundesebene beschlossen wird, einen Wettlauf liefert: Wer macht das härteste Polizeigesetz? Und im Ergebnis haben wir im Grunde freie Auswahl für die Sicherheitsbehörden. Sie können sich aussuchen: Wo sind gerade die weitergehenden Befugnisse, im Strafverfahrensrecht oder im Polizeirecht? Und das Polizeirecht ist ja im Vorfeld einer Straftat anwendbar. Dabei sind die Sicherungen, die dort enthalten sind, ein ganzes Stück geringer als bei Strafverfahrensrecht.

Constanze Kurz: *In Bayern drehte sich die Debatte viel um den Begriff der „drohenden Gefahr“. Viele erinnerten sich an den Begriff, weil beim Bundesverfassungsgericht um das BKA-Gesetz gestritten wurde. Was dabei auffiel – jenseits von den juristischen Details und was wirklich im Urteil zum BKA-Gesetz steht –, ist wieder dieses Muster, dass man scheibchenweise die polizeilichen Befugnisse hinausschiebt. Man kommt offenbar gar nicht mehr auf die Idee, dass man nicht maximal ausnutzt, was in den Urteilen aus Karlsruhe als Grenze gesetzt wurde. Wie kann man das wieder drehen, auch angesichts der abnehmenden Kriminalitätsentwicklung und der Aufklärungsquoten, die ja ausgesprochen positiv in Deutschland sind?*

Eindrücke von derm Protest in München gegen das PAG Freistaat statt Polizeistaat – Fotos: Günther Gerstenberg, CC BY

Peter Schaar: Zum einen denke ich, dass man die Maßnahmen im Zusammenhang sehen muss. Es ist zwar richtig, dass der Begriff der „drohenden Gefahr“ auch vom Bundesverfassungsgericht gebraucht wurde, aber in einem Kontext, der mit entsprechenden sehr schweren Straftaten im Zusammenhang steht. Außerdem sagt das Bundesverfassungsgericht auch in der Zusammenschau: Wenn die Überwachung überhand nimmt und zu einer kompletten Abbildung der Persönlichkeit führt oder aber zu einer umfassenderen Überwachung von völlig unverdächtigen Personen, dann ist der Gesetzgeber zu weit gegangen. Und diesen Eindruck habe ich in Bayern, dass man hier zu weit gegangen ist.

Ich bin mir ziemlich sicher, dass auch diese neuen Regelungen wieder vor dem Bundesverfassungsgericht landen. Und ich erwarte, dass das Bundesverfassungsgericht hier auch einiges wieder zurücknehmen wird. Aber generell wirkt immer noch das Phänomen: Wenn man die verschiedenen Gesetzesänderungen verteilt und die einzelnen Maßnahmen dann stückchenweise einführt, ist der Widerstand normalerweise nicht allzu groß. Das ist vielleicht der taktische Fehler gewesen in Bayern, dass man da alles reingepackt hat, was sich Sicherheitspolitiker in den letzten Jahren ausgedacht hatten. Vielleicht könnte man sich über ein solches nicht zu Ende gedachtes Verfahren sogar ein Stück weit freuen – aber mir fällt das angesichts der Wirkungen auf unsere Gesellschaft schwer.



Wer nichts zu verbergen hat, hat auch nichts zu sagen?

„Wenn ich nicht mehr weiter weiß, gründ‘ ich einen Arbeitskreis“

Constanze Kurz: *Hat Sie das eigentlich überrascht, der große Protest?*

Peter Schaar: Die Größe hat mich schon überrascht, ja. Aber es ist auch deutlich geworden, dass die bayerische Landesregierung und die CSU kein Jota zurückgewichen sind. Das war offenbar eine Frage der Gesichtswahrung. Wenn man sich etwas offener gezeigt hätte für die Kritik – und das muss man auch von Gesetzgebern erwarten –, dann wäre möglicherweise der Protest nicht so massiv ausgefallen.

Aber jetzt ist das Gesetz erstmal beschlossen worden. Ich finde es bezeichnend, dass jetzt gesagt wird, die Polizisten sollen dieses Gesetz in den Schulen[7] und in den Universitäten erklären. Eigentlich wäre es Aufgabe der Politik, das zu erklären.

Constanze Kurz: *Dazu ist auch eine „begleitende“ Kommission vom bayerischen Ministerpräsidenten angekündigt worden.*

Peter Schaar: Ja, „Wenn ich nicht mehr weiter weiß, gründ‘ ich einen Arbeitskreis“, heißt es. Und hier scheint man diesen Satz mit Leben zu füllen.

„Das ist symbolisches Handeln“

Constanze Kurz: *Es gibt auch in Nordrhein-Westfalen und Niedersachsen gegen die Polizeigesetze Proteste und ebenso in Bremen. In Bremen drehte sich die Debatte vor allem um den Brementrojaner, also das staatliche Hacken von Computern, und unter welchen Umständen das möglich sein soll. Wie bewerten Sie die politische Situation und dass die Regierung in Bremen einen anderen Weg gegangen ist und das Vorhaben gestoppt hat?*[8]

Peter Schaar: Bisher gab es nur einen Referentenentwurf, der ist nicht offiziell bekanntgegeben worden – bis heute. Insofern fällt die Bewertung natürlich schwer. Aber richtig ist, dass das Vorhaben in Bremen nicht durchgezogen worden ist, sondern dass das Thema auch in der Regierung – in dem Falle durch die Grünen – kritisch reflektiert wird. Auch in der SPD gibt es offensichtlich Politiker, denen dieser Referentenentwurf zu weit geht. Man muss auch hier die Frage beantworten: Wozu braucht die Polizei präventiv-polizeiliche Befugnisse zum Einschleusen von Trojanern, also von entsprechender Spionagesoftware, in technische Geräte? Wenn es wirklich um Terrorismusabwehr geht, dann reicht das Strafrecht vollständig aus. Da muss ich sagen: Ich kann die bisher vertretene Linie des Innensenators nicht verstehen. Aber ich finde es erstmal gut, dass es diese Diskussion in Bremen gibt.

Kritisch sehe ich auch die Ausweitung der Videoüberwachung, die in Bremen wie auch andernorts begründet wird mit der Terrorgefahr. Wenn man sich die bekanntgewordenen Regelungen anschaut, stellt man fest, dass auch die Bremer Regelung sehr weitgehend ist. Die Bremer Polizei darf heute schon an Kriminalitätsschwerpunkten videoüberwachen. In Zukunft soll sie überall dort videoüberwachen können, wo sich viele Menschen aufhalten. Nun halten sich in Bremen – das ist schließlich eine Großstadt – an vielen Orten viele Menschen auf, im Grunde genommen im gesamten Innenstadtbereich.

Nach dieser neuen Bestimmung, wenn sie denn beschlossen werden sollte, würde das einer flächendeckenden Überwachung ganzer Stadtviertel das Wort reden. Das hielte ich für unverhältnismäßig. Und ich verstehe auch nicht, wieso die Bremer Innenbehörde vorschlägt, die Videoüberwachungsbefugnisse auszuweiten, wenn heute nicht mal dort überwacht wird, wo Kriminalitätsschwerpunkte sind. Das ist wieder ein typisches Muster, dass man die Gesetzgebungsmaschine anwirft, aber wenn man dann genauer hinschaut, entsteht der Eindruck: Das ist symbolisches Handeln, das in erster Linie dazu dient, deutlich zu machen, dass man ja irgendetwas unternimmt.

Constanze Kurz: *Trügerische Sicherheit, sozusagen.*

Peter Schaar: Das ist nur eine vermeintliche Verbesserung der Sicherheit, und in Wirklichkeit geht es eher darum, das eigene Image aufzubessern. Dafür sind unsere Bürgerrechte zu wertvoll, dass man sie solchem Kalkül opfert.

Constanze Kurz: *Vielen Dank für das Gespräch!*

Quelle: https://netzpolitik.org/2018/protest-nicht-nur-in-bayern-peter-schaar-ueber-den-widerstand-gegen-polizeigesetze/

Anmerkungen

1 *https://netzpolitik.org/2017/truegerische-sicherheit-peter-schaars-rundumschlag-in-einem-buch/*
2 *https://netzpolitik.org/2017/zwei-schritte-vor-keinen-zurueck-ueberwachungsausbau-in-der-grossen-koalition/*
3 *https://netzpolitik.org/2008/union-schlaegt-peter-schaar-fuer-zweite-amtszeit-vor/*
4 *https://www.eaid-berlin.de/*
5 *https://netzpolitik.org/category/ueberwachung/*
6 *https://www.swr.de/swr2/kultur-info/peter-schaar-buch-truegerische-sicherheit/-/id=9597116/did=20268206/nid=9597116/18ezmpl/index.html*
7 *https://www.br.de/nachrichten/lehrer-lehnen-pag-aufklaerung-an-schulen-ab-100.html*
8 *https://netzpolitik.org/2018/nach-kritik-verschaerfung-des-polizeigesetzes-in-bremen-auf-eis-gelegt/*

Fronttransparent

Stefan Hügel

„Ich möchte nicht in einer Welt leben,
in der alles, was ich tue und sage, aufgezeichnet wird.
Solche Bedingungen bin ich weder bereit zu unterstützen,
noch will ich unter solchen leben."

Edward Snowden

5 Jahre Snowden-Enthüllungen

Geheimdienstliche Ausspähung – Sargnagel der freiheitlichen Gesellschaft

Mitte 2013 waren gerade die Arbeiten der Enquête-Kommission *Internet und digitale Gesellschaft* zum Abschluss gekommen. In der Ausgabe 2/2013 hatten wir dieser Kommission einen umfassenden Schwerpunkt gewidmet. Das Heft war bereits fertig, da erreichten uns die ersten Nachrichten über die umfassende Überwachung des gesamten weltweiten Datenverkehrs im Internet durch die US-amerikanische *National Security Agency* (NSA). Ein wenig verstört ergänzten wir das Heft beim Inhaltsverzeichnis um einen kurzen Hinweis:

> *„Der Redaktionsschluss dieses Hefts lag vor dem Zeitpunkt, zu dem das Projekt PRISM öffentlich bekannt wurde. Mit dieser Kenntnis wären einzelne Bewertungen möglicherweise anders ausgefallen."*[1]

Der Vorsitzende der Kommission und alle Obleute der Bundestagsfraktionen hatten – ebenso wie einige Sachverständige – Beiträge zu der Ausgabe geleistet. Doch mir erschien das gerade fertig gestellte Heft, auf das ich so stolz gewesen war, plötzlich als ziemlich wertlos, ging es darin ja gerade darum, wie wir das Internet der Zukunft positiv gestalten können. Aus heutiger Sicht fällt auf, dass das Thema der geheimdienstlichen und militärischen Überwachung in der Enquête-Kommission praktisch keine Rolle gespielt hat. Überhaupt sind ihre auf rund 2.000 Seiten festgehaltenen Ergebnisse (leider) weitgehend in Vergessenheit geraten.

Im folgenden Heft 3/2013 widmeten wir dann den immer weiter gehenden Enthüllungen einen eigenen Schwerpunkt. Im *Brief an das FIfF*[2] war zu lesen:

> *„… Es war der Tag*[3]*, an dem wir einer Illusion beraubt wurden: der Illusion der freien Kommunikation im Internet als eines Grundbausteins der freiheitlichen Demokratie.*
>
> *Am 6. Juni 2013 wurden erstmals Unterlagen veröffentlicht, die auf eine umfassende Überwachung der Bevölkerung durch den US-amerikanischen Geheimdienst NSA – die National Security Agency – hinweisen. In den folgenden Wochen wurden immer weitere Enthüllungen öffentlich – über die Ausspähung durch die NSA, durch den britischen Geheimdienst GCHQ, zuletzt gab es Berichte über eine intensive Zusammenarbeit mit dem deutschen Bundesnachrichtendienst. Auch die anfänglichen Beteuerungen, die Überwachung würde sich im Rahmen des geltenden Rechts bewegen, wurden zunehmend angezweifelt. Was wäre das aber auch für ein Recht, das eine solche umfassende Ausspähung zulässt?*
>
> *Die Reaktionen der verantwortlichen Bundesregierung waren auffällig verhalten. Artig fragte man bei den USA an, ob sie denn wohl deutsches Recht gebrochen hätten. Auf weitere Nachfragen erklärten Regierungsvertreter, sie wüssten von nichts. Am Ende wurde das Thema noch zum Wahlkampftheater*[4]*, bevor Kanzleramtsminister Ronald Pofalla die Affäre kurzerhand für beendet erklärte.*

Davor, dass Geheimdienste zu solchen Mitteln greifen, hatten ExpertInnen immer wieder gewarnt. Wir wussten seit 2001 von Echelon, in Bad Aibling, und gerade hatte der Historiker Josef Foschepoth die Überwachung des Post- und Telekommunikationsverkehrs in Deutschland seit dem 2. Weltkrieg in einer umfassenden, auf Originalquellen basierenden Studie[5] dokumentiert – viele hielten es dennoch damals nicht für möglich, dass eine Überwachung in einem solchen monströsen Ausmaß stattfindet. „Verschwörungstheorien!" hieß es davor häufig; eine auch heute gern genommene Methode, unerwünschte Ansichten zu diskreditieren[6]. Die Enthüllungen von Edward Snowden, deren Validität wohl nicht mehr in Zweifel gezogen wird, hast uns eines klar gemacht: Die Ausspähung existiert und wird immer weiter verfeinert.

Konsequenzen

Glenn Greenwald schreibt in seinem Buch über die durch Edward Snowden bekannt gemachte Überwachung:

> *„Bei unserem allerersten Kontakt sagte Edward Snowden, er fürchte nur eines, wenn er an die Öffentlichkeit gehe: dass seine Enthüllungen mit Gleichgültigkeit und Desinteresse aufgenommen würden und er dann sein altes Leben umsonst aufgegeben und für nichts eine Haftstrafe riskiert hätte."*[7]

Es ist wohl nicht mehr zu bestreiten, auch wenn die Diskussion über die Enthüllungen von Edward Snowden, 5 Jahre danach, weitgehend abgeebbt ist: Zweifellos hat er vieles bewegt, seine Befürchtungen hinsichtlich Gleichgültigkeit und Desinteresse haben sich nicht bewahrheitet.[8] Das Bewusstsein für IT-Sicherheit[9] und Datenschutz hat zugenommen. Verschlüsselung wird zur Selbstverständlichkeit. Man darf annehmen, dass sich die Snowden-Enthüllungen auch positiv auf die Debatten um die europäische Datenschutz-Grundverordnung ausgewirkt haben, die trotz erbittertem Widerstand der Profiteure des weltweiten Datenhandels ebenfalls in diesen Tagen in Kraft getreten ist.[10]

Doch andererseits können wir naiv fragen: Kann es denn sein, dass wir uns, unsere Grundrechte, gegen unseren eigenen Staat, den Staat den wir beauftragt haben, unsere Interessen wahrzunehmen, durch Verschlüsselung und weitere Maßnahmen der IT-Sicherheit schützen müssen? Ich erwarte von meinem Staat, dass er mir die Einhaltung der verfassungsrechtlichen Grundrechte garantiert. Der demokratische, freiheitliche Staat darf keine Institution sein oder betreiben, gegen den ich mich verteidigen muss, damit meine Grundrechte gewährleistet sind.

Edward Snowdens Handeln gilt heute vielen als bespielhaft; mehrere Bürgerrechtspreise wurden ihm verliehen. Stellvertretend seien hier genannt der Fritz-Bauer-Preis der Humanistischen Union 2014[11] und der Internationale Whistleblower-Preis 2013[12]; vergeben von Transparency International, der International Association of Lawyers against Nuclear Arms (IALANA) und der Vereinigung Deutscher Wissenschaftler.

In Deutschland wurde die Überwachung in einem Untersuchungsausschuss aufgearbeitet, der in seinem umfangreichen Bericht vieles ans Licht gebracht hat. Doch bereits über dessen Ergebnisse herrscht Uneinigkeit. In ihrem umfassenden Sondervotum kommt die Opposition zu anderen Ergebnissen als die VertreterInnen der Regierungsfraktionen – dieses wurde zunächst nicht veröffentlicht, da es aus Sicht des Vorsitzenden als geheim eingestufte Inhalte enthielt. Auf dem Abschlussbericht[13], der dem Deutschen Bundestag vorgelegt wurde, fehlen die Namen der Obleute der Oppositionsfraktionen, Konstantin von Notz (Bündnis 90/Die Grünen) und Martina Renner (Die Linke) – sie wurden vom Vorsitzenden des Ausschusses, Patrick Sensburg, kurzerhand ihrer Funktion enthoben. Sensburg selbst hatte allerdings, Wochen vor der Veröffentlichung des Abschlussberichts, in einer Buchpublikation[14] seine Sicht der Dinge dargestellt. Allein dieser Vorfall zeigt, in welchem Ausmaß es hier um die Deutungshoheit ging – aber Deutungshoheit in wessen Interesse und in wessen Sinn?

Snowden lebt immer noch im Exil in Russland; in seiner Heimat USA erwartet ihn wohl mindestens eine langjährige Haftstrafe. Aktuelle Gesetzgebungsinitiativen verstärken die geheimdienstliche Überwachung. Nur ein Beispiel unter vielen ist der sogenannte „Hessentrojaner", mit dem in Hessen von CDU und Bündnis 90/Die Grünen weitgehende Befugnisse für den Verfassungsschutz festgeschrieben werden sollen. In anderen Bundesländern ist die Debatte über entsprechende Landesgesetze voll entbrannt, so beispielweise in Bayern. In Bremen wurden entsprechende Initiativen (vorläufig?) auf Eis gelegt.

Wie schwierig es ist, gegen die geheimdienstliche Überwachung vorzugehen, zeigt gerade wieder der gescheiterte Versuch der Betreiberunternehmens des weltweit größten Internet-Knotens DE-CIX in Frankfurt am Main, die Ausleitung des Internetverkehrs an den BND vor dem Bundesverwaltungsgericht anzugreifen. Es überrascht dann auch nicht mehr, wenn auch der Untersuchungsausschuss Ziel geheimdienstlicher Spionage gewesen sein sollte: Offenbar hat der als Spion der CIA verhaftete BND-Beamte Markus R. auch über den NSA-Untersuchungsausschuss Bericht erstattet.

All das lässt die Frage aufkommen: Haben wir es hier „nur" mit unterschiedlichen politischen Sichtweisen der Bürgerrechte – Freiheit vs. Sicherheit – zwischen politischen Parteien mit unterschiedlichen Wertvorstellungen zu tun, oder mit der Stabilität und Macht von (Sicherheits-) Behörden, die schon längst in der Lage sind, sich jeglicher demokratischen Kontrolle zu entziehen?

Mit unserer umfangreichen Retrospektive anlässlich des 5. Jahrestags der Enthüllungen von Edward Snowden laden wir dazu ein, über solche Fragen zu reflektieren. Dazu haben wir drei Beiträge von 2013 zusammengestellt, mit denen damals über die Ereignisse berichtet und sie kommentiert wurden:

- von **Andre Meister** (*netzpolitik.org*) stammt der erste Bericht, in dem er damals über die ersten Informationen über PRISM berichtete, dem Programm zur Ausspähung von Personen innerhalb und außerhalb der USA, die digital kommunizieren und an dem unter anderen offenbar die größten Internetkonzerne wie Microsoft, Google, Facebook, Yahoo, Apple und AOL beteiligt waren,

- **Sara Stadler** hatte eine Chronologie der Ereignisse auf Basis von Berichten unterschiedlicher Medien zusammengestellt, die den Fortgang der Ereignisse nach den Enthüllungen illustrieren und die wir ebenfalls hier wiederholen,

- **Klaus Fuchs-Kittowski** stellte die Frage nach ethischem Handeln in der Informatik und der Rolle von Whistleblowern wie Edward Snowden.

Insgesamt wollen wir mit dieser Retrospektive dazu einladen, die Ereignisse und Enthüllungen der letzten fünf Jahre zu reflektieren. Hatten sie die richtigen Konsequenzen? Haben die Enthüllungen zu einem bürgerrechtlichen Fortschritt geführt? Welches Gewicht hat die freie und unbeobachtete Kommunikation als Bürgerrecht – auch angesichts terroristischer Bedrohung? Und was ist auf dem Weg zu einer freiheitlichen Gesellschaft noch zu tun?

Manche haben die Veröffentlichungen von Edward Snowden schockiert, manchen erschienen sie unerfreulich aber nicht überraschend, manche hielten sie für eine Gefährung der öffentlichen Sicherheit, gar für Verrat. In den vergangenen fünf Jahren sind rechtspopulistische und autoritäre Parteien und Regierungen weltweit auf dem Vormarsch. Welchen Nutzen ziehen sie aus der geheimdienstlichen Überwachung? Wie würden sie deren Arbeit bewerten. Damals hatten wir Erich Mielke zitiert, der sich und die Tätigkeit der Staatssicherheit 1989 rechtfertigte:

> *„Ich liebe – Ich liebe doch alle – alle Menschen – Na ich liebe doch – Ich setze mich doch dafür ein."*

Wollen wir auf diese Weise „geliebt" werden?

Anmerkungen

1 *FIfF-Kommunikation 2/2013, S. 2*

2 *Der Traum ist aus. Brief an das FIfF, FIfF-Kommunikation 3/2013, S. 5–6*

3 *Der 6. Juni 2013, der Tag, an dem die Berichte über das Projekt PRISM öffentlich wurden. Zuvor war bereits bekannt geworden, dass in den USA der Telefonanbieter Verizon ausgespäht worden war.*

4 *Wir erinnern uns: Damals standen die Bundestagswahlen 2013 unmittelbar bevor.*

5 *Josef Foschepoth (2012): Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik. Göttingen und Bristol CT USA: Vandenhoeck & Ruprecht. Der Band kann auch über die Bundeszentrale für politische Bildung bezogen werden.*

6 *Dem Autor ist sehr bewusst, dass häufig haarsträubender Unsinn verbreitet und völlig zu Recht als „Verschwörungstheorie" verworfen wird. Offenbar ist es aber nicht immer einfach, zu unterscheiden. Dafür bedarf es der Medienkompetenz: Die Fähigkeit, Nachrichten kritisch zu beurteilen (und sich dabei auch nicht vom eigenen Weltbild täuschen zu lassen), ist wohl eine der wichtigsten Qualifikationen der digitalen Gesellschaft. Dies hat auch die Enquête-Kommission festgestellt.*

7 *Glenn Greenwald (2014): Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. München: Droemer-Verlag*

8 *Zu einer ernüchternden Einschätzung kommt dagegen Daniel Leisegang: Er stellt fest, „... dass die politische und juristische Aufarbeitung des Abhörskandals hierzulande keine nennenswerten Konsequenzen zeitigte. Im Gegenteil hat die Macht des BND in den vergangenen Jahren erheblich zugenommen. [...] Dafür verantwortlich ist vor allem das dramatische Versagen der parlamentarischen Kontrolle. Sie hat die massenhafte Ausspähung weder im Vorfeld verhindert noch im Nachhinein aufgeklärt." Daniel Leisegang (2018): Fünf Jahre NSA-Affäre: Die neue Macht des BND. Blätter für deutsche und internationale Politik 6'18, S. 21–24*

9 *Wobei IT-Sicherheit, gerade im Zusammenhang mit Edward Snowden, differenziert betrachtet werden muss: Bob Toxen hat darauf hingewiesen, dass wir die Snowden-Enthüllungen möglicherweise gerade mangelnder IT-Sicherheit bei der NSA zu verdanken haben: Bob Toxen (2014): The NSA and Snowden: Securing the All-Seeing Eye. How good security at the NSA could have stopped him. Communications of the ACM Vol. 57 No. 5*

10 *Freilich gibt es auch berechtigte Kritik an der Datenschutz-Grundverordnung; stellvertretend Alexander Roßnagel (2018): Datenschutz-Grundverordnung – was bewirkt sie für den Datenschutz? in: vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik #211/212 (1/2–2018) S. 17–29 und in diesem Heft, S. 15–21*

11 *Informationen dazu unter http://www.humanistische-union.de/veranstaltungen/buergerrechtspreise/fritz_bauer_preis/2014/. Auch die Verleihung des Fritz-Bauer-Preises 2018 an Hans-Christian Ströbele steht in dieser Tradition, nachdem seine politische Arbeit auch stets der Kontrolle von Geheimdiensten gewidmet war, er im NSA-Untersuchungsausschuss (als stellvertretendes Mitglied) mitgewirkt hat und er ein persönliches Treffen mit Edward Snowden in Moskau arrangiert hat, nachdem der Untersuchungsausschuss zu einer Vernehmung als Zeuge nicht in der Lage war.*

12 *https://vdw-ev.de/wp-content/uploads/2016/02/Begruendung-der-Jury-Whistleblowerpreis-2013-Edward-Snowden.pdf*

13 *Deutscher Bundestag, 18. Wahlperiode (2017): Beschlussempfehlung und Bericht des 1. Untersuchungsausschusses gemäß Artikel 44 des Grundgesetzes. BT-Drs. 18/12850, http://dip21.bundestag.de/dip21/btd/18/128/1812850.pdf*

14 *Patrick Sensburg, Armin Fuhrer (2017): Unter Freunden. Die NSA, der BND und unsere Handys - wurden wir alle getäuscht? Kulmbach: Plassen-Verlag*

Andre Meister, netzpolitik.org

PRISM: Amerikanischer Geheimdienst NSA hat direkten Zugriff auf alle Daten der großen Internet-Unternehmen

Der amerikanische Militärnachrichtendienst NSA hat direkten Zugriff auf alle Daten der großen amerikanischen Internet-Unternehmen. Das geht aus einer Präsentation seiner eigenen Abteilung „Special Source Operations" hervor, die auszugsweise veröffentlicht wurde. Damit festigt die NSA einmal mehr ihren Ruf als größter Datenstaubsauger der Welt, der Daten in kaum vorstellbarem Ausmaß sammelt.

Nach dem Scoop[1] über das Absaugen der Vorratsdaten beim amerikanischen Telekommunikationsanbieter Verizon legt Glenn Greenwald noch einen drauf. Wieder beim britischen Guardian[2] zitiert er aus einer nur zwei Monate alten, 41-seitigen Powerpoint-Präsentation, dessen Authentizität der Guardian laut eigenen Angaben verifiziert hat.

In diesem „streng geheimen" Dokument gibt der amerikanische Nachrichtendienst National Security Agency (NSA) zu, „direkten Zugriff auf die Systeme" von neun der größten amerikanischen Internet-Firmen zu haben, um so ziemlich alle anfallenden Daten „direkt von den Servern" abzuschnorcheln (Abbildung 1).

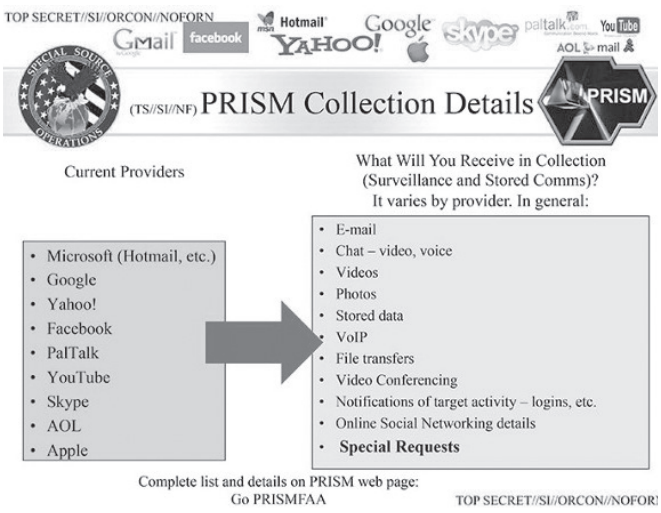


Abbildung 1: PRISM Collection Details

Damit ist endlich offiziell, was Interessierten schon lange klar ist: Die NSA hat direkten Zugriff auf **alle** Daten der großen amerikanischen Internet-Dienste. Nicht „nur" Metadaten, sondern alle Inhalte, egal ob E-Mails, Chats (Video, Voice, Text), Fotos, Videos, Direktnachrichten, Dateien, Nachrichten oder Skype-Gespräche. Alles.

> *The program facilitates extensive, in-depth surveillance on live communications and stored information.*

All diese Daten dürften in eigene Rechenzentren wie das monströse NSA-Spionage-Center[4] in Utah fließen, für immer gespeichert und permanent gerastert werden. Die Behörde selbst lobt das Programm als „einen der wertvollsten, einzigartigen und produktiven Zugriffe für die NSA".

Microsoft ist demnach seit 11. September 2007 dabei, Apple „erst" seit Oktober 2012 (Abbildung 2).

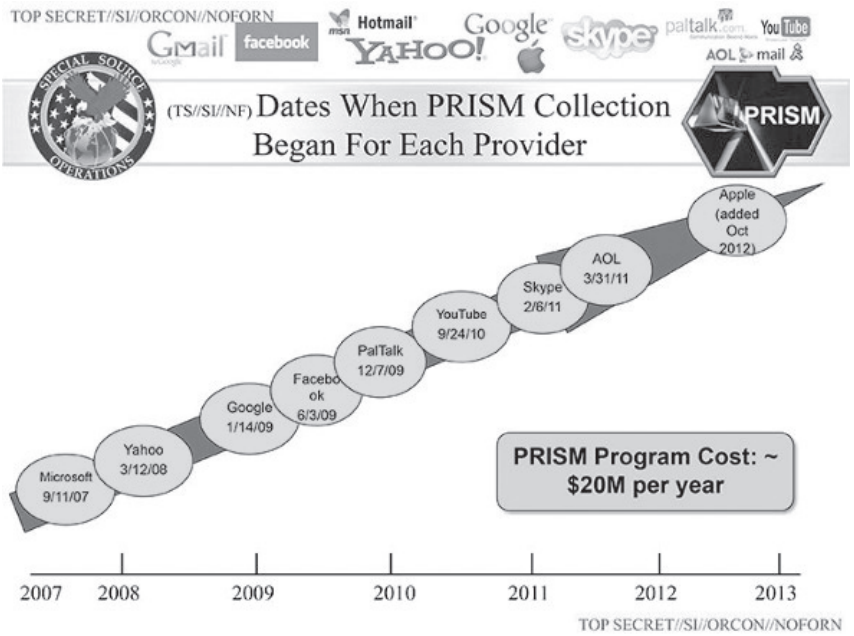


Abbildung 2: Dates when PRISM Collection began for each Provider

Möglich wird das durch den Foreign Intelligence Surveillance Act[5] (FISA), der nach 2001 immer wieder erweitert wurde, unter anderem durch den FISA Amendments Act von 2008[6]. Und auch von der Obama-Regierung wurde er immer wieder verlängert. Schon bei der Verabschiedung warnten Kongress-Abgeordnete, dass die amerikanische Öffentlichkeit schockiert sein würde, wenn sie erfahren würde, wie weit die Überwachung der Geheimdienste wirklich geht.

Die NSA, eigentlich Teil des Militärs, hat laut dem Dokument die „Unterstützung von Kommunikations-Anbietern in den USA". Die genannten Firmen streiten alles ab[7]. Ein hoher Beamter sagte dem Guardian jedoch[8]:

> *Die Informationen, die im Rahmen dieses Programms gesammelt werden, zählen zu den wichtigsten und wertvollsten nachrichtendienstlichen Informationen, die wir sammeln und werden verwendet, um unserer Land von einer Vielzahl an Bedrohungen zu schützen.*

America, fuck yeah![9]

Quelle: https://netzpolitik.org/2013/prism-amerikanischer-geheimdienst-nsa-hat-direkten-zugriff-auf-alle-daten-der-grosen-internet-unternehmen/, 7. Juni 2013, letzte Änderung 29. August 2017. Wir danken dem Autor für die Genehmigung zum Abdruck.

Anmerkungen

1 *https://netzpolitik.org/2013/us-geheimdienst-nsa-der-geheimen-vorratsdatenspeicherung-uberfuhrt/*
2 *http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data*
3 *http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/*
4 *https://netzpolitik.org/2012/wired-reportage-uber-neues-nsa-spionage-center/*
5 *https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act*
6 *https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978_Amendments_Act_of_2008*
7 *http://www.guardian.co.uk/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining*
8 *http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data*
9 *https://www.youtube.com/watch?v=IhnUgAaea4M*
10 *https://www.netzpolitik.org/wp-upload/Master-Meister-Zugangserschwerungsgesetz.pdf*
11 *https://fragdenstaat.de/profil/a.meister/*
12 *https://netzpolitik.org/2015/verdacht-des-landesverrats-generalbundesanwalt-ermittelt-doch-auch-gegen-uns-nicht-nur-unsere-quellen/*

Andre Meister

Andre Meister ist schon lange bei *netzpolitik.org*, seit 2012 auch als festangestellter Redakteur. Er hat einen Master in Sozialwissenschaften[10], ist Mitgründer der Vereine *Digitale Gesellschaft*, *Gesellschaft für Freiheitsrechte* und *netzpolitik.org* sowie Mitglied im *Chaos Computer Club* und Beobachter bei *European Digital Rights*. Außerdem arbeitet er als System-Administrator, so hat er u. a. den Mail-Server von *Frag Den Staat*[11] aufgesetzt und nutzt ihn gerne. Und irgendwas mit Landesverrat[12].

Sara Stadler

Telefon- und Internetüberwachung

Chronologie der Enthüllungen

Seit mehr als 2 Monaten nimmt der Skandal um die Internetüberwachung unter anderem durch US-amerikanische und europäische Geheimdienste einen zentralen Platz in den täglichen Nachrichten ein. Beinahe jeden Tag wird eine neue Enthüllung präsentiert und oft empören sich die selben sogleich über die NSA, die am nächsten Tag die Notwendigkeit vergleichbarer Überwachungsmaßnahmen in der EU, wie der Vorratsdatenspeicherung, unterstreichen. Die Fülle der Ereignisse und Berichte ist uns eine detaillierte Übersicht wert.

Juni 2013

6. Juni 2013: Die britische Zeitung *The Guardian* berichtet, dass der US-Geheimdienst NSA Telefondaten von Millionen US-EinwohnerInnen sammele. Einem streng geheimen Gerichtsbeschluss zufolge müsse der Telefonanbieter Verizon Informationen wie Rufnummern, Standort und Dauer bezüglich aller Telefonate innerhalb der USA und von dort aus ins Ausland an den Geheimdienst weitergeben (Quelle: Heise, The Guardian).

7. Juni 2013: Die Berichte über die Spionageaktionen der US-Geheimdienste weiten sich aus. Laut dem *Wall Street Journal* sammelt die NSA neben den Telefondaten von Verizon auch jene der Kunden von AT&T und Sprint Nextel, sowie Metadaten über E-Mails, Internetsuchen und Kreditkartenzahlungen.

Der Guardian berichtet, dass NSA und FBI seit 2007 im Rahmen des streng geheimen Programms PRISM die zentralen Rechner von Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube und Apple anzapfe und damit Zugriff auf alle dort gesammelten Daten, wie Fotos, Emails, Dokumente oder Kontaktdaten erhalte. Dass dies mit ihrer Genehmigung erfolge, bestreiten die genannten Unternehmen. US-Präsident Barack Obama rechtfertigt die Telefon- und Internetüberwachung durch seine Regierung als Mittel zur Terrorismusbekämpfung.

Am selben Tag berichtet der Guardian, dass auch der britische Geheimdienst GCHQ seit 2010 von dem Netzspionage-Programm PRISM profitiere und insgesamt 197 Berichte auf Grundlage der so gewonnen Daten erstellt habe. Diese könnten über ein gesondertes Programm abgegriffen werden, das speziell für den GCHQ eingerichtet worden sei. Wie lange und unter wessen Mitwisserschaft auf PRISM zugegriffen wurde, bleibe unklar (Quelle: The Guardian, Heise, Wall Street Journal).

8. Juni 2013: Der 29-jährige Techniker Edward Snowden bekennt sich in einem Videointerview mit dem Guardian öffentlich, die Quelle der Enthüllungen um das US-Spionageprogramm PRISM gewesen zu sein. Während die US-Regierung das ausufernde Sammeln von Daten leugnet und PRISM lediglich als ein internes Computersystem zur legalen Datensammlung darstellt, spricht Snowden, der als Mitarbeiter externer Unternehmen für den Geheimdienst tätig war, von einer „*infrastructure that allows it to intercept almost everything*" (dt: „Infrastruktur, die es erlaubt, fast alles abzufangen") (Quelle: The Guardian, Heise).

12. Juni 2013: Aus Kanada wird bekannt gegeben, dass dort ebenfalls seit Jahren eine massive Telefon- und Internetüberwachung stattfindet. Der Verteidigungsminister Peter MacKay gibt zu, den Geheimdienst CSE zur weltweiten Ausspähung von Verbindungsdaten autorisiert zu haben (Quelle: Heise).

13. Juni 2013: Edward Snowden bringt einen neuen Aspekt in die Debatte um Hackerangriffe aus China gegen die USA, indem er berichtet, dass der US-Geheimdienst NSA China seit Jahren durch Hacker angreifen lasse. Seit 2009 habe es mehrere hundert Hackerangriffe auf China, weltweit mehr als 61.000 gegeben (Quelle: The Guardian, Heise).

14. Juni 2013: Die Finanznachrichtenagentur *Bloomberg* berichtet unter Bezugnahme auf nicht namentlich genannte InsiderInnen, dass die Zusammenarbeit zwischen Unternehmen und Geheimdiensten in den USA noch umfangreicher gewesen sei als bisher angenommen. Die Rede ist von tausenden Firmen, unter anderem Microsoft, die die Geheimdienste mit Informationen versorgt hätten. Dabei gehe es jedoch nicht um Kundendaten, sondern vor allem um Software-Schwachstellen, die das Hacken fremder Rechner erleichtern (Quelle: Bloomberg, Heise).

16. Juni 2013: Einem Bericht des *Spiegel* zufolge will der Bundesnachrichtendienst (BND) trotz des Skandals um PRISM & Co die Internetüberwachung wesentlich ausweiten. Mit einem 100 Millionen Euro teuren „Technikaufwuchsprogramm" sollen sowohl der MitarbeiterInnenstab, als auch die technischen Möglichkeiten hierfür erweitert werden. 5 Millionen Euro seien bereits durch die Bundesregierung freigegeben worden.

Gleichzeitig spricht sich der Präsident des Bundeskriminalamtes (BKA) weiterhin vehement für die Vorratsdatenspeicherung, also die generelle, verdachtsunabhängige Speicherung von NutzerInnendaten, aus (Quelle: Spiegel, Heise).

19. Juni 2013: Die *New York Times* rückt erneut die enge Verbindung zwischen US-Geheimdiensten und Internetunternehmen in den Fokus. So berichtet sie, dass Max Kelly, ehemals Sicherheitschef bei Facebook, inzwischen für die NSA arbeite. Weiter legt die Zeitung dar, dass Skype 2008 mit der Entwicklung eines geheimen Programms *Project Chess* begonnen habe, das den Sicherheitsbehörden den Zugang zu der Kommunikation der NutzerInnen erleichtern solle. Dies steht der Behauptung der in den PRISM-Skandal verwickelten Unternehmen entgegen, den Behörden sei kein direkter Zugriff auf ihre Server gewährt worden (Quelle: New York Times, Heise).

20. Juni 2013: Einem Bericht der *Times of India* zufolge, hat Indien im April 2013 ein *Central Monitoring System* (CMS) einge-

führt, das Sicherheits- und Steuerbehörden eine umfangreiche Überwachung von Internetkommunikation und Telefonanrufen ohne richterliche Genehmigung erlaubt.

Der *Guardian* veröffentlicht am gleichen Tag zwei streng geheime Dokumente, welche die Zielgruppe der Überwachungsprogramme in den USA konkretisieren. Danach könne eine Person, von der „vernünftigerweise" angenommen werden kann, dass sie keinE US-StaatsbürgerIn ist und sich nicht in den USA aufhält, ohne richterliche Genehmigung von der NSA überwacht werden (Quelle: The Guardian, Heise).

21. Juni 2013: Edward Snowden gibt, wie der *Guardian* berichtet, belastende Informationen über den britischen Geheimdienst GCHQ preis. Dessen vor 18 Monaten in Betrieb genommenes Spionageprogramm *Tempora* sei sogar noch umfangreicher als PRISM. So fange der Geheimdienst in großem Stil Daten, wie E-Mails, Telefongespräche oder Einträge bei Facebook, über die transatlantischen Glasfaserkabel ab. Diese Daten würden auch der NSA zur Verfügung gestellt. In einem von Snowden überlassenen Dokument rühme sich der Geheimdienst damit, den *„biggest internet access"* (dt.: umfassensten Internet-Zugang) in einer Verbindung der Geheimdienste der USA, Großbritanniens, Kanadas, Neuseelands und Australiens unter dem Namen *Five Eyes* zu haben und *„larger amounts of metadata than NSA"* (dt.: größere Mengen an Metadaten als die NSA) zu erfassen (Quelle: The Guardian, Heise).

22. Juni 2013: Die *New York Times* berichtet, dass von den USA am 14. Juni eine Anklage gegen Edward Snowden wegen Spionage und Diebstahl von Regierungseigentum beim Bundesgericht in Virginia eingereicht worden sei. Snowden hält sich zu diesem Zeitpunkt in Hongkong auf (Quelle: New York Times, Heise).

23. Juni 2013: Edward Snowden berichtet in einem Interview mit der *South China Morning Post*, dass die NSA in China Millionen Mobilfunknachrichten abgehört und Datenübertragungsleitung der Pekinger Tsinghua-Universität überwacht habe. Weiter habe es Snowden zufolge 2009 Angriffe auf Computer von Pacnet, Betreiber eines der größten Glasfasernetze in der Asien-Pazifik-Region und verantwortlich für den Internetverkehr mit den USA, gegeben. Diese seien jedoch wieder eingestellt worden (Quelle: Heise).

24. Juni 2013: Die *Süddeutsche Zeitung* berichtet, dass im Rahmen des britischen Überwachungs-Programms *Tempora* auch das Glasfaserkabel TAT-14 ausgespäht worden sei, über das ein beträchtlicher Teil der Übersee-Kommunikation aus Deutschland laufe. Entsprechend sei auch der deutsche Telefon- und Internetverkehr Gegenstand der Überwachung gewesen. Die Bundesregierung und der Bundesnachrichtendienst (BND) bestreiten, darüber Kenntnis gehabt zu haben (Quelle: Süddeutsche Zeitung, Heise).

30. Juni 2013: Aus neu ausgewerteten NSA-Dokumenten geht dem *Spiegel* zufolge hervor, dass die Bundesrepublik in besonderem Maße von den US-Geheimdiensten überwacht wurde. Rund eine halbe Million Kommunikationsverbindungen seien betroffen. Auch die EU sei den Dokumenten zufolge Ziel der Spionageattacken geworden. In einem anderen Dokument, das dem *Guardian* vorliegt, werden 38 Botschaften und diplomatische Vertretungen aufgeführt, die von der massiven Ausspähung durch den US-Geheimdienst betroffen seien, unter ihnen auch die Botschaften Frankreichs, Italiens, Griechenlands, sowie Japans, Mexikos, Südkoreas, Indiens und der Türkei.

Die *Washington Post* veröffentlicht unterdessen neue Folien zum US-Überwachungsprogramm PRISM, aus denen hervorgeht, dass Daten von Microsoft, Google, Facebook, Youtube, Skype und anderen nicht einfach abgefragt, sondern in Echtzeit überwacht wurden. Mit einer beim Dienstanbieter installierten Filtersoftware seien Daten nach Schlüsselwörtern durchsucht worden, um die Datenströme auszudünnen (Quelle: Der Spiegel, Heise, The Guardian, Washington Post).

Juli 2013

2. Juli 2013: Wie Experten aus dem Umfeld des deutschen Internet-Knotens De-CIX in Frankfurt am Main gegenüber *heise online* bestätigten, wird ein nicht näher definierter Teil der über den Knoten laufenden Daten an den BND und andere „Bedarfsträger" übermittelt. Dem Vorsitzenden der G10-Kommission Hans De With zufolge, der die Abhörtätigkeit wie auch die Justizministerin Sabine Leutheusser-Schnarrenberger bestätigte, bestünde eine Obergrenze von 20 Prozent des Datenverkehrs (Quelle: Heise).

3. Juli 2013: Über einen Bericht der *New York Times* wird bekannt, dass die US-Geheimdienste den gesamten Briefverkehr innerhalb des Landes registrieren lassen. Im Rahmen des Programms *Mail Isolation Control and Tracking* wurden den InformantInnen aus Justizministerium und FBI zufolge AbsenderInnen und EmpfängerInnen von rund 160 Milliarden Postsendungen abfotografiert und gespeichert (Quelle: New York Times, Heise).

4. Juli 2013: Wie die Tageszeitung *Le Monde* berichtet, überwacht und speichert der französische Auslandsnachrichtendienst *Direction Générale de la Sécurité Extérieure* (DGSE) die Kommunikation der französischen StaatsbürgerInnen seit Jahren. Zu den gespeicherten Daten, die bei Bedarf an andere Behörden weitergeleitet würden, gehörten die Metadaten aller Telefongespräche, E-Mails, SMS, sämtliche Aktivitäten bei Google, Facebook, Microsoft, Apple oder Yahoo (Quelle: Heise).

6. Juli 2013: Die *New York Times berichtet* von einer erheblichen Erweiterung der NSA-Befugnisse durch den *Foreign Intelligence Surveillance Court* (FISC). In geheimen Urteilen sei der NSA unter anderem gestattet worden, Daten etwa bei Verdacht auf einen Zusammenhang mit Cyberangriffen oder dem iranischen Atomwaffenprogramm auch ohne richterliche Genehmigung auszuspähen (Quelle: Heise, New York Times, Süddeutsches Zeitung).

7. Juli 2013: Einem Bericht der brasilianischen Zeitung *O Globo* zufolge wurden auch brasilianische BürgerInnen konstant durch die NSA überwacht. E-Mails und Telefongespräche seien hier in noch größerem Ausmaß abgefangen worden als in anderen lateinamerikanischen Ländern. Der Zeitung vorliegenden Dokumenten zufolge seien die Daten mit Hilfe des Programms *Fairview* ausgespäht worden, das gemeinsam mit einer großen US-Telekom-

munikationsfirma genutzt werde. Partnerschaften des Unternehmens mit anderen Firmen der Telekom-Branche, unter anderem in Brasilien, ermöglichten es der NSA schließlich auf die Daten in verschiedenen Ländern der Welt zuzugreifen. Inwieweit die Telkom-Firmen darüber informiert sind, sei nicht bekannt.

Der *Spiegel* veröffentlicht ein Interview mit Edward Snowden, in dem dieser erklärt, dass der BND und andere ausländische Geheimdienste, ebenso wie verschiedene Telekom-Firmen, eng mit der NSA zusammenarbeiten. So habe die NSA dem BND etwa Analyse-Werkzeuge zur Verfügung gestellt, mit denen der BND Datenströme aus fünf digitalen Knotenpunkten anzapfe und an die Zentrale in Pullach weiterleite. Ob auch die NSA selbst Internetknotenpunkte in Deutschland ausspioniere, sei nicht geklärt. Weiter ist die Rede von einem geheimen NSA-Abhörzentrum namens *Consolidated Intelligence Center* in Wiesbaden, dessen Neubau durch den BND genehmigt worden sei.

Nach dem Bekanntwerden der Post-Überwachung in den USA, räumt auch die deutsche Post auf einen entsprechenden Tweet des CCC-Sprechers Frank Rieger hin ein, Adressdaten auf Briefen und Paketen automatisch zu scannen und zu speichern (Quelle: Heise, Spiegel).

9. Juli 2013: Anlässlich mehrerer Klagen vor dem EuGH gegen die Vorratsdatenspeicherung verteidigen VertreterInnen der EU-Gremien und -Mitgliedsstaaten die Richtlinie zur verdachtsunabhängigen Speicherung aller Verbindungsdaten in einer Anhörung.

Das Urteil zu dem nun beendeten Verfahren wird in etwa sechs Monaten erwartet. Das Gutachten des Generalanwalts soll am 9. November 2013 veröffentlicht werden (Quelle: Heise, Netzpolitik.org).

12. Juli 2013: Einem Bericht des *Guardian* zufolge hat Microsoft die NSA darin unterstützt, auch verschlüsselte NutzerInnendaten auszuspähen. So sei etwa vor dem Start des Mail-Portals Outlook.com sichergestellt worden, dass die NSA auf Daten zugreifen könne, bevor sie verschlüsselt werden. Auch an der Erleichterung des Zugangs zu Daten in dem Online-Speicherdienst SkyDrive und der Kommunikation via Skype sei gemeinsam gearbeitet worden (Quelle: The Guardian, Heise).

15. Juli 2013: Nachdem bereits in der vergangenen Woche Edward Snowden im *Spiegel* von einer umfangreichen Zusammenarbeit zwischen NSA und BND berichtet hatte, schaltet sich nun auch die *Bild* in die Debatte ein, die anführt, aus US-Regierungskreisen weitere Details dieser Zusammenarbeit erfahren zu haben. Der BND habe über Jahre von der umfangreichen Überwachung durch die NSA profitiert, etwa im Falle einer Entführung deutscher StaatsbürgerInnen. Es sei, so folgert die Zeitung, daher nur naheliegend, dass er über die umfangreiche Überwachung und Datensammlung durch den US-amerikanischen Geheimdienst informiert gewesen sei. Auch zieht die *Bild* die Behauptung des jüngst von einer umstrittenen USA-Reise zurückgekehrten Bundesinnenministers Hans-Peter Friedrich in Zweifel, dass die Überwachungsprogramme Daten gezielt nach Inhalten scannen würden – die Kommunikation würde vielmehr flächendeckend gespeichert (Quelle: Heise, Bild.de).

17. Juli 2013: Auch die Bundeswehr arbeite, so die *Bild*, mit der NSA zusammen. Einem geheimen Nato-Dokument zu Folge sei sie seit Herbst 2011 über PRISM informiert. Die Vorwürfe würden durch das Auftauchen einer zweiten Datenbank mit dem Namen PRISM erhärtet, die im Kommandobereich der Bundeswehr in Afghanistan zur Überwachung von Terrorverdächtigen genutzt worden sei. Ein Zusammenhang zwischen den beiden Programmen weisen SprecherInnen der Bundesregierung und des BND zurück. Bei PRISM II handele es sich um ein nicht geheimes Isaf-Programm zur Radaraufklärung und Luftüberwachung. Dies steht Berichten der *Bild* entgegen, denen zufolge beide Programme auf dieselben NSA-Datenbanken zugreifen würden.

Das ARD Magazin FAKT berichtet,dass es sich bei der vom BND verwendetet Software der Boeing-Tochter Naurus um PRISM-Software handele (Quelle: Heise, Bild.de).

18. Juli 2013: Die *Mitteldeutsche Zeitung Halle* berichtet, dass in Wiesbaden-Erbenheim aktuell ein Zentrum für militärische Aufklärung, *Consolidated Intelligence Center*, durch die ausamerikanischen Streitkräfte gebaut wird. Der Zeitung zufolge handelt es sich dabei um ein Abhörzentrum der NSA (Quelle: Heise).

20. Juli 2013: Wie der *Spiegel* berichtet, nutzen deutsche Geheimdienste die Ausspähdatenbanken der NSA stärker als sie zugeben wollen. Geheimen Unterlagen zufolge setzten BND und BfV eine NSA-Software namens *XKeyscore* ein, die quasi eine „digitale Totalüberwachung" ermögliche. Von dem Programm sei ein Teil der monatlich bis zu 500 Millionen Datensätze aus Deutschland, unter anderem Telefonnummern, E-Mail-Adressen und Zeitstempel von Nutzeraktivitäten, erfasst, auf die auch die NSA Zugriff habe.

In den USA wird die die Genehmigung zum Sammeln von Telefonverbindungsdaten durch die US-Behörden derweil verlängert (Quelle: Heise, Spiegel).

26. Juli 2013: Die Gewerkschaft der Polizei spricht sich trotz der jüngsten Überwachungsskandale für die Vorratsdatenspeicherung aus.

US-Medien berichten, dass Regierungsbehörden von Dienstanbietern im Internet die Herausgabe der geheimen Schlüssel ihrer

Sara Stadler

Sara Stadler studierte Informatik an der Hochschule Bremen und arbeitete in der FIfF-Geschäftsstelle.

Server mit SSL-Verschlüsselung verlangten. Die Konzerne würden die Herausgabe der *Master-Keys,* mit denen die gesamte Kommunikation des Servers auch im Nachhinein entschlüsselt werden könnte, jedoch bislang verweigern (Quelle: Heise).

27. Juli 2013: Der frühere Bundesinnenminister Otto Schily (SPD) räumt in einem Interview mit dem *Spiegel* ein, dass PRISM im Grunde nichts anderes sei als die Vorratsdatenspeicherung (Quelle: Spiegel).

31. Juli 2013: Der *Guardian* veröffentlicht weitere Details zum NSA-Programm *XKeyscore*. Folien aus dem Fundus Edward Snowdens zufolge ermögliche das Programm eine nahezu vollständige Überwachung der Internetnutzung (E-Mails, Chats, Browser-Chroniken, Aktivitäten auf Facebook) sowie die Möglichkeit einer vollständigen Überwachung jeder beliebigen Person bis hin zum US-Präsidenten (Quelle: Heise, The Guardian, Spiegel).

August 2013

1. August 2013: Unter Berufung auf weitere, von Edward Snowden ausgehändigte Dokumente berichtet der *Guardian* von einer umfangreichen Finanzierung des britischen Geheimdienstes GCHQ durch die NSA. Mindestens 100 Millionen Pfund seien in der vergangenen drei Jahren geflossen. Dass dafür auch US-BürgerInnen vom GCHQ überwacht worden seien, weise die NSA zurück. Weitere aus den Dokumenten gewonnene Erkenntnisse beziehen sich auf die Telefonüberwachung, in die der GCHQ massiv investiert habe, sowie den GCHQ-Standort in der Küstenstadt Bude, an dem der Geheimdienst Berichten der *Süddeutschen Zeitung* und des *NDR* zufolge Daten aus dem Glasfaserkabel TAT-14 abgefangen habe. Für die Sanierung diese Standortes habe Großbritannien 15,5 Millionen Pfund von der NSA erhalten (Quelle: Heise, The Guardian).

2. August 2013: Die *Süddeutsche Zeitung* und der *NDR* veröffentlichen die Namen derjenigen Telekom-Firmen, die dem britischen Nachrichtendienst GCHQ bei der Internetüberwachung behilflich waren. Genannt werden unter anderem die international tätigen Unternehmen British Telecom, Verizon und Vodafone.

Aus Neuseeland werden einstweilen Pläne bekannt, die Befugnisse des Geheimdienstes GSCB auszuweiten und den bestehenden Apparat zur Überwachung von Telefon und Internetkommunikation fortan auch für die Überwachung von StaatsbürgerInnen und Personen mit einem dauerhaften Aufenthaltsstatus zu nutzen (Quelle: Süddeutsche Zeitung, NDR, Heise).

3. August 2013: *CNET News* berichtet, dass die US-Regierung und das FBI NetzbetreiberInnen zur Installation von Port Readern zwängen (Quelle: Heise, CNET).

4. August 2013: Aus einem Bericht des *Spiegel* geht hervor, dass der BND Daten aus der eigenen Fernmeldeaufklärung an die NSA übermittele. Hinter einer der Datensammelstellen, über die die NSA im Dezember vergangenen Jahres rund 500 Millionen Metadaten aus der Bundesrepublik erfasst habe, verberge sich möglicherweise der BND-Standort Bad Aibling. Auch ansonsten sei die Zusammenarbeit zwischen BND und NSA enger als bisher angenommen. Die Zeitschrift berichtet von Schulungen – unter anderem im Umgang mit dem Programm *XKeyscore* – die VertreterInnen des BND und des Bundesamtes für Verfassungsschutz von NSA-SpezialistInnen erhalten hätten (Quelle: Heise, Spiegel).

5. August 2013: Die New York Times berichtet, dass die NSA Informationen an Ermittlungsbehörden weiterleite, obwohl deren Einsatz gegen in den USA lebende StaatsbürgerInnen nicht ohne weiteres möglich sein sollte (Quelle: Heise, New York Times).

7. August 2013: Der ehemalige NSA-Direktor Michael Hayden bestätigt in einem Interview mit CNN alle aus den von Snowden veröffentlichten Folien hervorgehenden Daten über das Programm XKeyscore und bewertet diese als positive Errungenschaft.

Die *Tagesschau* berichtet einstweilen unter Berufung auf den stellvertretenden Sprecher der Bundesregierung Georg Streiter, dass die Zusammenarbeit zwischen BND und NSA im April 2002 von der rot-grünen Bundesregierung vertraglich festgelegt und von dem damaligen Kanzleramtsminister Frank-Walter Steinmeier (SPD) abgesegnet worden sei (Quelle: Heise, Tagesschau.de).

8. August 2013: Die EU-Kommission legt ein Papier zum *Nachweis der Erforderlichkeit der Vorratsdatenspeicherung* vor.

Die *New York Times* fördert unterdessen neue Informationen über das Ausmaß der Online-Überwachung in den USA durch die NSA zutage. So sei nicht, wie von offizieller Seite stets betont wurde, „lediglich" die Kommunikation mit nicht-US-BürgerInnen ohne Genehmigung überwacht, sondern jegliche Kommunikation nach Verweisen auf überwachte Personen gescannt worden (Quelle: Heise, New York Times).

9. August 2013: Die US-amerikanischen E-Mail-Anbieter *Lavabit* und *Silent Circle* machen dicht. Beide hatten ihren NutzerInnen verschlüsselte Kommunikation angeboten. Auch wenn die Anbieter die Gründe für das Aus nicht nennen (dürfen), legen die Aussagen des Lavabit-Chefs Ladar Levison nahe, dass sie, zumindest in diesem Fall, etwas mit der Weigerung zu tun hatten, den US-Behörden Zugriff auf Kommunikationsdaten zu ermöglichen (Quelle: Heise).

16. August 2013: Nach Berichten der *Washington Post* hat die NSA entgegen anderslautender Beteuerungen in erheblichem Umfang illegal US-BürgerInnen überwacht. Ein geheimer Bericht, der den Großraum Washington D.C. abdeckt, berichte von 2776 „Vorfällen" über einen Zeitraum von 12 Monaten. Nach Angaben der NSA sei die Überwachung „versehentlich" aufgrund eines Programmierfehlers erfolgt. Offenbar wurde bei der Telefonüberwachung die Vorwahl von Washington D.C. (202) mit der Ländervorwahl von Ägypten (20) verwechselt (Quelle: Washington Post, Spiegel).

Klaus Fuchs-Kittowski

Ethik und Informatik – Moralität und Historizität

Zur notwendigen Solidarität mit den Whistleblowern

Als ich in den 80er Jahren die Leitung der Arbeitsgruppe 1: Computer and Work *des Technischen Komitees 9:* Wechselbeziehungen zwischen Computer und Gesellschaft *(TC9) der Internationalen Föderation für Informationsverarbeitung (IFIP) übernahm, hatten die Themen Computer und Arbeit Hochkonjunktur. Denn die Qualität des Arbeitslebens, arbeitsorganisatorische, arbeitspsychologische Probleme im Zusammenhang mit der Automatisierung der Arbeitsprozesse wurden in der Informatik und in der Politik weithin auf nationaler und internationaler Ebene diskutiert. Ein sichtbares Ergebnis dieser Debatten waren die in enger Zusammenarbeit mit den arbeitswissenschaftlichen Instituten (u. a. in Berlin, Zürich und Dresden) erarbeiteten Humankriterien der Arbeits- und Organisationsgestaltung sowie die für die Technikbewertung erarbeitete VDI-Richtlinie 3780.*[1] *Wir führten zwei internationale Workshops der Working Group 1 des TC9 in Berlin durch.*[2] [3] *Eine umfangreiche wissenschaftliche Literatur entstand zu den Problemen einer am Menschen orientierten Informationssystemgestaltung (z. B.* [4] [5]*).*

Unter der Leitung von *Jacques Berleur* war die Arbeitsgruppe 2: *Social Accountability* sehr aktiv. Hier ging es insbesondere um das auch heute besonders aktuelle Thema Datenschutz. Viele der dort entwickelten Ideen und Grundsätze fanden ihren Niederschlag in den nationalen Datenschutzgesetzen – bis hin zur Einführung des Rechts auf *informationelle Selbstbestimmung* in das Grundgesetz der Bundesrepublik. Damit wurde auch das Ausspähen privater Daten aus staatlichem Interesse geregelt und strengen Beschränkungen unterworfen. Nach bestimmter Frist müssen die Daten wieder gelöscht und dem Ausgespähten Kenntnis über den Vorgang gegeben werden. Der Hinweis *Wilhelm Steinmüllers*, der als Mitbegründer der Rechtsinformatik in Deutschland gilt[6] und aktiv in der WG 2 tätig war, dass die vom BND über den Briefverkehr zwischen Ost- und Westdeutschland gewonnen Daten nicht fristgemäß gelöscht wurden, brachten ihn schon damals in große Schwierigkeiten. Ihm wurde dadurch sehr geholfen, dass die IFIP zu ihm stand. Die Informatik hat also schon Erfahrung mit Whistleblowern aus den eigenen Reihen. Erinnert sei insbesondere auch an die große Tat von *David Lorge Parnas*, der aus der Beratergruppe des Starwars-Projekts mit der alarmierenden These austrat:

> *„Software muss getestet werden. Diese Software in den sogenannten Frühwarnsystemen ist nicht getestet. Ein Krieg aus Zufall wird immer wahrscheinlicher!"*

Natürlich war dies ein Affront gegenüber der amerikanischen Regierung, der Parnas sehr verübelt wurde. Für alle in der Friedensbewegung, für uns speziell in der Task-force der IFIP für *Peace and Disarmament*, war jedoch diese fachliche Stellungnahme eines international respektierten Informatikers von größter Bedeutung. Denn die Generalversammlung der IFIP hatte von uns immer wieder eine „nicht politische", „rein fachliche" Stellungnahme zu dem Wettrüsten gefordert, um selbst öffentlich Stellung beziehen zu können. So wie die Bewegung *Ärzte gegen den Atomtod* die fachlich unwiderlegbare These vertrat: „Nach einem Atomschlag gibt es keine Heilung mehr", konnten die InformatikerInnen in Bezug auf die installierten Frühwarnsysteme nun formulieren: „Es gibt keine fehlerfreie Software, eine zufällige Auslösung eines Krieges wird daher immer wahrscheinlicher." Auch hier stand die Frage, was wiegt mehr, die Förderung nationaler Machtinteressen oder das Wohl der Menschheit als Ganzes? Der Bewegung war dann doch der entscheidende Erfolg beschieden, dass die Raketen von der deutsch/deutschen Grenze abgezogen wurden.

Wie stellen wir uns nun heute persönlich und auch unsere Fachorganisationen zu den Computerspezialisten *Bradley Manning*[7] und *Edward Snowden*? Es gilt für die InformatikerInnen, für jeden persönlich und die Fachorganisationen, Position zu Kriegsverbrechen und zur Ausspähung durch Geheimdienste und damit auch zu den Handlungen von Bradley Manning und Edward Snowden zu beziehen. Es ist doch paradox, wenn offensichtliche Kriegsverbrechen verurteilt und die Ausspähung durch den Geheimdienst NSA empört abgelehnt werden, diejenigen aber, die es auf sich nehmen, diese Geschehnisse aufzudecken, verfolgt und verurteilt werden.

Sie haben in der Tat Verrat gegenüber ihren Auftraggebern und ihrem Vaterland verübt. Verschärfend zum Geheimnisverrat kommt noch dazu, dass sie dies als Soldat bzw. als Geheimdienstler begangen haben. Verräter oder Helden, dies mag für

Klaus Fuchs-Kittowski

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

viele schwer zu beurteilen sein. Diese innere Zerrissenheit, in der sich sicher viele befinden, konnte kaum deutlicher werden, als in dem kürzlich in der *Berliner Zeitung* veröffentlichen Interview des Bundesdatenschutzbeauftragten *Peter Schaar*: *„Überwachung gehört ans Licht der Öffentlichkeit"*[8]. Dieses Interview ist ein engagiertes Plädoyer für den Datenschutz. Dem Enthüller Snowden kann er aber nur für kurze Zeit einen Schutzraum anbieten, nur damit er vom Generalbundesanwalt verhört werden kann. Snowden ist ein Verräter, obwohl die Geschichte vielleicht einmal zeigen wird, dass er ein Held ist. Müssen wir wirklich lange warten bis wir die historische Dimension der Enthüllungen Mannings und Snowdens einschätzen können? Die weltgeschichtliche Bedeutung ihrer Entscheidung sollte deutlich genug sein und ihr muss eine höhere Präferenz beigemessen werden, denn sie besaß für die getroffene Entscheidung offensichtlich größere Kraft, als die Verpflichtung zur individuellen Loyalität gegenüber den nationalen Institutionen.

Solange wir uns im Rahmen der gewöhnlichen Moralität bewegen, wird man kaum anders urteilen können, als den Verrat zu verurteilen. Denn es gibt in diesem Rahmen keine Möglichkeit zu seiner Legitimierung. Es gibt keine unmittelbaren moralischen Gründe, die die Weitergabe von hoch brisanten militärischen oder industriellen Geheimnissen an einen anderen Staat legitimieren würden. Und doch stehen viele mutige Amerikaner auf, wie z. B. *Daniel Elsberg*, der Friedensaktivist und ehemalige Whistleblower, durch dessen mutige Enthüllung der sogenannten Pentagonpapers die amerikanische Öffentlichkeit über die reale Situation im Vietnamkrieg informiert wurde. Sie rufen: *„Ich bin Bradley Manning! Lasst die Anklage gegen ihn fallen!"*

Woher kann man die Rechtfertigung für diese m.E. richtige und notwendige Haltung nehmen? Moralische Prinzipien können zwar, wie z. B. beim *kategorischen Imperativ* von *Immanuel Kant* mit dem Anspruch auf Allgemeingültigkeit verbunden werden. Es wird sich aber bald zeigen, dass uns ein solches formales Schema: *„Handle so, dass die Maxime deines Willens jederzeit zugleich als Prinzip einer allgemeinen Gesetzgebung gelten könne"*[9] schon bei einfachen Konflikten kaum weiter hilft. Denn die zunächst einleuchtende Regel muss auf die konkrete Situation bezogen werden, die eben nicht formal behandelt werden kann. Wer sollte dieses besser wissen als die (Rechts-) Informatiker. Wie ist es aber dann erst bei wirklich komplizierten Situationen, die die Welt erschüttern? Wissenschaftler mit entscheidenden Erkenntnissen, Ingenieure mit wichtigen Erfindungen, die für die Gesellschaftsentwicklung relevant werden, und wie wir sehen, auch Informatikspezialisten können offensichtlich in hoch komplizierte Konfliktsituationen geraten. Eine Antwort auf diese uns so bedrängende Frage finden wir bei dem weiteren großen Vertreter der Deutschen Klassischen Philosophie *Georg Wilhelm Friedrich Hegel*. Er schreibt:

> *„Denn Weltgeschichte bewegt sich auf einem höheren Boden, als der ist, auf dem die Moralität ihre eigentliche Stätte hat, welche die Privatinteressen, das Gewissen der Individuen, ihr eigentümlicher Wille und ihre Handlungsweise ist."*[10]

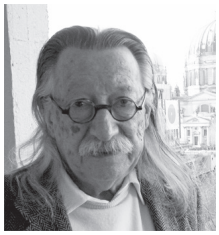
Hegel verdeutlicht damit, dass der Gesichtspunkt privater Moralität unvollständig und unzureichend ist. Unvollständig, weil der Kontext der geschichtlichen Situation, von der der Handelnde ein konstitutives Glied ist, unberücksichtigt bleibt und unzureichend, weil die aus der historischen Sachlage entspringenden Entscheidungsgründe ein übergreifendes Allgemeines darstellen, das die ihnen entgegenstehenden moralischen Erwägungen in sich aufhebt.[11]

Der weltgeschichtlichen Bedeutung einer Entscheidung muss eine höhere Präferenz beigemessen werden. Die weltgeschichtliche Situation ist die Grundlage für die individuelle Entscheidung in der Humanitäts- und Freiheitsgewinn als ein für die Menschheit allgemeiner Wert gegenüber den individuellen Werten logisch zwingend die Priorität erhält. Jedes Festhalten an privater Moralität und Negieren des Einsatzes von Menschen (wie der Whistleblower) im Allgemeininteresse für die Gewährleistung der Bürger- und Menschenrechte könnte die Menschheit nur in die Katastrophe führen.

Die Anklage wegen Feindbegünstigung und damit die Todesstrafe für Bradley Manning ist zum Glück schon fallen gelassen worden. Aber ihn erwarten noch bis zu 130 Jahre Gefängnis. Daher muss sich ein Sturm der Entrüstung gegen die Verfolgung und Verurteilung erheben, Solidarität bekundet werden, mit dem Ruf: *„Ich bin Bradley Manning!"* Ständig erfahren wir neue Details zur NSA-Spionage und auch die BND-Datenweitergabe ist zu klären und doch muss Edward Snowden, der den bürger- und menschenrechtswidrigen Spähskandal aufgedeckt hat, in seinem Heimatland mit einer hohen Gefängnisstrafe rechnen. Auch für ihn müssen wir Solidarität bekunden, mit dem Ruf: *„Ich bin Edward Snowden!"*

Anmerkungen

1 *Friedrich Rapp (Hrsg.): Normative Technikbewertung – Wertprobleme der Technik und die Erfahrungen mit der VDI-Richtlinie 3780*
2 *P. Docherty, K. Fuchs-Kittowski, P. Kolm, I. Mathiassen (Editors): System Design for Human Development and Productivity: Participation and Beyond, North-Holland, Amsterdam, 1986*
3 *P. Van Den Besselaar, A. Clement, P. Järvinen (Editors): Information System, Work and Organization Design, North-Holland, Amsterdam, 1991*
4 *Klaus Kornwachs, Information und Kommunikation – Zur menschengerechten Technikgestaltung, Springer-Verlag, Berlin, New York, 1993*
5 *Peter Brödner, Der überlistete Odysseus – Über das zerrüttete Verhältnis von Mensch und Maschine, edition sigmar, Berlin, 1997*
6 *Wilhelm Steinmüller, Informationstechnologie und Gesellschaft – Einführung in die Angewandte Informatik, Wissenschaftliche Buchgesellschaft, Darmstadt, 1993*
7 *Heute Chelsea Manning. Sie wurde zunächst zu 35 Jahren Haft verurteilt und später durch US-Präsident Barack Obama zum Ende seiner Amtszeit begnadigt.*
8 *Peter Schaar, Überwachung gehört ans Licht der Öffentlichkeit, Berliner Zeitung, Freitag den 2. August 2013, S.6*
9 *Immanuel: Kant Kritik der praktischen Vernunft, Riga 1788, S. 54.*
10 *Georg Wilhelm Friedrich Hegel, Vorlesungen über die Philosophie der Geschichte, Werke, Suhrkamp Band 12, Frankfurt am Main 1970, S. 40 und 90f.*
11 *Hans Heinz Holz, Wissenschaft und Verantwortung – Historizität und Moralität, in: Ethik in der Wissenschaft – Die Verantwortung der Wissenschaftler – zum Gedenken an Klaus Fuchs, Abhandlungen der Leibniz-Sozietat, trafo Verlag der Wissenschaften, Berlin, S. 151-159*



„Daß die Menschheit in diesem höchst instabilen und gefährlichen Zustand lebt und abhängig ist von einer Technik, die sie kaum noch durchschaut, ist keine zwangsläufige Folge der technischen und wissenschaftlichen Entwicklung – es ist eine Folge des moralischen und politischen Entwicklungsstandes der Gesellschaft."

Joseph Weizenbaum

#FIfFKon18: Brave New World

Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme
28.–30. September 2018 in Berlin

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

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

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

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

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

Einladung zur Mitgliederversammlung 2018

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

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2018 ein.

Sie findet am Sonntag, den 30. September 2018 in Berlin statt.
Uhrzeit und genauer Ort werden noch rechtzeitig bekannt gegeben.

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht und Berichte aus den Regionalgruppen
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,
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

FIfF e. V. – Pressemitteilung

FIfF ist ab 2019 Mitherausgeber des Grundrechte-Reports

Grundrechte-Report 2018 wird am 29. Mai 2018 in Karlsruhe vorgestellt

29. Mai 2018 – Das FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung – wird künftig Mitherausgeber des jährlich im Fischer-Taschenbuchverlag erscheinenden Grundrechte-Reports sein. Damit wird die Zahl der herausgebenden Bürgerrechtsorganisationen auf neun anwachsen.

Stefan Hügel, Vorsitzender des FIfF, sagt dazu: „Wir freuen uns sehr, dass uns die bisherigen HerausgeberInnen in ihren Kreis aufgenommen haben. Mit unserer Kompetenz in den informationstechnischen Themen der Bürgerrechtsarbeit wollen wir substanzielle Beiträge zu den künftigen Ausgaben des Grundrechte-Reports leisten. Wir können damit die juristisch geprägte Sicht durch unseren Informatik-bezogenen Blick ergänzen."

„Der Einfluss der Informationstechnik und der Digitalisierung auf die Bürgerrechte nehmen stetig zu", so erläutert Prof. Dr. Hans-Jörg Kreowski, der als Vorstandsmitglied für das FIfF die Herausgeberschaft übernehmen wird. „Technologien und Methoden wie Künstliche Intelligenz, Big Data und Lernalgorithmen werden in ihrer Bedeutung erheblich zunehmen. Auch der Einfluss des Transhumanismus und seines Menschenbildes auf die Menschenwürde ist ein wichtiges Thema des FIfF mit heute noch nicht absehbaren langfristigen Auswirkungen auf die Bürgerrechte."

„Dazu kommt das klassische FIfF-Thema: Informatik und Rüstung", ergänzt Stefan Hügel. „‚Frieden ist erstes Menschenrecht', so hat es unser Beiratsmitglied Klaus Fuchs-Kittowski einmal formuliert."

Bereits im aktuellen Grundrechte-Report ist ein Beitrag des FIfF-Vorsitzenden Stefan Hügel enthalten, in dem er sich anhand des Trojaners *WannaCry* mit dem Umgang von Bundeswehr und Bundesnachrichtendienst mit Schwachstellen der IT-Sicherheit auseinandersetzt: *Öffentliche Sicherheit durch unsichere IT?*

Der Grundrechte-Report stellt die Einschränkungen und Gefährdungen der Menschen- und Grundrechte in Deutschland dar und versteht sich als alternativer Verfassungsschutzbericht. Er nennt aktuelle Missstände beim Namen und zeigt auf, wie Gesetzgeber, Verwaltung und Behörden, aber auch Gerichte und Privatunternehmen die demokratischen und freiheitlichen Grundlagen unserer Gesellschaft gefährden. Er beruht auf der Expertise seiner herausgebenden Organisationen und auf deren praktischen Erfahrungen in der Bürgerrechtsarbeit. Das FIfF wird dort mit der Humanistischen Union, dem Komitee für Grundrechte und Demokratie, dem Bundesarbeitskreis Kritischer Juragruppen, PRO ASYL, dem Republikanischen Anwältinnen- und Anwälteverein, der Vereinigung Demokratischer Juristinnen und Juristen, der Internationalen Liga für Menschenrechte und der Neuen Richtervereinigung zusammenarbeiten.

Hinweis: Die Ankündigung des diesjährigen Grundrechte-Reports findet sich auf Seite 62, eine Rezension von Marie-Theres Tinnefeld in der nächsten Ausgabe.

~ Bits & Bäume ~

Die Konferenz für Digitalisierung und Nachhaltigkeit 17.–18. November 2018

Ort: Technische Universität Berlin, Straße des 17. Juni 135, 10623 Berlin

Wir bringen Communities zusammen!

In den letzten Jahrzehnten sind gesellschaftsverändernde Bewegungen gewachsen, die ihrer jeweils eigenen Utopie folgen: Sie kämpfen dafür, die Natur und unsere Lebensgrundlagen zu erhalten, für faire Arbeitsbedingungen ohne Ausbeutung, für eine Eindämmung der Macht von Konzernen und gegen die Zerstörung des Planeten. Sie setzen sich ein für demokratische Teilhabe, für nachhaltige Produktions- und Konsumweisen, für gerechten Handel zwischen globalem Süden und Norden und für verbindliche Regeln für die Wirtschaft im Sinne dieser Ziele. Andere Communities arbeiten konkret daran, die Digitalisierung so zu gestalten, dass Bürgerrechte, Schutz der Privatsphäre, Datenschutz, Souveränität und Demokratie für eine offene Gesellschaft gewahrt sind. Sie stehen auf für einen freien Zugang zum Wissen der Mächtigen, für eine Kultur des Miteinander-Teilens, für eine überwachungsfreie digitale Welt, für flache Hierarchien, globale Vernetzung und Dezentralität, für Selbstbestimmung und Menschenrechte angesichts eines Zeitalters der Künstlichen Intelligenz und der Übermacht globaler Internet-Monopole.

Bislang agieren diese Bewegungen der Umwelt-AktivistInnen und digitalen MenschenrechtlerInnen oft nebeneinander. Sie bieten Lösungsansätze und Ideen für ihre jeweils eigenen Themen, die inzwischen nicht nur Politik, Zivilgesellschaft, Wirtschaft, sondern sogar fast jeden Haushalt erreicht haben. Beide wollen die Welt verstehen, aber vor allem aktiv gestalten. Sie sehen, dass wesentliche Veränderungen für ein ‚gutes Leben' sowie eine gerechte und zukunftsfähige Gesellschaft nötig sind. Doch eine ökologische, soziale und ökonomische Nachhaltigkeit kann nur gemeinsam gelingen – dafür müssen diese Communities zusammenkommen, voneinander lernen, die Gemeinsamkeiten ihrer Utopien erkennen und diese mit neuer Wucht umsetzen!

Wie also kann die Digitalisierung eine Transformation hin zu einer nachhaltigen Gesellschaft unterstützen? Wie kann Nachhaltigkeitsdenken die Techie-Szene inspirieren, sodass die Digitalisierung langfristig Bürgerrechte und individuelle Freiheiten garantiert? Wie können beispielsweise erneuerbarer Strom und intelligente Netze mit vereintem Wissen weiterentwickelt werden? Welche Rolle spielen die drei Facetten der Nachhaltigkeit für stabile Tech-Communities? Welche ökologischen Chancen stecken in digitalen Anwendungen etwa für Klima- und Ressourcenschutz? Welche Arten von Digitalisierung stehen diesen Zielen entgegen oder sind sogar grob kontraproduktiv? Wie kann die digitale Gesellschaft demokratisch und gerecht gestaltet und zugleich darauf ausgerichtet sein, auf friedvolle Weise die Grundlagen unseres Lebens auf diesem Planeten zu bewahren?

Unter diesen Leitfragen steht *Bits & Bäume* als eine offene Vernetzungskonferenz – für neue Perspektiven auf eine Digitalisierung mit Nachhaltigkeit! Wir wollen gegenseitigen Austausch, wir brauchen aktive Vernetzung.

Dafür wollen wir

- unterschiedliche Szenen, Akteure und Organisationen in die Diskussion bringen,
- Schnittstellen zwischen Nachhaltigkeitsthemen und einer umsichtigen Digitalisierung herausarbeiten,
- visionäre Lösungen finden und mit gemeinsamer Vehemenz umsetzen.

Neben Vorträgen wird es Raum geben für Diskussionsrunden sowie für die Planung von Projekten und Kampagnen, die die unterschiedlichen Communities verbinden: Hands-on-Workshops, Aktivisten-Infotische, Sofas oder Hackathons. *Bits & Bäume* soll politisieren und den Auftakt geben für gemeinsame Positionen zu einer nachhaltigen Digitalisierung und wider demokratiefeindliche Trends. Zwei Konferenztage geben Anstoß für intensiven Austausch und politische Aktivitäten. Neben Akteuren aus zivilgesellschaftlichen Organisationen richten wir uns auch ausdrücklich an die interessierte Öffentlichkeit.

Bits & Bäume wird organisiert von:

- Bund für Umwelt und Naturschutz Deutschland (BUND)
- Brot für die Welt
- Chaos Computer Club (CCC)
- Deutscher Naturschutz Ring (DNR)
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)
- Germanwatch
- Institut für ökologische Wirtschaftsforschung (iöw)
- Konzeptwerk Neue Ökonomie
- Open Knowledge Foundation Deutschland (OKF)
- PowerShift
- Technische Universität Berlin, Fachgebiet Sozial-ökologische Transformation (TU-Berlin)

Medienpartner:

- Netzpolitik.org

Die Veranstaltungsplanung und -organisation wird Nachhaltigkeitskriterien entsprechen: Wir achten bei der Nutzung und Bereitstellung digitaler und analoger Infrastrukturen auf Ressourcenschonung, Datenschutz und Gemeinwohlorientierung gleichermaßen und stellen unsere Erfahrungen und Materialien offen zur Verfügung.

FIfF stiftet Weizenbaum-Preis

Nachfolger des bisherigen FIfF-Studienpreises ist dem Informatiker und Gesellschaftskritiker Joseph Weizenbaum gewidmet

18. Mai 2018 – *Das FIfF stiftet den Weizenbaum-Preis in Erinnerung an den Wissenschaftler und Informatik-Pionier Professor Dr. Joseph Weizenbaum in Würdigung seiner Verdienste um einen kritischen Blick auf die Informatik. Joseph Weizenbaum war an der Gründung des FIfF maßgeblich beteiligt, wirkte lange Zeit im Vorstand mit und trug durch seine wissenschaftlichen Leistungen in vorbildlicher Weise zur Arbeit und zu den Zielen des FIfF bei.*

„Mit der Vergabe des Preises wollen wir auch die Bedeutung der Informatik für die gesellschaftliche Entwicklung betonen und auf die kritische, öffentliche Auseinandersetzung mit den Erkenntnissen und Artefakten der Informatik dringen", erläutert der FIfF-Vorsitzende und Mitglied der Jury Stefan Hügel. „Den Weizenbaum-Preis wollen wir in zwei Bereichen vergeben:

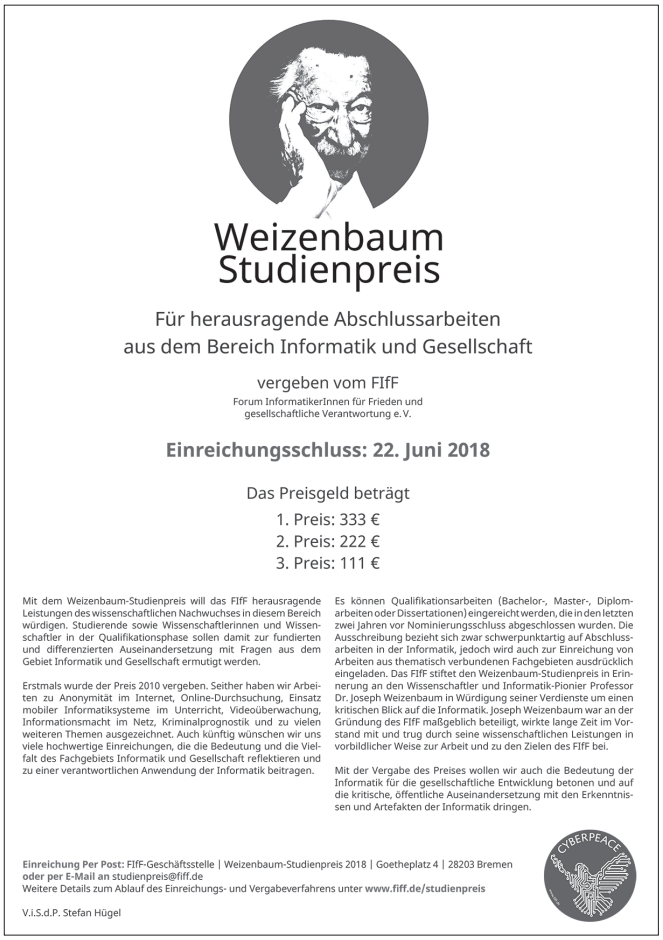
Mit dem Weizenbaum-Studienpreis will das FIfF herausragende Leistungen des wissenschaftlichen Nachwuchses in diesem Bereich würdigen. Studierende sowie Wissenschaftlerinnen und Wissenschaftler in der Qualifikationsphase sollen damit zur fundierten und differenzierten Auseinandersetzung mit Fragen aus dem Gebiet Informatik und Gesellschaft ermutigt werden.

Mit einem Joseph Weizenbaum gewidmeten Ehrenpreis [der Weizenbaum-Medaille (d. Red.)] wollen wir künftig zusätzlich Persönlichkeiten auszeichnen, die sich in besonderer Weise um das Themengebiet Informatik und Gesellschaft durch wissenschaftliche Leistungen, politsches Wirken und persönliches Handeln verdient gemacht haben oder durch ihr Handeln dazu beitragen, die Anwendung der Informatik am Nutzen der Gesellschaft und der Menschen auszurichten."

„Mit der Verleihung des Studienpreises möchte das FIfF einen Beitrag leisten, die immer wieder von Sparzwängen an den Hochschulen betroffene Forschung zu den gesellschaftlichen Auswirkungen der Informationstechnologie zu fördern, gerade in einer Zeit sich ausbreitender Digitalisierung aller Lebensbereiche", erklärt Hans Jörg Kreowski, ebenfalls Mitglied des FIfF-Vorstandes.

Erstmals wurde der FIfF-Studienpreis im Jahr 2010 vergeben. Seither haben wir Arbeiten zur Anonymität im Internet, zur Online-Durchsuchung, zum Einsatz mobiler Informatiksysteme im Unterricht, zur Videoüberwachung, zur Informationsmacht im Netz, zur Kriminalprognostik und zu vielen weiteren Themen ausgezeichnet. Auch künftig wünschen wir uns viele hochwertige Einreichungen, die die Bedeutung und die Vielfalt des Fachgebiets Informatik und Gesellschaft reflektieren und zu einer verantwortlichen Anwendung der Informatik beitragen.

Joseph Weizenbaum wurde am 8. Januar 1923 in Berlin geboren und starb am 5. März 2008 in Gröben. 1935 musste er mit seiner Familie das nationalsozialistische Deutschland verlassen, studierte in den USA Mathematik und arbeitete ab 1955 bei General Electric an einem frühen Computersystem für die Bank of America mit. 1963 wurde Joseph Weizenbaum Visiting Professor, 1964 Associate Professor und 1970 ordentlicher Professor für Computer Science (Informatik) am Massachusetts Institute of Technology (MIT), wo sowohl seine Arbeiten zu ELIZA entstanden als auch sein wegweisendes Buch *Computer Power and Human Reason – From Judgement to Calculation* (Die Macht der Computer und die Ohnmacht der Vernunft). Ab den 70er Jahren intensivierten sich seine Kontakte nach Deutschland mehr und mehr.



Lange vor der Gründung von CPSR und FIfF nahm er deutlich Stellung gegen den Vietnamkrieg und den Bau von Anti-Ballistic-Missile-Systemen. Als in den 80er Jahren die Kritik an SDI laut wurde, war er einer der Protagonisten dieser Kritik. Zur Gründung des FIfF 1984 brachte er hierzulande nur schwer zugängliche Strategiepapiere des Pentagon mit. 1996 verlegte er seinen Lebensmittelpunkt wieder nach Berlin. Auf Vorschlag des Bundesministers des Auswärtigen wurde Joseph Weizenbaum am 25. Juli 2001 das Große Verdienstkreuz des Verdienstordens der Bundesrepublik Deutschland verliehen. Am 8. Januar 1998 erhielt er den Preis des FIfF.

„Neues“ Hambacher Fest

Vom rechtspopulistischen Missbrauch eines Symbols der Freiheit, des gesellschaftlichen Fortschritts und der internationalen Verantwortung

Im September 2017 feierten wir in Berlin die Festtafel der Freiheit – wir nahmen uns das Hambacher Fest von 1832 zum historischen Vorbild, bei Wein, Brot und Tischreden für die Freiheit und gegen staatliche Überwachung einzutreten.

Einleitend schrieben wir:

> *Pate für diese Protestform stand eines der bedeutendsten Ereignisse der deutschen Demokratiegeschichte: das Hambacher Fest um den 27. Mai 1832. In einer Zeit von Zensur und Unterdrückung, einer Zeit ohne Versammlungsrecht und Pressefreiheit, einer Zeit des Rückzugs ins Private und in politisch unverfänglichen Zeitvertreib mussten Forderungen nach Freiheiten und Bürgerrechten als Bankett getarnt werden. Zugleich gelten diese Festtage heute als Wiege der europäischen Einigung. In diesem Geiste war auch unsere „Festtafel der Freiheit“ ein Forum für alle freiheitlichen Gedanken.*[1]

Es ist nicht zu bestreiten: Das historische Hambacher Fest trug auch nationale Züge. Diese sind aber aus dem historischen Kontext eines in viele Einzelstaaten zersplitterten und vom Absolutismus geprägten Staatsgebildes zu verstehen. Doch auch Nationalsozialisten und Rechtsextreme beriefen sich später auf die Tradition des Hambacher Fests – zu Unrecht, meinen wir:

> *Mehrere Jahre nach dem Hambacher Fest entwickelten sich aus der damals geforderten Vereinigungsfreiheit heraus u. a. die bündischen Bewegungen, in deren enger Tradition sich später die Nationalsozialisten sahen und denen sich auch heute viele Rechtsextreme verbunden fühlen. Die Formulierungen von Nationalismus und Volksbund im Rahmen des Hambacher Festes erscheinen uns in der Tat heute überaus befremdlich. Sie sind jedoch aus der krisenbehafteten Grundsituation des zersplitterten und unterschiedlich regierten Deutschlands zu sehen, in dem nicht nur wirtschaftlich ein gemeinsamer Handel schwierig war, sondern in welchem sich auch Bürgerinnen und Bürger der einzelnen Hoheitsgebiete miteinander grenzüberschreitend als ein Volk und in geistiger Verbundenheit sahen und gemeinsam die Befreiung von Obrigkeit, Absolutismus und Aristokratenherrschaft forderten. Stattdessen traten sie für ein einiges starkes Gesamtdeutschland ein und mehrere Redner an der Hambacher Festtafel verlangten explizit feste demokratische Strukturen und Verfassungen. Bedauerlicherweise benutzen heute Rechtsextreme u. a. die Formulierungen des Hambacher Festes in ihrem anders motivierten nationalistischen Sinne und den geschichtlichen Zusammenhängen entrissen. Umso wichtiger ist es, die Reden des Hambacher Festes in ihren historischen Kontext zu stellen und sie so positiv zu verstehen, wie sie in großen Teilen gemeint waren: Als Aufruf zu einem einigen Miteinander, innerhalb Deutschlands ebenso wie auch innerhalb Europas.*[2]

Anfang Mai fand nun eine Veranstaltung[3] auf dem Hambacher Schloss statt, die in der dunklen Tradition der deutschen Geschichte steht: Nationalismus und Abschottung stehen dabei im Vordergrund. Zu Wort kamen die Protagonisten eines Rechtspopulismus, der den gesellschaftlichen Fortschritt leugnet und ablehnt: die Fortschritte seit 1968 gelten für sie als die Wurzel allen Übels, sie sprechen von „linksversifften 1968ern“. Sie lehnen Diskriminierungsfreiheit ab und versuchen, die überfällige Durchsetzung der Gleichberechtigung von Frauen als „Genderismus“ lächerlich zu machen. Sie fordern die Abschottung gegen Migranten und Flüchtlinge, die bei uns Schutz suchen und gefunden haben. Sie wollen Fortschritte aus der europäischen Einigung rückgängig machen und in eine nationalstaatliche Ordnung zurückfallen. Stellvertretend sei hier nur Jörg Meuthen genannt, der Bundesvorsitzende der sogenannten „Alternative für Deutschland“.

Nein, das ist nicht die Tradition des Hambacher Fests. Das Hambacher Fest war in die Zukunft gerichtet, das Gesellschaftsbild der AfD ist rückwärtsgewandt. Ein heutiges Hambacher Fest ist ein Fest für Freiheit und gesellschaftlichen Fortschritt, für internationale Verantwortung und für die europäische Einigung. Dafür steht das FIfF – die Instrumentalisierung und den Missbrauch des Hambacher Festes für ein rückständiges und nationalistisches Gesellschaftsbild weisen wir zurück.

Anmerkungen

1 *Juliane Krüger, Rainer Rehak: In welcher digitalen Gesellschaft wollen wir leben. FIfF-Kommunikation 4/2017, S. 21-23*

2 *ebd.*

3 *https://neues-hambacher-fest.de*

Hambacher Schloss - Blick vom Sühnekreuz am Rittersberg

Grundrechte-Report 2018: „Gefährder“ Staat

29. Mai 2018 – Am Dienstag, den 29. Mai 2018, stellen in Karlsruhe acht deutsche Bürger- und Menschenrechtsorganisationen[1] den neuen Grundrechte-Report 2018 der Öffentlichkeit vor – wie seit 1997 jährlich um den Verfassungstag herum. In 45 Beiträgen werden Grundrechtsverletzungen und -gefährdungen des vergangenen Jahres geschildert – sowie einige wenige Verbesserungen. Während die Verfassungsschutzberichte von Bund und Ländern lediglich die angeblichen Gefährdungen der freiheitlich demokratischen Grundordnung durch Organisationen und Parteien, Gruppen und Grüppchen schildern, die zu keinem Zeitpunkt je die Bundesrepublik ernsthaft haben in Gefahr bringen können, versteht sich der Grundrechte-Report als der wahre Verfassungsschutzbericht, der deutlich macht, dass die hauptsächlichen Gefährdungen für den Rechtsstaat und die Grundrechte vom Staat und seinen Institutionen ausgehen.

Der Öffentlichkeit vorgestellt wird der Grundrechte-Report von dem langjährigen Bundestagsabgeordneten und Parlamentarischen Geschäftsführer von Bündnis 90/Die Grünen, Volker Beck. Er erinnert anlässlich der Präsentation an die doppelte Funktion der Freiheitsbestimmungen der Verfassung: „Die Freiheiten des Grundgesetzes sind Garantie und Verheißung zugleich. Eine wache Zivilgesellschaft muss stets darüber wachen und immer neu dafür kämpfen, dass die Grundrechte, in denen sich die Unantastbarkeit der Menschenwürde konkretisiert, gewahrt bleiben.“

Ein Schwerpunkt des diesjährigen Berichtes sind die Einschränkungen von Freiheitsrechten und die überbordende Überwachung. Die Pariser Rechtsanwältin Dorothee Wildt kritisiert, dass trotz eines eindeutigen Urteils des Europäischen Gerichtshofs zur Unzulässigkeit der anlasslosen Vorratsdatenspeicherung der nationale Gesetzgeber das deutsche Gesetz nicht aufhebt, sondern daran festhält. Fredrik Roggan, Professor an der Hochschule der Polizei von Brandenburg, weist auf die Verfassungswidrigkeit der Quellen-TKÜ („Staatstrojaner“) und der Online-Durchsuchung hin. Der ehemalige Bundesdatenschutzbeauftragte Peter Schaar berichtet über den unkontrollierten Zugriff u. a. der Nachrichtendienste auf die biometrischen Verbunddateien anderer Behörden. Mehrere Autoren befassen sich mit den Eingriffen gegen den schwammigen Begriff des „Gefährders“. Benjamin Gremmelspacher schildert die rechtswidrige Überwachung des Freiburger Anwalts Moos durch den Verfassungsschutz. Heiner Busch stellt fest, dass im Jahr 2017 die Statistik der polizeilichen Todesschüsse eine Höchstzahl seit 1999 ausweist.

Aber auch zahlreiche Themen außerhalb des Sicherheits- und Überwachungsbereichs werden behandelt. Sophie Rotino berichtet über das Urteil des Bundesverfassungsgerichts, dass die Ehe für alle verfassungsrechtlich geboten ist. Alexander Graser schildert die Grundrechtsverletzungen durch den Pflegenotstand und mahnt die staatliche Schutzpflicht gegenüber Menschen in stationärer Pflege an. Die Sozialrichterin Julia Heesen schildert, wie Hartz IV-Empfänger wegen unsinniger Regelungen ihre Wohnung verlassen müssen. Till Müller-Heidelberg freut sich über Entscheidungen des Bundesverfassungsgerichts und des Europäischen Gerichtshofs, die die vorgesehenen Schiedsgerichte für ausländische Investoren im CETA- und TTIP-Abkommen für möglicherweise demokratiegefährdend erklären, und Jacqueline Neumann fordert anlässlich eines Münsteraner Urteils die überfällige Abschaffung des Gotteslästerungsparagrafen im Strafgesetzbuch.

Grundrechte-Report 2018 – Zur Lage der Bürger- und Menschenrechte in Deutschland.
Herausgeber: Till Müller-Heidelberg, Marei Pelzer, Martin Heiming, Cara Röhner, Rolf Gössner, Matthias Fahrner, Helmut Pollähne und Maria Seitz.
Fischer Taschenbuch Verlag, Frankfurt/M., Juni 2018,
ISBN 978-3-596-70189-6, 240 Seiten, 10,99 Euro.

Natürlich wird auch die Verurteilung der Medizinerin Kristina Hänel durch Maria Wersig behandelt und die Abschaffung oder Reform des § 219a StGB gefordert, der es Ärzten verbietet, die Öffentlichkeit darüber zu informieren, ob sie auch Schwangerschaftsabbrüche durchführen. Kristina Hänel wird bei der Präsentation stellvertretend für viele Fälle bei der Vorstellung des Grundrechte-Reports anwesend sein. Anlässlich der Vorstellung wiederholt sie ihr Anliegen, für das sie verurteilt wurde: „Ich möchte das Informationsrecht für Frauen zum Schwangerschaftsabbruch durchsetzen. Informationsrecht ist ein Menschenrecht. Gleichzeitig setze ich mich dafür ein, dass nie mehr eine Frau gezwungen wird, auf der Suche nach Informationen auf die widerlichen Seiten der Abtreibungsgegner gehen zu müssen.“

Schließlich befasst sich der Grundrechte-Report auch mit dem das Jahr 2017 beherrschenden Diesel-Skandal: Remo Klinger sieht angesichts der Untätigkeit der Bundesregierung eine „ungeschriebene Bereichsausnahme für die Automobilität“ und fordert die Schutzpflicht des Staates nach Art. 20 a Grundgesetz zum Schutz der Umwelt ein.

Anmerkungen

1 *Trägerkreis: Der Grundrechte-Report 2018 wird gemeinschaftlich herausgegeben von Humanistischer Union, vereinigt mit der Gustav Heinemann-Initiative | Bundesarbeitskreis Kritischer Juragruppen | Internationale Liga für Menschenrechte | Komitee für Grundrechte und Demokratie | Neue Richtervereinigung | PRO ASYL | Republikanischer Anwältinnen- und Anwälteverein | Vereinigung Demokratischer Juristinnen und Juristen. Ab 2019 wird das FIfF neues Mitglied des Trägerkreises.*

Perspektiven des Datenschutzes nach der Datenschutz-Grundverordnung

Bis vor wenigen Jahren pflegten nicht nur die Politik, sondern auch deutsche Gerichte das Bild, wonach das Datenschutz-Niveau hierzulande vorbildhaft sei und deutlich mehr Schutz biete als die europäischen Gemeinschaftsstandards. Dieses Bild ist mittlerweile überholt, wie nicht zuletzt die beiden Entscheidungen des Bundesverfassungsgerichts und des Gerichtshofs der Europäischen Union zur Vorratsdatenspeicherung zeigen: was in Deutschland noch als verfassungskonform galt, stufte das europäische Gericht als Verstoß gegen die Grundrechte-Charta und weitgehend unzulässig ein. Die Maßstäbe haben sich verschoben, grundrechtliche Schutzstandards (wie etwas das „Recht auf Vergessenwerden") werden in zunehmendem Maß auf europäischer Ebene definiert und durchgesetzt. Umso größer waren und sind die Erwartungen an die neue Datenschutz-Grundverordnung (DSGVO) der EU, die am 25. Mai 2018 auch in Deutschland anwendbar wird. Was beinhaltet das neue europäische Datenschutzrecht? Welche Zugewinne, aber auch welche Verluste für den Schutz der informationellen Selbstbestimmung gilt es zu verzeichnen? Und was ändert sich konkret für Bürger, Verbraucher und private Anbieter? Mit diesen Fragen befasst sich die neue Ausgabe der vorgänge in ihrem Schwerpunkt.

Der erste Beitrag des Themenschwerpunkts stammt von *Thilo Weichert*. Er stellt die Grundzüge der neuen Verordnung vor: ihre Ziele, ihre grundlegenden Prinzipien und Regelungsinhalte sowie ihren Anwendungs- und Geltungsbereich. Die Gewinne der Verordnung sieht er vor allem in einer stärkeren Systematik des Datenschutzrechts (die freilich durch zahlreiche nationale Öffnungsklauseln wieder verschenkt wird), in einigen neuen Betroffenenrechten (z. B. Breach Notification und Übertragbarkeit), in verbesserten Möglichkeiten ihrer Durchsetzung sowie in schärferen Sanktionsmöglichkeiten für die Aufsichtsbehörden.

Eine grundlegende Einordnung des neuen Datenschutzrechts nimmt *Alexander Roßnagel* vor. Er beschreibt die bisherige Entwicklung des Datenschutzrechts seit den 1970er Jahren, das zunächst als Reaktion auf maschinelle Informationsverarbeitungen in Großrechenanlagen entstand. Dabei macht er drei Stufen des Datenschutzrechts aus, die an technologische Entwicklungssprünge der Informationsverarbeitung gekoppelt sind: die Computerisierung von Abläufen; die zunehmende Vernetzung der IT-Systeme; die Durchdringung aller Lebensbereiche mit Smarten Technologien. Die DSGVO ist nach Roßnagels Einschätzung kaum in der Lage, die speziellen Risiken neuer Informationstechnologien adäquat einzuhegen. Von einigen kleinen Neuerungen (etwa dem Recht auf Datenübertragbarkeit oder den Vorgaben zur Systemgestaltung) abgesehen, bleibe die Verordnung auf dem Stand der alten EU-Datenschutzrichtlinie von 1995; eine wirkliche Modernisierung des Datenschutzrechts finde nicht statt. Letztlich beschränken sich die materiellen datenschutzrechtlichen Vorgaben der Grundverordnung auf ein zu allgemeines und formelhaftes Niveau, das den „Bäcker um die Ecke" mit den gleichen Maßstäben wie Facebook behandle. Konkrete Antworten auf spezielle Risiken, wie sie etwa mit Sozialen Netzwerken, mit Cloud Computing, Big Data oder „intelligenter" Videoüberwachung einher gehen, suche man daher in der Verordnung vergebens. Ihren größten Gewinn sieht Roßnagel noch in den teilweise gestärkten Kontrollkompetenzen und den verschärften Sanktionsmöglichkeiten gegen Datenschutzverstöße.

Nach dieser Darstellung des europäischen Standards widmet sich *Peter Schaar* der Umsetzung der europäischen Vorgaben im neuen Bundesdatenschutzgesetz (BDSG). Obwohl die DSGVO als Verordnung in allen Mitgliedstaaten unmittelbar geltendes Recht darstellt, das keiner speziellen Umsetzung in deutsches Recht bedarf, enthält sie 70 Öffnungsklauseln, mit deren Hilfe die nationalen Gesetzgeber einzelne Bereiche des Datenschutzrechts (z. B. für Gesundheitsdaten, die Datenverarbeitung von Berufsgeheimnisträgern oder Kirchen) gesondert regeln können bzw. dort, wo die Verordnung selbst keine Regelungen trifft, sogar erlassen müssen. Mit den Öffnungsklauseln bietet sich die Chance, auf besondere Gefahren einzelner Sachgebiete sowie auf nationale Tradierungen zu reagieren. Von dieser Möglichkeit hat der Bundesgesetzgeber im vergangenen Jahr reichlich Gebrauch gemacht, als er das Bundesdatenschutzgesetz (BDSG) an die Vorgaben der DSGVO anpasste. Schaar geht zunächst auf die Entstehungsgeschichte der Grundverordnung ein, vor deren Hintergrund die Öffnungsklauseln zu verstehen sind. Dann stellt er das neu gefasste BDSG in Grundzügen vor, das nicht nur die bestehenden Öffnungsklauseln exzessiv nutzt, sondern zum Teil sogar darüber hinaus Sonderregeln aufstellt, mit denen der deutsche Datenschutzstandard gegenüber der DSGVO abgesenkt wird: So werden die Rechte der Betroffenen beschnitten,

die Zuständigkeit der Aufsichtsbehörden sowie ihre Sanktionsmöglichkeiten gegenüber staatlichen Stellen deutlich eingeschränkt. Für die Zukunft sieht Schaar sogar die Gefahr, dass sich andere Mitgliedstaaten an der deutschen Umsetzung auf Minimalniveau orientieren und Deutschland zum Negativvorbild eines Unterbietungswettbewerbs im Datenschutz werde.

Nach diesen eher grundsätzlichen Abhandlungen widmen wir uns im Folgenden konkreten Einzelfragen der Datenschutzreform: *Marie-Theres Tinnefeld* diskutiert die Möglichkeiten und Grenzen der selbstbestimmten Einwilligung durch Betroffene, die nach wie vor wichtigste Legitimationsquelle für Datenverarbeitungsvorgänge ist. Tinnefeld schildert zunächst den menschenrechtlichen Kontext des Datenschutzes und der freien Einwilligung, bevor sie die konkreten Anforderungen an die Freiwilligkeit, die Folgenabschätzung, die Transparenz und die Formerfordernisse bzw. Nachweispflichtigkeit der Erteilung darstellt. Zum Schluss ihres Beitrags zeigt sie die Grenzen der Einwilligung auf, d. h. welche Datenverarbeitung auch bei etwaiger Zustimmung der Betroffenen unzulässig ist. Angesichts der immer komplexeren Verarbeitungsprozesse, die gerade bei smarten, global vernetzten Systemen zum Einsatz kommen, bleibt jedoch offen, wie weit das Konzept einer informierten und sachkundigen Entscheidung heute noch realistisch ist, wo die AGB-Texte vieler Angebote fast so umfangreich wie klassische Romane sind und die Konsequenzen selbst für IT-kundige kaum zu überblicken sind.

Marit Hansen und *Sven Polenz* knüpfen an diese grundsätzlichen Betrachtungen an und stellen die wichtigsten Änderungen vor, die sich aus Verbrauchersicht mit der DSGVO ergeben. Sie erläutern die praktischen Voraussetzungen, die für eine wirksame Einwilligung erfüllt sein müssen und geben anschließend einen Überblick über die wichtigsten Neuerungen bei den Verbraucherrechten, etwa den Informations- und Benachrichtigungspflichten. Nach einem kurzen Überblick der technischen und systemischen Vorgaben zum Datenschutz gehen sie auf die Möglichkeiten zur Durchsetzung der Betroffenenrechte sowie die Klage-, Untersagungs- und Sanktionsmöglichkeiten von Verbraucherverbänden bzw. Aufsichtsbehörden ein.

Wenn die rechtlichen Möglichkeiten zur Durchsetzung von Datenschutz-Anforderungen an ihre Grenzen kommen, wird häufig der Ruf nach einem bereits auf technischer bzw. systemischer Ebene verankerten Datenschutz laut. Privacy by design und Privacy by default finden sich als Vorgaben auch in der DSGVO wieder. Inwiefern sie dazu beitragen können, das europäische Schutzniveau anzuheben, ist Thema des Beitrags von *Clemens Heinrich Cap*. Bevor er diese Frage beantwortet, geht er zunächst auf den Stellenwert von Privatheit und informationeller Selbstbestimmung in der heutigen Gesellschaft ein. Daran schließt eine Bestandsaufnahme an, welche Möglichkeiten für einen stärkeren Datenschutz sich ergeben, wenn dessen Anforderungen von Anfang an beim Technik- und Ablaufdesign berücksichtigt werden. Cap warnt jedoch vor zu hohen Erwartungen an einen programmierten Datenschutz, denn die Gestaltung neuer Informationstechniken folge i. d. R. anderen (mutmaßlichen) Nutzerwünschen, und das schwächste Glied in der IT-Systemreihe seien immer noch die nach Bequemlichkeit strebenden Anwender, die Sicherheitsvorkehrungen außer Kraft setzen. Cap fordert deshalb eine digitale Aufklärung 2.0, um den unmündigen Umgang mit IT-Systemen und ihrer Datenverarbeitung zu beenden.

Mit einigen Banalisierungen und Verengungen des Datenschutz-Begriffes befasst sich *Martin Rost*: Seine Kritik wendet sich dagegen, Datenschutz allein auf die Minimierung von technischen Risiken und damit ein Problem der Systemsicherheit zu reduzieren. Das Ziel des Datenschutzes sei nicht die Bewahrung einer ‚idyllischen Privatheit', die sich von der Gesellschaft abschotten will, sondern bestehe darin, den Einzelnen gegenüber staatlicher wie unternehmerischer Übermacht zu bewahren, die sich aus der Verfügbarkeit über Daten ergeben kann. Wenn die DSGVO daher von den Risiken der Datenverarbeitung spreche (wie in Erwägungsgrund 75 der Verordnung), dürfe die Risikoanalyse nicht auf Missbrauchs- und Fehlerszenarien beschränkt bleiben, sondern müsse auch die strukturellen Gefahren für die Betroffenen in den Blick nehmen, die mit einer fehlerfrei funktionierenden Verarbeitung verbunden sind. Rost spannt dazu acht Dimensionen des Risikobegriffs auf, die für eine umfassende Folgeabschätzung, aber auch für eine wirksame Datenschutzkontrolle zu berücksichtigen sind.

Den Themenschwerpunkt schließen wir mit drei Beiträgen ab, die über den Tellerrand der DSGVO hinaus schauen: Parallel zur DSGVO wurde auch eine europäische Richtlinie zur Datenverarbeitung bei Strafverfolgungs- und Strafvollstreckungsbehören verabschiedet (EU-RL 2016/680), die einen einheitlichen Datenschutzstandard in diesem Bereich vorgibt. Mit dem Anwendungsbereich der Richtlinie, den zahlreichen Ausnahmen und ihrer ersten Umsetzung im Bundesdatenschutzgesetz sowie im BKA-Gesetz befasst sich der Beitrag von *Hartmut Aden*.

Florian Glatzer geht auf die Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-Verordnung) ein, mit der die Datenschutzstandards für den gesamten digitalen Kommunikationsbereich neu geregelt werden. Mit der Verordnung soll der Schutz vertraulicher Kommunikation, der nach der bisherigen EU-Richtlinie nur für klassische telefoniegestützte Kommunikation (einschließlich SMS) gilt, auf die neuen netzbasierten Angebote von Instant Messenger Diensten (bspw. WhatsApp) und Sozialen Netzwerken (etwa Facebook) erweitert werden. Die neue ePrivacy-Verordnung sollte ursprünglich zeitgleich mit der DSGVO in Kraft treten – bisher liegen aber erst der Kommissionsentwurf und die Stellungnahme des EU-Parlaments vor, im Herbst beginnen voraussichtlich die Trilog-Verhandlungen mit dem Rat.

Martin Kutscha nimmt einen kürzlich erschienenen Sammelband zur „Informationellen Selbstbestimmung im digitalen Wandel" zum Anlass, um die ketzerische Frage zu stellen, ob das Datenschutz-Grundrecht überhaupt noch eine realistische Zukunft habe. Mit seinem Kommentar beenden wir diesen Schwerpunkt.

(*Aus dem Editorial von Sven Lüders*)

Dazu enthält die Ausgabe weitere Hintergrundberichte und Rezensionen. Die Beiträge von Alexander Roßnagel und Marie-Theres Tinnefeld sind mit freundlicher Genehmigung auch in dieser Ausgabe der *FIfF-Kommunikation* enthalten.

vorgänge #221/212 Perspektiven des Datenschutzes nach der Datenschutz-Grundverordnung, 57. Jahrgang, Mai 2018, Hefte 1/2, ISSN 0507-4150

Wissenschaft & Frieden 2/2018

„Wissenschaft im Dienste des Militärs“

Seit der Gründung von *Wissenschaft und Frieden* vor 35 Jahren beleuchtet die Zeitschrift kritisch die Beziehungen zwischen ziviler und militärischer Forschung und Technik. In dieses Geflecht eingebunden sind zahlreiche Akteure, wissentlich und willentlich arbeitende oder eher durch die Hintertür, z. B. an Universitätsinstituten oder Einrichtungen der Fraunhofer-Gesellschaft. Um diese Ambivalenz, um die Dual-use-Nutzung von Forschungsergebnissen oder die dezidierte Forschung für das Militär dreht sich der Schwerpunkt von W&F 2/2018. Die Artikel befassen sich mit Rüstungsforschung in Deutschland und der EU, in der Mathematik und der Kultur- und Sozialanthropologie, und fragen nach der Rolle der Friedensforschung in diesem Feld.

Im einzelnen schreiben:

- *Jürgen Scheffran*: Militarisierung oder Zivilisierung?
- *Nicole Gohlke*: „Zivile“ Forschung für militärische Zwecke
- *Cornelia Mannewitz*: Der Einfluss von Militär und Rüstungsindustrie auf die Wissenschaft
- *Eric Töpfer*: Paradigmenwechsel? – Rüstungsforschung in der EU
- *Thomas Gruber*: Mathematik und Krieg – Forschung für die moderne Kriegsführung
- *Benjamin Hirschfeld*: Ein „Cultural Turn“? Sozial- und Kulturanthropologie im Auftrag des Militärs
- *Thomas Mickan*: Friedensforschung im Dienst des Militärs?
- *Thomas Mickan*: Nachgefragt: Was ist epistemische Gewalt? Ein Interview mit Claudia Brunner

Außerhalb des Schwerpunktes geht es um Deutschlands militärische Rückkehr auf die Weltbühne (Werner Ruf), um das letztes Jahr vereinbarte Atomwaffenverbot (Rainer Lucht), um Syrien und den Einsatz von Chemiewaffen (Wissenschaftlicher Dienste des Bundestages) und – anstelle eines Nachrufs auf Ekkehard Krippendorf – um die alte Weltmilitärordnung. Der Gastkommentar von Philipp Naucke und Anika Oettler schildert die Gefahr für den Frieden in Kolumbien und die kommentierte Presseschau von Jürgen Nieth „USA a-lone“ gibt einen Überblick über die Reaktionen auf die Ankündigung Trumps, die internationalen Vereinbarungen mit dem Iran zu brechen und die Sanktionen einseitig wieder in Kraft zu setzen.

Ergänzt werden die Artikel durch die Reden zur Verleihung des Göttinger Friedenspreises 2018 an Wissenschaft & Frieden. *Wachsendes Ungleichgewicht – Cyberrüstung und zivile IT-Sicherheit* stehen im Mittelpunkt des W&F beiliegenden Dossiers, das von der Informationsstelle Wissenschaft und Frieden in Zusammenarbeit mit dem FIfF herausgegeben wird und auch dieser Ausgabe der FIfF-Kommunikation beigelegt ist.

Wissenschaft & Frieden, 2/2018: „Wissenschaft im Dienste des Militärs“, 9,00 € Innland, EU plus 3,00 € Porto.

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

Bitte um Vorkasse: Sparkasse KölnBonn, DE86 3705 0198 0048 0007 72, SWIFT-BIC COLSDE33XXX

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

FIfF e.V.

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

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

FIfF-Mailinglisten

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

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

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

FIfF online

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

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

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

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

FIfF-Beirat

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

FIfF-Vorstand

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

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck, Eberhard Zehendner
Schwerpunktredaktion	Stefan Hügel, Rainer Rehak
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de*. Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
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
Cover	https://commons.wikimedia.org/wiki/Category:Edward_Snowden_in_art#/media/
Druck	Meiners Druck, Bremen

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

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

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

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

Aktuelle Ankündigungen

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

34. FIfF-Konferenz – #FIfFKon18
„Brave New World" – Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme
28. bis 30. September 2018, Berlin

~ Bits & Bäume ~
Die Konferenz für Digitalisierung und Nachhaltigkeit
17. bis 18. November 2018, Berlin

FIfF-Kommunikation

3/2018 „Informatik und Gesellschaft"
Stefan Hügel
Redaktionsschluss: 3. August 2018

4/2018 „Alter(n)sgerechte Informatik"
Eberhard Zehendner, Stefanie Jäckel
Redaktionsschluss: 2. November 2018

1/2019 „Brave New World"
Rainer Rehak, Benjamin Kees, Anne Schnerrer u. a.
Redaktionsschluss: 1. Februar 2019

W&F – Wissenschaft & Frieden

4/17 Eingefrorene Konflikte (mit Dossier 85: Transhumanismus und Militär)
1/18 USA – eine Inventur
2/18 Wissenschaft im Dienste des Militärs? (mit Dossier 86: Cyberrüstung und zivile IT-Sicherheit)

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#219 Soziale Menschenrechte
#220 Europa in der Krise
#221/222 Datenschutz nach der DSGVO
#223 Bürgerrechte im Sport
#224 Die Rechte im Osten?

DANA – Datenschutz-Nachrichten

1/17 Verbraucherschutz
2/17 BDSG-Nachfolgegesetz
3/17 40 Jahre DVD
4/17 Gesundheitsdatenschutz
1/18 Polizeigesetze

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung), Michael Jacobsen
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

FIfF e.V.

Vorstellung des Weizenbaum-Instituts für die vernetzte Gesellschaft

Am 5. Juni 2018 stellten WissenschaftlerInnen auf dem regelmäßig stattfindenden „Netzpolitischen Abend" das kürzlich gegründete Weizenbaum-Institut für die vernetzte Gesellschaft vor. In der gut gefüllten c-base (Berlin) durften auch ein paar Worte zum Namensgeber Joseph Weizenbaum nicht fehlen, der als kritischer Informatiker und überzeugter Antimilitarist auch Mitgründer und langjähriges Mitglied des FIfF war. Wir wünschen dem Institut daher alles Gute beim Weiterentwickeln der kritischen Analysen Weizenbaums.

Es gibt von der Veranstaltung auch einen Mitschnitt (das Weizenbaum-Institut kommt ab 2:55)
https://digitalegesellschaft.de/2018/06/72-npa-videos-zum-nachschauen/

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