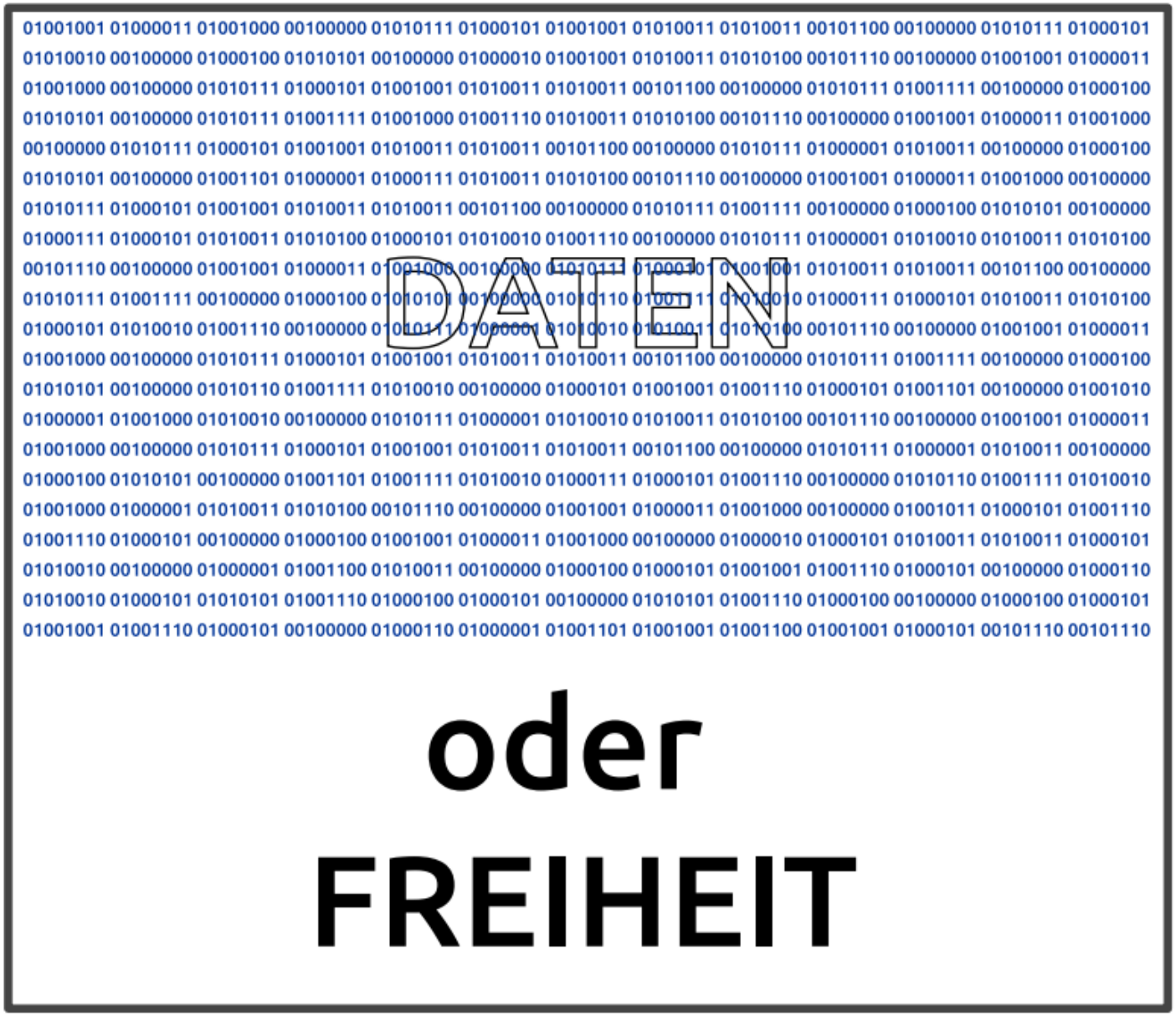

oder
FREIHEIT

Ein Debattenbeitrag.

Sebastian Raupach

Gerne können Sie mir Ihre Anmerkungen und Kritik zusenden:
https://www.europahelden.eu/datenfreiheit_kommentar.html

Braunschweig, Mai 2021 (v20210516)

Art. 2
(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

[…]

Art. 5
(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.

(aus: Grundgesetz für die Bundesrepublik Deutschland)

Jeder hat das Recht auf seine eigene Meinung, aber er hat keinen Anspruch darauf, dass andere sie teilen.

(M. Rommel, CDU)

[Das Persönlichkeitsrecht] umfasst […] auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden […]. Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. […] Sie ist vor allem deshalb gefährdet, weil […] heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person […] technisch gesehen unbegrenzt speicherbar und jederzeit […] abrufbar sind. Sie können darüber hinaus […] mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsabbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. […] Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.

(Bundesverfassungsgericht, Urteil vom 15. Dezember 1983 („Volkszählungsurteil“))

Datenschutz ist was für Gesunde.

(der spätere Bundesminister Jens Spahn (CDU) in: Spahn/Müschenich/Debatin: „App vom Arzt“, Herder Verlag, 2016)

Artikel 1 - Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

[…]

Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

*a) auf rechtmäßige Weise [...] in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („*Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz*“);*

*b) für festgelegte, eindeutige und legitime Zwecke erhoben werden […] („*Zweckbindung*“);*

*c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („*Datenminimierung*“);*

*d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; [...] („*Richtigkeit*“);*

*e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; […] („*Speicherbegrenzung*“);*

*f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung [...] („*Integrität und Vertraulichkeit*“);*

(aus: Europäische Datenschutz-Grundverordnung vom 27. April 2016)

Von schlechtem oder dysfunktionalem Datenschutz spreche ich, wenn er nicht mehr zu den Gegebenheiten passt oder wenn er wichtige soziale Güter unmöglich macht. Dann ist Datenschutz auch ein Innovationshemmer.

(Prof. Dr. Alena Buyx, Vorsitzende des Deutschen Ethikrates, in einer Werbebroschüre des Unternehmens „Google“, 2021)

Halten wir in unserem Leitfaden für die nächste Katastrophe *zunächst einmal fest, dass alle Risikosysteme von ihren Auftraggebern für sicher gehalten werden (andernfalls würden sie nicht gebaut). Häufig stellt sich sogar heraus, dass diese Systeme noch wenige Monate vor einer Katastrophe einer Routineüberprüfung unterzogen worden waren.*

(aus: Prof. Dr. Charles Perrow, *Normale Katastrophen*, 2. Auflage, 1992)

Inhaltsverzeichnis

Einleitung

Als die Strahlungsmessgeräte im schwedischen Kernkraftwerk Forsmark am Morgen des 28. April 1986 Alarm schlagen, ist es der erste Vorbote einer Katastrophe biblischen Ausmaßes.

Bei der sofort eingeleiteten Überprüfung der Anlage kann zunächst kein Grund für die erhöhten Strahlungswerte gefunden werden. Erst als zwölf Stunden später eine dürre Nachricht der sowjetischen Staatsnachrichten veröffentlicht wird, kommt nach und nach ans Tageslicht: Im mehr als 1000 Kilometer entfernten Tschernobyl hat es einen katastrophalen Reaktorunfall gegeben.

Ähnlich wie 2019 die chinesischen Behörden in Wuhan versuchen auch 1986 die sowjetischen Behörden zunächst, die Fakten der sich abzeichnenden Katastrophe und die Berichterstattung dazu zu unterdrücken. Daher wird es noch mehrere Tage dauern und unabhängige Messungen erfordern, bis das Ausmaß der Katastrophe klar wird: Bereits zwei Tage zuvor, am 26. April, hatte sich in Tschernobyl ein „GAU“ ereignet, der „Größte Anzunehmende Unfall“:

Die kontrollierte Kernspaltung war außer Kontrolle geraten, mehrere Explosionen hatten die Ummantelung des Reaktors zerstört, das Graphit im Reaktor war in Brand geraten. Und während das Graphit in den folgenden Tagen tonnenweise verbrennt, transportiert die Hitze riesige Mengen radioaktiver Teilchen hoch in die Atmosphäre. Dort werden sie von den herrschenden Winden über große Gebiete verteilt.

Rund 200000 km² der Oberfläche unseres Planeten wurden massiv radioaktiv belastet, allein im Gebiet der heutigen Ukraine, Belarus‘ und Russlands waren fünf Millionen Menschen unmittelbar betroffen[1]. 330.000 Menschen mussten aus der unmittelbaren Umgebung evakuiert, eine Fläche von 6400 km² für die menschliche Nutzung dauerhaft aufgegeben werden[2]. Für das Jahr 1986 erhöhte sich selbst im weit entfernten Deutschland die jährliche Strahlungsdosis um das Zehnfache. Und noch über ein Vierteljahrhundert nach der Katastrophe ist Tschernobyl von einer Sperrzone mit einer Fläche von 4300 km² umgeben[3], entsprechend einem Kreis mit 37 km Durchmesser.

Über die Reaktorkatastrophe von Tschernobyl lässt sich Vieles sagen. Nur eins nicht: Dass sie eine Überraschung war.

Nicht nur später, wie im japanischen Fukushima, auch schon früher hatte es Reaktorunfälle gegeben. Die gerade noch glimpflich verliefen. Wie beispielsweise in Harrisburg (Three Mile Island) im Jahr 1979, als es bereits zu einer partiellen Kernschmelze kam[4].

Seit den 1970er Jahren gab es unter anderem in Deutschland eine immer aktivere Bürgerbewegung, die unentwegt auf die Gefahren und Risiken der Kernkraft hinwies. In Westdeutschland trug sie zur Gründung der Graswurzelpartei „Die Grünen“ im Jahr 1980 bei. Auch in der DDR gab es kritische Stimmen zur Nutzung der Kernspaltung. Diese hatten allerdings aufgrund der Unterdrückung des Rechts auf freie Meinungsäußerung und staatlich gelenkter Medien[5] nie die Chance, sich in gleicher Weise Gehör zu verschaffen wie ihre Mitstreiter in der Bundesrepublik[6].

---

1 Landeszentrale für politische Bildung BW: „*Die Atomkatastrophe von Tschernobyl – 26. April 1986*“ (https://www.lpb-bw.de/tschernobyl, abgerufen 27.01.2021)
2 https://de.wikipedia.org/wiki/Nuklearkatastrophe_von_Tschernobyl, abgerufen 25.01.2021
3 Landeszentrale für politische Bildung BW: „*Die Atomkatastrophe von Tschernobyl – 26. April 1986*“
4 z.B.: Charles Perrow: „Normale Katastrophen“, Campus Verlag Frankfurt/New York, 2. Aufl. (1992)
5 Einer ähnlichen Situation wie heute in China und wohl auch in Russland unter Wladimir Putin.
6 Siehe z.B. https://de.wikipedia.org/wiki/Anti-Atomkraft-Bewegung_in_Deutschland, abgerufen 25.01.2021

Wenn aber die Risiken und die katastrophalen Gefahren öffentlich bekannt waren – warum wurde jahrzehntelang mit Milliardeninvestition eine potentiell katastrophale Entwicklung befeuert? Warum konnte es im schwedischen Kernkraftwerk Forsmark im Jahr 2006 doch noch zu einer Beinahe-Katastrophe kommen[7]? Warum dauerte es nach Tschernobyl noch über 15 Jahre, bis man sich zum Ausstieg aus einem bekannten Hochrisikosystem entschließen konnte? Warum brauchte es die Katastrophe von Fukushima, um die Entscheidung umzusetzen?

In seinem erstmals 1984 erschienenen Buch „Normale Katastrophen“ versucht der amerikanische Professor Charles Perrow, eine Antwort auf die Fragen zu geben, was Hochrisikosysteme eigentlich ausmacht und warum sie immer wieder realisiert werden.

Perrow zufolge steuern Großtechnologien oder Systeme nahezu unvermeidlich in die Katastrophe, wenn zwei Zutaten in ausreichender Menge zusammenkommen: Komplexität und starke Wechselwirkungen - ein Rezept, das kein menschliches Versagen als Schein-Erklärung erfordert. Zumal das vermeintliche „menschliche Versagen“ nur zu oft ganz normales und realistischerweise zu erwartendes menschliches Verhalten sei.

„Hohe Komplexität“, also ein System, das für die damit befassten Menschen nicht mehr durchschaubar ist, plus „starke Wechselwirkung“ zwischen den Teilen des Systems: Diese Zutaten sorgen dafür, dass es - wie im Fall des Flugzeugtyps Boeing 737 MAX - zu unvorhergesehenem, „chaotischen“ Verhalten des Gesamtsystems kommt.

Komplex und eng vernetzt: Das ist das einfache Rezept für eine Katastrophe.

Wenn Ihnen dabei spontan „Digitalisierung“ als Schlagwort einer Gesellschaft in den Sinn kommt, die immer stärker von der Erzeugung, zentraler Speicherung, algorithmengesteuerter Verarbeitung und Rückspeisung von Datenströmen durchzogen wird, ist das durchaus beabsichtigt.

Eine Anekdote aus dem Bekanntenkreis: Ein Sohn erzählte, dass er sich selbst „gegoogelt“ habe, und dass in den Suchergebnissen merkwürdigerweise seine Mutter aufgetaucht sei. Das war in der Tat merkwürdig. Seine Mutter war in keinem „Sozialen Netzwerk“ aktiv und auch sonst gab es keine im Internet veröffentlichten Bezüge zwischen den beiden. Noch merkwürdiger: Sein Vater tauchte nicht in den Suchergebnissen auf. Der Unterschied? Die Mutter verwendete bis dahin für ihre privaten E-Mails - z.B. für solche mit der Schule ihres Sohnes - den Mailserver „Gmail“ von Google... Der Vater nicht.
Wir werden auf die „Datenschutz“-Erklärung von Google zurückkommen.

Wie kommt es aber dazu, dass Hochrisikosysteme oder Implementierungen einer Technologie, die realistischerweise mit katastrophalen Konsequenzen einhergehen, trotzdem über Jahre mit enormen Ressourcen auf- und ausgebaut werden? Und dass sie selbst im Angesicht der Katastrophe noch mit glühendem Eifer verteidigt werden?

Die Antwort ist einfach und steckt in dem Wort „realistischerweise“: um die Katastrophe zu vermeiden, müsste man erst einmal die Realität und auch unliebsame Fakten anerkennen.

Charles Perrow weist in seinem Buch auf „ausgelagerte Kosten“[8] als eine Ursache für realitätsfremde Fehlentwicklungen hin. Diese Auslagerung von Kosten bzw. Konsequenzen macht es leicht, sie zu ignorieren und lassen hochriskante Fehlentwicklungen erst weniger riskant und sogar wirtschaftlich attraktiv erscheinen.

---

7 z.B. Der Spiegel: „*Der Mann der den GAU verhinderte*“ (4.8.2006), https://www.spiegel.de/politik/ausland/akw-stierfall-in-schweden-der-mann-der-den-gau-verhinderte-a-430234.html, abgerufen 27.01.2021

8 Im Original: „*externalities*“

In manchen Fällen sind die „Kosten“, die Konsequenzen im Fall einer Katastrophe vielleicht tatsächlich erst einmal ausgelagert in dem Sinne, dass sie Spätere oder Andere treffen, die von der Hochrisikotechnologie unter Umständen nicht einmal profitieren.

Ein Beispiel dafür sind die ersten Kosten, die für ein seit rund 200 Jahren laufendes Großexperiment anfallen. Das Experiment besteht darin, innerhalb weniger Jahrhunderte einen möglichst großen Teil des Kohlenstoffs, der über rund 1,5 Milliarden Jahre der einst lebensfeindlichen Atmosphäre unseres Planeten entzogenen wurde, in Form von CO_2 wieder in die Atmosphäre zurückzublasen. Die ersten Kosten z.B. in Form steigender Meeresspiegel tragen ausgerechnet Südsee-Staaten auf der anderen Seite der Erde wie Tuvalu, die weder an der industriellen Revolution teilnahmen noch um Erlaubnis gefragt wurden. Gleichzeitig rufen sich aber auch rund um den Globus die fälligen Kosten für alle immer stärker in Erinnerung, in Form von Extremwetter wie Dürren, Stürmen und Überflutungen.

Bewusst oder unbewusst werden, so Perrow, so lange wie möglich Kosten und Konsequenzen ausgeklammert oder ignoriert, die mit dem Aufbau von „Katastrophensystemen“ einhergehen. Mit anderen Worten: Der Boden für die nächste Katastrophe ist bereitet, wenn die Realität und Fakten verdrängt, verleugnet, relativiert oder zurechtgebogen werden.

Muss man dazu ein krankhafter Lügner und Volksverführer sein wie der frühere US Präsident Trump? Ein eiskalt kalkulierender Geheimdienstoffizier und Propaganda-Fachmann an der Spitze einer gelenkten Demokratie wie der ewige russische Präsident Putin? Oder autokratischer Generalsekretär eines zensurgebeugten Ein-Parteien-Staates mit dem Staatsziel der totalen Überwachung und Kontrolle seiner Bürgerinnen und Bürger?

Na gut, ich nehme mal an, es hilft.

Aber ich denke, es kann auch schon reichen, einfach ein ganz normaler Mensch mit all seinen menschlichen Schwächen und Fehlern zu sein. Fehler, zu denen Wunschdenken ebenso gehört wie der Wunsch nach Anerkennung oder die Sorge, „abgehängt“ zu werden. Nur zu leicht gerät man so in scheinbar bester Absicht in eine Art selbst gestellter psychologischer Falle:

Jeder hat wohl schon einmal das Gefühl gehabt, vor einer scheinbar unauflösbaren Aufgabe zu stehen und (hoffentlich) auch das Erlebnis der Erleichterung und Euphorie, wenn es plötzlich doch gelingt. Genau das erleben auch Wissenschaftler und Ingenieure.

Manchmal sind es Generationen von Wissenschaftlern und Technikern, die sich vergeblich an der Lösung eines Problems versuchen. Sich aufgrund der technischen Begrenzungen ihrer Zeit allenfalls mit umständlichen Lösungen für wenige Spezialfälle zufriedengeben müssen. Um so überschwänglicher die Euphorie, wenn aufgrund einer neuen Entwicklung oder einer neuen Entdeckung bisher unüberwindliche Hürden einfach fallen. Plötzlich scheint die Lösung für alle Probleme der Welt zum Greifen nah.

Die gesamte Menschheit mit Energie versorgen? Dank Kernspaltung kein Problem. Vielleicht kann in Zukunft jeder statt eines Kohleofens oder eine Ölheizung einen kleinen Kernreaktor im Keller haben – warum nicht?

Die perfekte Gesellschaft? Optimierung des Alltags und der Menschen? Totale Ehrlichkeit? Dank besserer Speichertechnologien, riesiger Rechenkapazitäten, neuer Algorithmen und enger Vernetzung kein Problem! In Zukunft kann jede und jeder alles selbst in der Hand haben, sich selbst und sein Umfeld optimieren, seine intimsten Gedanken und Gefühle ständig mit allen teilen, kontinuierlich Rückmeldung bekommen. Statt Privatsphäre totale Ehrlichkeit, in der alle alles wissen und Algorithmen uns ständig erfassen, unseren Alltag durchplanen und uns besser kennen und formen als unser Partner oder unsere Freunde - die perfekte Welt in Reichweite!

Tja, und dann kommt der verstörende Moment, in dem man merkt, dass nicht alle Menschen die Begeisterung teilen. Sie vielleicht sogar den großartigen Zielen oder dem doch so offensichtlichen Weg dorthin kritisch gegenüber stehen. Und wenn man nicht aufpasst, ist ein psychologisch (Fehl-)Schluss sehr naheliegend und die Falle schnappt zu.

Nämlich mit dem Schluss, dass die anderen nur zu dumm oder zu uninformiert sind. Dass man die anderen nur für die Großartigkeit der eigenen Ziele begeistern muss, die man bloß besser „verkaufen“ muss. Die Kritiker müssen doch halsstarrig, böswillig oder dumm sein oder haben es bestenfalls einfach nur noch nicht verstanden. Gerade dann ein besonders verlockender Gedanke, wenn die Kritiker weniger von der Materie verstehen als man selbst (was für Fachexperten leicht auf 99,99% der Bevölkerung zutrifft…).

So kann sich aus dem Gefühlsmix von Euphorie und Unverstandenheit nur zu schnell ein missionarischer, blinder Eifer entwickeln, die Zweifler mit allen Mitteln dazu zu bringen, die Großartigkeit des angestrebten Systems zu erkennen. Sie notfalls zu ihrem Glück zu zwingen – zu ihrem eigenen Besten! Das Tückische an dem Fehlschluss: Er verhindert, sich in Ruhe mit sachlich geäußerter Kritik inhaltlich auseinanderzusetzen und sie als Chance zu sehen, die eigenen Überzeugungen zu überprüfen.

Als letzte Zutat fehlt dann nur noch eine gesellschaftlich einflussreiche Schar blind gläubiger „Jünger“, um den Weg für Hochrisikosysteme frei zu machen. Jünger, die mit gesundem Halbwissen jede Kritik abtun als Ausdruck von Unwissenheit der noch nicht Erleuchteten. Gläubige Anhänger, die für alle sich abzeichnende Probleme Entschuldigungen wie „Kinderkrankheiten“ und „Umsetzungsprobleme“ finden, die durch Geduld, festen Glauben und unbeirrtes Verfolgen der angestrebten Ziele von ganz alleine verschwinden...

Damit hat man das flankierende Ökosystem für katastrophale Fehlentwicklungen geschaffen, das selbst in freiheitlichen Gesellschaften zu dem Versuch führt, gesellschaftliche Korrekturmechanismen zu umgehen.

Ein Extrembeispiel für diese psychologische Falle aus dem politischen Bereich sind rechtsextreme Akteure, die scheinbar einfache, in der Konsequenz aber katastrophale Antworten auf gesellschaftliche Fragen liefern. Und deren Anhängerschaft lieber die Realität ignoriert und aufgibt als ihre Überzeugungen; die die Augen vor allem verschließt, was nicht zu ihren Überzeugungen passt, da für sie Verschwörungsmythen glaubwürdiger sind als der Glaube an den Menschen.

Ein subtileres, mit einer freiheitlichen Demokratie aus meiner Sicht aber ebensowenig vereinbares Beispiel werden wir auf den folgenden Seiten näher anschauen: die Einführung zentraler Datenbanken für medizinische Daten.

Wir werden sehen, wie auch dort der Mix aus euphorischer Technikgläubigkeit und dem Gefühl fehlenden Verständnisses der Bürgerinnen und Bürger zu einem missionarischen Eifer führt, der sich blind und taub stellt für die Wirklichkeit und alle Warnsignale und der die Kosten des Hochrisikosystems konsequent ignoriert.

Gleichzeitig haben wir als Bürgerinnen und Bürger in einer freiheitlichen Demokratie die Chance, solche Fehlentwicklung zu korrigieren und Hochrisikosysteme unserer Daten zu verhindern oder zu entschärfen.

Wir können aktiv werden, uns informieren, hinschauen, unsere Kritik äußern und diskutieren. Wir können nachfragen und notfalls vor Gericht ziehen.

Wir können die Chancen nutzen, die uns das Verfassungsgericht mit dem Recht auf informationelle Selbstbestimmung und die Europäische Union mit der „Datenschutz-Grundverordnung“ eröffnet haben.

Wir tragen die Verantwortung für unsere Daten und für das, was mit ihnen geschieht.

Unsere Daten gehören uns.

Kein Vorwort

Falls Sie beim Blick auf die Seitenzahl dieses Debattenbeitrags erschrocken festgestellt haben, dass es mehr als drei sind, habe ich hier ein Angebot für Sie. Auf den nächsten drei Seiten habe ich versucht, einige zentrale Punkte kurz und knapp zusammenzufassen.

Wenn Sie den Rest nicht (oder noch nicht) lesen wollen, können Sie also diese Mini-Version lesen. Und den Rest einfach danach, wenn Sie neugierig geworden sind oder sich für die Quellen interessieren.

Wenn Sie dagegen sowieso alles lesen wollen, würde ich vorschlagen, diese Kurzzusammenfassung erst einmal zu überspringen.

Aber: Wie Sie wollen. ;-)

Teil 0 – In aller Kürze

Zum 1. Januar 2021 hat der Gesetzgeber eine „elektronische Patientenakte“ eingeführt. Dabei handelt es sich um eine rein virtuelle Patientenakte in Form eines Datensatzes in zentralen Datenbanken, in denen potentiell alle relevanten medizinischen Daten aller Bürgerinnen und Bürger gespeichert werden können.
Es ist davon auszugehen, dass sich aufgrund der Mitgliederzahlen und technischen Gegebenheiten der Krankenkassen ein Großteil der Daten in wenigen zentralen Datenbanken konzentrieren wird. Auf die Datenbanken kann aus technischer Sicht über das Internet grundsätzlich weltweit zugegriffen werden, auch wenn es sich um ein virtuelles privates Netz handelt.
Aus dem Zusammenhang, Prozess und Ziel der durch den Bundesgesundheitsminister initiierten Gesetzgebung, sowie aus relevanten Aussagen, ergibt sich, dass das eigentliche Ziel keine verbesserte medizinische Versorgung sondern eine Wirtschafts- und Technologieförderung ist.
Digitalisierung erfordert jedoch keine Zentralisierung: Die zentrale Speicherung leistet aus medizinischer Sicht praktisch keinen Beitrag zu einer besseren Versorgung des Patienten, insbesondere nicht im Vergleich zu einer von diesem mitgeführten, echten elektronischen Patientenakte.
In der Praxis haben alle Personen mit Administratorrechten Zugriff auf die in der virtuellen Akte gespeicherten Dateien und können sie zudem kopieren. Diese Personen sind Arzt und Patient typischerweise nicht bekannt, können beliebig wechseln, und ihre Zugriffsrechte sind medizinisch nicht gerechtfertigt.
Personenbezogene medizinische Daten sind besonders intime und sensible persönliche Daten, die dauerhaft mit der jeweiligen Person verbunden sind. Aufgrund ihrer Intimität und der ihnen inhärenten Beschreibung der Persönlichkeit und psychologischer oder medizinischer Verletzbarkeiten, können sie im schlimmsten Fall durch Dritte zur Manipulation der Betroffenen verwendet werden.
Die momentane Verschlüsselung der lebenslang relevanten Daten bietet keine hinreichende Sicherheit. Eine Entschlüsselung auf Vorrat gespeicherter Daten kann zeitversetzt mit fortschreitender Technik erfolgen, da medizinische Daten dauerhaft und unauslöschlich mit der jeweiligen Person verbunden sind.
Das Datenumfeld („informationeller Kontext“) ist dadurch geprägt, dass aufgrund des Geschäftsgebarens privater Unternehmen eine unüberschaubare Vielzahl personenbezogener Daten erhoben wurde und wird, im Umlauf ist, kommerziell erworben werden kann. Sie wurden zudem zur massenhaften Bildung von Persönlichkeitsprofilen verwendet, die aufgrund der zugrundeliegenden Geschäftsmodelle wiederum der gezielten Beeinflussung von Bürgerinnen und Bürgern dienen.
Der informationelle Kontext ist zudem durch zahlreiche und weitreichende, erfolgreiche Hackerangriffe selbst auf stark gesicherte Datensätze und Netzwerke geprägt, die zu einem irregulären und unkontrollierten Datenzugriff und ihrer Ausleitung führen. Dies betrifft insbesondere auch zentrale Sammlungen personenbezogener medizinischer Daten. Die Akteure umfassen hier insbesondere auch professionelle Dienstleister aus dem Bereich der Organisierten Kriminalität, sowie Nachrichtendienste mit staatlichen Ressourcen an Personal, Infrastruktur und Finanzmitteln.
Der informationelle Kontext ist zudem dadurch geprägt, dass diese Akteure mithilfe von massenhaft erstellten Persönlichkeitsprofilen nachweislich und in signifikanter Weise manipulativ Einfluss auf demokratische Prozesse genommen haben. Dies geschah im Einklang mit Parteien aus dem extremen rechten Spektrum, zu dessen Netzwerk auch eine im Bundestag vertretene Partei gehört.
Der informationelle Kontext ist zudem dadurch geprägt, dass Unternehmen, deren Geschäftsmodell auf der Erstellung und Verwertung von Persönlichkeitsprofilen beruht, zunehmend Interesse an Sammlungen personenbezogener medizinischer Daten haben. Sie stehen zudem in enger Kooperation mit Universitäten in Deutschland.

Der informationelle Kontext ist auch dadurch geprägt, dass insbesondere für staatliche oder staatsnahe Akteure in der Vergangenheit die erfolgreiche Umgehung von Verschlüsselungen und Unterwanderung kryptographischer Infrastruktur bekannt ist. Für staatliche und privatwirtschaftliche Stellen sind zudem massive Investitionen in innovative Technologien dokumentiert, die in der Lage sind, aktuelle Verschlüsselungen effizient zu brechen.
Jede weitere zentrale Sammlung und Verarbeitung personenbezogener Daten vollzieht sich in diesem Datenumfeld und informationellen Kontext.
Der Gesetzgeber vergrößert durch die Einführung zentraler Datenbanken zur Speicherung personenbezogener medizinischer Daten („elektronische Patientenakte“, „Forschungsdatenbank“) die Attraktivität der Patientendaten für Hackerangriffe und die Effektivität letzterer in wesentlicher Weise. Er schafft durch die Möglichkeit des Zugriffs mit mobilen Endgeräten wie Smartphones und immer mehr angeschlossene Akteure eine unüberschaubare Anzahl von Angriffspunkten. Nachdem er in der Vergangenheit durch den Zwang zur Aufhebung von Medienbrüchen und zum physischen Anschluss vormals isolierter informationstechnischer Systeme, z.B. in den Arztpraxen, an das globale Internet bereits die latente Gefahr eines groß angelegten informationstechnischen Angriffs geschaffen hat, wandelt der Gesetzgeber sie durch sein Handeln zunehmend in eine konkrete Gefahr.
Er erleichtert zudem faktisch den Zugriff auf und die Verarbeitung von personenbezogenen medizinischen Daten durch Unternehmen, deren Geschäftsmodell auf der Erstellung und Verwertung von Persönlichkeitsprofilen beruht und trägt dazu bei, ihrem Geschäftsmodell den Anschein von Legitimität zu verleihen.
Der Gesetzgeber fordert zudem die Krankenkassen faktisch zur Erstellung von medizinischen Persönlichkeitsprofilen ihrer Versicherten auf. Er bringt sie auch in eine neue Rolle, in der sie nicht länger neutraler Dienstleister ihrer Versicherten sind, sondern von wirtschaftlichen Eigeninteressen an der Verwertung medizinischer Daten geleitet werden. Der Gesetzgeber versucht, ein Biotop zur Förderung eines auf Verwertung personenbezogener medizinischer Daten beruhenden Marktes zu erstellen. Ein Markt, in dem die Krankenkassen als Projektförderer und Investoren auftreten und das ärztliche Personal zwangsweise die Rolle eines Maklers und Datenzuträgers hat, ohne dass dies dem Wohl oder in signifikanter Weise der besseren medizinischen Versorgung des Patienten dient. Damit korrumpiert der Gesetzgeber das Gesundheitssystem.
Die massenhafte Vorratssammlung personenbezogener Daten in zentralen Datenbanken hat keinen signifikanten medizinischen Nutzen und ist aus medizinischer Sicht nicht gerechtfertigt, erhöht aber exponentiell die Gefahr irregulärer Datenzugriffe und -aneignung und eines Missbrauchs zum Schaden des Patienten: Einerseits direkt durch dessen individuelle Manipulation beispielsweise in erpresserischer Absicht, andererseits indirekt durch ihre Nutzung zu koordinierten Angriffen auf die freiheitlich-demokratische Grundordnung.

Der Gesetzgeber schränkt – vielleicht unabsichtlich - die Versicherten trotz der formalen Freiwilligkeit der Datenpreisgabe in ihrem Recht auf wirksame informationelle Selbstbestimmung ein, das dem Schutz des Rechts auf freie Entfaltung der Persönlichkeit dient. Dies geschieht, indem er das gegebene Datenumfeld ignoriert und ohne hinreichenden Grund eine weitere Sammlung und Akkumulation personenbezogener Daten initiiert. Er nimmt durch Initiierung der zentralen Sammlung intimster personenbezogener Daten in unzulässiger Weise in Kauf, dass sie absehbar zum Ziel ausgefeilter Hackerangriffe werden. Angriffe, die aller Erfahrung nach zum Erfolg führen und zu einer Verwendung der Daten zum Schaden der freiheitlich-demokratischen Grundordnung und damit auch des Rechts auf freie Entfaltung der Persönlichkeit.

Das Handeln des Gesetzgebers mit Blick auf die Möglichkeit der Bürgerinnen und Bürger, ihre Freiheitsrechte wirksam zu schützen, lässt sich vielleicht am besten anhand eines bildhaften Vergleichs verdeutlichen.

Stellen wir uns vor, während eines langen und trockenen Sommers beschließt in einer bereits stark waldbrandgefährdeten Kleinstadt im Schwarzwald oder der Lüneburger Heide der Bürgermeister, dass das Erscheinungsbild des Ortes verbessert werden müsse. Zum Beispiel,

um ihn attraktiver für Investoren zu machen. Leider kann er die Bürgerinnen und Bürger nicht dazu zwingen, ihre Vorgärten nach seinen Vorstellungen in Ordnung zu bringen. Also hat er eine richtig gute Idee.
Er stattet alle Haushalte mit Gasbrennern sowie Streichholz und Benzinkanister zum – natürlich freiwilligen - Abbrennen von Unkraut aus. Und macht ihnen gleichzeitig deutlich, dass durch das Abbrennen des Unkrauts ihr Gebäudewert steigt bzw. andernfalls leider weiter sinkt, vor allem im Vergleich zu den Nachbarn, die sich beteiligen. Außerdem verpflichtet er die Feuerwehr per Anordnung, die Bewohner der Stadt in die Handhabung der Brandmittel einzuweisen und bei der effektiven Anwendung zu unterstützen.
Offensichtlich nützt es dem Einzelnen ziemlich wenig, wenn er für sich entscheidet, dass das Ganze mit Blick auf die bereits bestehende Waldbrandgefahr wohl keine gute Idee ist, wenn seine Nachbarn links und rechts ermuntert durch den Bürgermeister beginnen, Feuer zu legen: Freiwilligkeit der Brandlegung ist keine hinreichende Bedingung, um einen Flächenbrand zu verhüten.

Analog verhält es sich aber mit der der Schaffung einer zentralen Sammlung persönlicher Daten höchster Intimität durch den Gesetzgeber und der Freiwilligkeit der Datenpreisgabe im gegebenen informationellen Kontext. Die Freiwilligkeit des Einzelnen, zu der Datensammlung beizutragen ist nicht ausreichend, um die durch den Gesetzgeber vorbereitete Katastrophe abzuwenden.

Der Staat verwandelt durch sein Handeln die abstrakte Gefahr eines Angriffs auf die freiheitlich-demokratische Grundordnung in eine konkrete Gefahr und entwertet die Möglichkeit des Einzelnen, durch umsichtiges Verhalten die Konsequenzen für sich selbst mit hinreichender Wahrscheinlichkeit abwenden zu können.

Daran sollte sich niemand beteiligen.

Teil 1 – Von Medizin und Daten

Wenn Sie dies hier lesen, haben Sie beschlossen, es nicht bei der Kurzzusammenfassung zu belassen, sondern etwas tiefer in das Thema einzusteigen. Das freut mich. Allerdings muss ich Sie auch vorwarnen: Sie sollten diesen Teil und vor allem auch den nächsten nicht zu spät am Abend lesen.

Natürlich sind Sie ein freier Mensch und können machen, was Sie wollen. Es könnte nur sein, dass Sie danach nicht besonders gut schlafen. So ging es mir jedenfalls, als ich anfing, mich intensiver mit dem Thema auseinanderzusetzen.

In diesem Teil geht es um ein aktuelles und besonders anschauliches Beispiel für den Aufbau eines Hochrisikosystems. Ein System, das von seinen Anhängern in missionarischem Eifer vorangetrieben wird: die zentrale Speicherung von personenbezogenen medizinischen Daten im ganz großen Maßstab.

Was ist die „elektronische Patientenakte“?

Unter dem Deckmantel der „elektronische Patientenakte“, die ursprünglich keineswegs als zentrale Datenbank gedacht war, wird das Projekt vorangetrieben als vermeintlich schicksalhafter, alternativloser Kern „der Digitalisierung“. Ein Begriff, der ja eigentlich einfach die ganz normale technische Weiterentwicklung von Prozessen auch im Gesundheitswesen beschreibt, nicht aber z.B. eine moralische Rechtfertigung oder gar Anspruch auf Datenanhäufung oder -verwertung.

Schauen wir also einmal genauer hin, was die vom Gesundheitsministerium forcierte „elektronische Patientenakte“ eigentlich meint. Lassen Sie uns auch einen Blick auf das Feuerwerk der zugehörigen Gesetzgebung werfen und uns fragen, was es uns verrät. Und wenn Sie jetzt bei „Patientenakte“ noch an verstaubte Aktenordner denken – da kann ich Sie definitiv beruhigen: Es ist alles digital.

Zum 1. Januar 2021 wurde per Gesetz die auch früher schon diskutierte „elektronische Patientenakte“ eingeführt, jetzt aber in einer Realisierung nach den Vorstellungen des aktuellen Bundesgesundheitsministers und Mitautor des Buchs „App vom Arzt“, Jens Spahn.

Fragen wir uns als Erstes einmal: Warum eine „elektronische Patientenakte“? Welches Problem soll sie lösen?

Vielleicht geht es um Autonomie für die Patienten, der Herr über seine Daten sein soll?
Na gut, das kann eigentlich nicht sein. Schon vor dem 1. Januar 2021 konnte ja jeder Patient von seiner Ärztin alle ihn betreffenden medizinischen Daten erhalten, und er hatte und hat ein Recht auf seine eigenen Daten.

Also hilft vielleicht ein Blick auf die Seiten des Bundesgesundheitsministeriums.

Im Jahr 2019 heißt es in den Erläuterungen zum „Terminservice- und Versorgungsgesetz“: „*Patientinnen und Patienten wollen einfach, sicher und schnell auf ihre Behandlungsdaten zugreifen können. Dafür muss die elektronische Patientenakte Alltag werden. Sie verbessert auch die medizinische Versorgung.*“[9]

Das klingt gut. Also wollen die Patientinnen und Patienten die elektronische Patientenakte unbedingt, und außerdem sind die Daten so sicherer, und sie verbessert die medizinische Versorgung. Aber wie macht sie das eigentlich?

9 www.bundesgesundheitsministerium.de/terminservice-und-versorgungsgesetz.html (zuletzt abgerufen Februar 2021)

Im Jahr 2020 wird zum „Patientendaten-Schutz-Gesetz“ markig verkündet: „*Der Patient wird Herr über seine Daten. Mit der elektronischen Patientenakte entscheidet allein der Patient, was mit seinen Daten geschieht.*“[10]

Moment mal, also doch? Aber war der Patient bisher nicht auch Herr seiner Daten? Also geht es jetzt doch nicht um eine bessere Versorgung?

Im Jahr 2021 heißt es zur „elektronischen Patientenakte“ (ePA): „*Warum brauchen wir überhaupt eine ePA? Je besser Ärztinnen und Ärzte sowie weitere Leistungserbringer die Krankengeschichte ihrer Patientinnen und Patienten nachvollziehen können, desto besser können sie die geeignete Behandlung wählen. […] Viele bisher analog oder in Papierform ablaufende Arbeitsschritte können durch die ePA digitalisiert und vereinfacht werden. Statt einer Lose-Blatt-Sammlung […] haben Arzt und Patient alle relevanten Dokument auf einen Blick sicher verfügbar. So können belastende Mehrfachuntersuchungen vermieden werden.*“[11]

OK, weniger unpraktische und lückenhafte Papiersammlungen durch Digitalisierung, das klingt plausibel. Also geht es eigentlich um Bequemlichkeit und Vollständigkeit? Ich kann mir nicht helfen - irgendwie klingt das insgesamt ein bisschen wie auf dem Wochenmarkt, wenn der Gemüse-Karl der Kundschaft seine nicht mehr ganz frischen Tomaten schmackhaft machen will.

Aber halten wir fest: Die Argumente für die „elektronische Patientenakte“ sind der Bedarf der Patientinnen und Patienten, mehr Datensicherheit, eine bessere medizinische Versorgung, weniger Abhängigkeit der Patienten bei der Verwaltung ihrer Daten, Bequemlichkeit, weniger Papierkram und dafür mehr Vollständigkeit. Das klingt doch gut.

Lassen Sie uns noch drei Punkte aus dem relevanten Gesetzbuch[12] dazunehmen: Die „elektronische Patientenakte“ soll „*der Verbesserung der Wirtschaftlichkeit, der Qualität und der Transparenz“* der medizinischen Versorgung dienen. Das ist zwar seit der Erfindung der Keilschrift vermutlich das Anliegen jedes Aktensystems, aber lassen Sie es uns gerade deshalb als vernünftigen Kern betrachten und zum Ausgangspunkt nehmen.

Dieses Ziel erreicht eine vollständige Patientenakte z.B. durch Vermeidung von Doppeluntersuchungen, durch die Möglichkeit der Einsichtnahme seitens des Patienten und damit Stärkung seiner Datenautonomie und -eigenverantwortung sowie dadurch, dass jeder behandelnde Arzt auf eine vollständige Fallgeschichte zurückgreifen kann und damit auf einer optimalen Informationsgrundlage Diagnosen stellen und Therapieentscheidungen treffen kann.

Also eine geeignet gestaltete elektronische Gesundheitskarte des Versicherten zu seinem persönlichen Gebrauch, auf der - verschlüsselt und passwortgeschützt – medizinische Daten wie Befunde, Diagnosen oder auch Röntgenbilder gespeichert sind. Sinnvollerweise wäre sie z.B. durch eine ebenfalls verschlüsselte, „treuhänderische“[13] Kopie gegen Datenverlust gesichert, die vielleicht am einfachsten beim Hausarzt lokal und isoliert gespeichert ist[14]. Geeignet gestaltet wiederum impliziert beispielsweise eine spezielle, zertifizierte und gesetzlich geschützte Hardware-Schnittstelle und hinreichenden Speicherplatz, wie ihn jede micro-SD-Karte aufweist[15]. Man würde also vermuten, dass es dem Bundesministerium für

10 www.bundesgesundheitsministerium.de/patientendaten-schutz-gesetz.html (zuletzt abgerufen Februar 2021)

11 www.bundesgesundheitsministerium.de/elektronische-patientenakte.html (zuletzt abgerufen Februar 2021)

12 „Fünftes Buch Sozialgesetzbuch“, „SGB V“, § 334

13 H. Federrath, Univ. Hamburg

14 Möglicherweise könnte der Datensatz als Blockchain gestaltet sein, als weitere Maßnahme zur Sicherung der Datenintegrität.

15 So gibt es derzeit typische SD-Speicherkarten mit einer Speicherfähigkeit von 256 GB. Dies entspricht in etwa dem Speicherbedarf von 200 Stunden hochauflösender Filmaufnahmen plus 5 Millionen voll

Gesundheit darum geht, z.B. die Spezifikationen der Gesundheitskarte mit ihrer antiken Speicherbegrenzung auf wenige Kilobyte[16] den 2020er Jahren anzupassen. Dies legt ja auch die zur „elektronischen Gesundheitskarte“ analoge Bezeichnung „elektronische Patientenakte“ nahe.

Eine derartige elektronische Patientenakte, die technisch problemlos umzusetzen ist und mit ihrem Datenbestand in der Eigenverantwortung des Versicherten liegt, wäre völlig legitim und zweckmäßig. Sie würde die genannten Ziele gut und in angemessener Weise realisieren. Der Patient hat seine Daten immer im Blick und unter Kontrolle, kann sie selbständig, physisch und in für ihn nachvollziehbarer Weise sichern, z.B. durch Wegschließen. Zur Verwendung und zum Auslesen der elektronischen Patientenakte ist kein Anschluss der entsprechenden Schreib-, Lese- und Sicherungsgeräte an eine unübersichtliche Infrastruktur wie das Internet erforderlich, die Datenübertragung bezüglich der Patientenakte zwischen behandelnden Ärzten geschieht durch den Versicherten selbst, indem er seine Gesundheitskarte in eigener Verantwortung mit sich führt[17]. Wie im realen Leben wäre auch in der Digitalen Welt der Patient der Inhaber seiner Daten.

Da zu keinem Zeitpunkt die Daten der elektronischen Patientenakten zentral und losgelöst von den Versicherten gesammelt, gespeichert oder verarbeitet würden, könnte das Führen und Füllen einer solchen elektronischen Patientenakte möglicherweise sogar gesetzlich geregelt werden, ohne gegen das Recht auf informationelle Selbstbestimmung zu verstoßen, d.h. das Recht darauf, selbst zu bestimmen, wem wann welche Daten weitergegeben und wofür sie verwendet werden.

Dies wäre ähnlich den gesetzlichen Regelungen zum Führen bestimmter Führerscheintypen, die ggf. regelmäßige Tauglichkeitsnachweise erfordern. Damit kann durch die Verpflichtung zum eigenständigen Führen einer elektronischen Patientenakte die Vollständigkeit der elektronischen Patientenakte für alle Versicherten sichergestellt werden, so dass sie medizinische sinnvoll nutzbar ist.

Im Fall von realistischerweise zu erwartendem „menschlichem Versagen“ Einzelner (Verlieren der Karte) oder kriminellen Handlungen (Diebstahl der Karte) wären die Daten zumindest wie in Datenbanken durch eine Verschlüsselung geschützt. Der Verlust wäre zwar ärgerlich für den Versicherten, da er dann die Patientenakte mithilfe der treuhänderischen Kopie wieder neu aufbauen müsste. Aber wenn er nicht gerade eine Top-Managerin oder ein Spitzenpolitiker ist, könnte er sich einigermaßen sicher sein, dass er zumindest nicht das Ziel professioneller Datendiebe war. Denn die würden bis auf einzelne Ausnahmefälle das Risiko und den hohen Aufwand eines physischen Diebstahls einzelner Gesundheitskarten scheuen. Zudem würde durch einzelne Diebstähle kein gesamtgesellschaftlicher Schaden entstehen, während ein massenhafter Diebstahl individueller „Patientenkarten“ einer Vielzahl von Bürgerinnen und Bürgern zum Einen unrealistisch wäre und zum Anderen nicht unentdeckt und wohl auch nicht unaufgeklärt bliebe.

Eine echte elektronische Patientenakte, wie sie wohl immer geplant war und deren gesetzliche Einführung wäre angemessen, verhältnismäßig und zweckmäßig. Damit wäre der Text an dieser Stelle beendet und ich könnte Ihnen einfach viel Spaß damit wünschen.

---

beschriebener DIN A4 Seiten Text plus Tausend unkomprimierten Bildern mit einer Auflösung von 12 Megapixeln bei 24 Bit pro Pixel. Das sollte erstmal reichen.

16 In den 1980er Jahren die typische Größenordnung für das Speichervolumen von Home-Computern (z.B. „C64“, „C16“); 1 Kilobyte entspricht ca. 1 Millionstel Gigabyte.

17 Das Einlesen elektronisch versandter Daten könnte in den Praxen beispielsweise in einer Einbahnstraße über „sterile“ Datenträger geschehen. Also Datenträger, die als Teil der „Digitalhygiene“ nach dem Einlesen der Daten routinemäßig in einer Station, die als „digitaler Autoklav“ dient, physikalisch gelöscht und neu formatiert werden.

Was aber, wenn sich hinter dem Etikett „elektronische Patientenakte“ etwas ganz Anderes verbirgt?

Eine *virtuelle* Patientenakte beispielsweise, die eine letztlich intransparente, zentrale Erhebung, Speicherung und Verarbeitung der medizinischen Patientendaten physisch losgelöst von den Versicherten darstellte, und welche zudem vielleicht zusätzlich die regelmäßige Anfertigung von Kopien der zentralen Datensammlungen zu Sicherungszwecken implizierte? Sie würde ja nicht nur eine faktische „informationelle Entmündigung“ des Versicherten und seine Abhängigkeit von einer undurchschaubaren Netzwerkstruktur mit vielen Beteiligten bedeuten, die auch durch programmiertechnische Einschränkungen regulärer Zugriffe nicht aufgehoben würde. Sie würde auch sofort in ein Dilemma führen.

Selbstbestimmung; Freiwilligkeit und die Vollständigkeit der Akte

Einerseits ist die Vollständigkeit der elektronischen Patientenakte erforderlich zur medizinisch sinnvollen Erreichung ihrer Ziele, da unvollständige, lückenhafte Datensätze nur von eingeschränktem Nutzen oder sogar nachteilig wären. Dies erfordert eine verbindliche Regelung, d.h. letztlich die Ausübung von Zwang, der sicherstellt, dass für den Versicherten wirklich alle medizinischen Daten in den zentralen Datensatz aufgenommen werden. Grundlage wäre z.B. eine gesetzliche Pflicht, alle Daten in die zentrale Sammlung einer virtuellen Akte zu übertragen.

Aber das ist genau der Fall, dem das Bundesverfassungsgericht 1983 in der Geburtsstunde des modernen Datenschutzes, dem sogenannten „Volkszählungsurteil“, klar die rote Karte gezeigt hat: Eine zwangsweise zentrale Sammlung der Daten würde das dort herausgearbeitete Recht auf informationelle Selbstbestimmung angesichts eines Zwangs (oder auch eines manipulativen Verleitens zur Datenpreisgabe) in unzulässiger Weise verletzen.

Dies gilt umso mehr, wenn man die Sensibilität und Intimität der medizinischen Daten berücksichtigt, die über die der im Rahmen des „Volkszählungsurteils“ betrachteten Daten deutlich hinausgeht und wohl kaum zu überbieten sind. In der Datenumgebung, also dem „informationellen Kontext“ von 1983 war dabei die Möglichkeit zur persönlichen Verweigerung der Datenpreisgabe nicht nur notwendig sondern auch hinreichend, um das Recht auf freie Entfaltung der Persönlichkeit wirksam zu sichern. Der Einzelne konnte im damaligen Kontext unabhängig von den Anderen für sich selbst durch Weigerung zur Datenpreisgabe sicherstellen, dass für ihn der notwendige Freiraum und die Grundlagen einer freiheitlichen Gesellschaftsordnung gewahrt waren.

Ein Leitprinzip des Bundesverfassungsgerichts im Rahmen des Grundsatzurteils war dabei, die Möglichkeit zur Erstellung von Persönlichkeitsprofilen („Teilabbilder/Totalabbilder der Persönlichkeit“) zu unterbinden, da dies die freiheitliche Grundordnung und die freie Entfaltung der Persönlichkeit des Einzelnen gefährde. Genau dieser Möglichkeit würde der Gesetzgeber aber durch die zentrale Datensammlung in einer virtuellen „elektronischen Patientenakte“ offensichtlich Vorschub leisten. Das gilt insbesondere angesichts der Vielzahl kommerziell verfügbarer und genutzter personenbezogener Datensätze und Nutzerprofile, mit denen die medizinischen Daten aus einer „virtuellen Patientenakte“ zusammengeführt werden könnten, sollten sie je in die falschen Hände geraten.

Der Gesetzgeber darf hier natürlich auch keinen unklaren Graubereich erzeugen und darf einen Zwang bzw. ein Verleiten zur Preisgabe der Daten auch nicht formal an Dritte delegieren. Auch nicht indem er ihm Anreize z.B. wirtschaftlicher Art bietet durch eine entsprechende Vergütung der behandelnden Ärzte für jeden Patienten, den er für die Weitergabe seiner Daten gewinnt oder durch deren Zwangsverpflichtung. Ebenso wenig darf er die Versicherten indirekt zu einer Datenpreisgabe verleiten, z.B. durch manipulative Botschaften oder Irreführung über Ziele und tatsächlichen Nutzen der Datensammlung. Dies gilt umso mehr, wenn die Versicherten damit ihre eigenen Interessen oder die der

Allgemeinheit verletzen würden oder auch nur die Folgen ihres Handelns realistischerweise nicht überblicken könnten.

Ebenso wenig darf der Gesetzgeber indirekten Zwang zur Datenpreisgabe ausüben. Genau dies geschähe jedoch, wenn er den Eindruck erweckte, dass die zentralen Datenbanken notwendig für eine bessere Behandlung und alternativlos wären. Oder wenn er es für die Versicherten systematisch immer schwerer machen würde, die Leistungen des Gesundheitssystems unabhängig von einer Zustimmung zur zentralen Datensammlung in Anspruch zu nehmen. Denn dann würde der Versicherte sich angesichts dieser Behauptung vor die Wahl gestellt sehen, entweder der angeblich alternativlosen zentralen Datensammlung in der virtuellen Patientenakte zuzustimmen oder zukünftig eine vermeintlich qualitativ schlechtere medizinische Versorgung in Kauf zu nehmen als möglich.

Dies könnte jedoch aus Sicht des Versicherten nicht als freie Wahl betrachtet werden, da die (scheinbare) Alternative einer schlechteren medizinischen Versorgung eine wesentliche Selbstbenachteiligung bedeuten würde. Hinzu käme, dass in einer medizinischen Behandlungssituation eine freie und unabhängige Entscheidungsfähigkeit frei von Einflüssen Dritter je nach Akutheit und Gegebenheit der medizinischen oder psychischen Situation nicht vorausgesetzt werden kann.

Mit der Einführung einer solchen virtuellen Patientenakte würde der Gesetzgeber sich also in selbst gewählte Dilemmata begeben, indem er versuchen würde, Unvereinbares miteinander zu vereinbaren: Die Notwendigkeit einer vollständigen Sammlung medizinischer Daten auf der einen Seite, und die Unmöglichkeit, dieses Ziel für eine zentrale Datenbank legitimer Weise zu erreichen. Hinzu kommt, dass der informationelle Kontext sich seit 1983 grundlegend gewandelt hat, wie wir später noch sehen werden. Daher kann nicht ohne weiteres davon ausgegangen werden, dass die Möglichkeit, für sich die Preisgabe seiner Daten zu verweigern, hinreichend für die Absicherung der freien Entfaltung der Persönlichkeit ist.

Tatsächlich kann man in Frage stellen, ob selbst die Freiwilligkeit, d.h. die Notwendigkeit der Zustimmung durch den Versicherten als Voraussetzung für die Erhebung, Verarbeitung und Nutzung oder auch Löschung der medizinischen Daten bzw. des einmal erstellten Datensatzes für die Zukunft wirklich als gesichert betrachtet werden kann.

Bereits in einer Studie aus dem Jahr 2017 zum Thema „Elektronische Patientenakten“ wird die Frage in den Raum gestellt:„*...in welchem Rahmen soll er [der Patient] Informationen ausschließen oder löschen können? Ab wann führt diese Wahrnehmung der informationellen Selbstbestimmung – ggf. auch falsch gehandhabt – die eEPA ad absurdum?*“[18]. Dass solche Überlegungen durchaus zu gesetzlichen Einschränkungen der Datenhoheit des Versicherten auch über seine medizinischen Daten führen können, zeigt ein scharfer Protest aus der dänischen Ärzteschaft gegen eine entsprechende Vorlage zur Änderung des dänischen Gesundheitsgesetzes (*sundhedslov*) aus dem Jahr 2018[19]. Dies im Verein mit der weiter unten beschriebenen, häppchenweisen Kettengesetzgebung lässt erahnen, dass in Zukunft scheinbare oder gezielt aufgebaute Systemzwänge die Wahlmöglichkeit einschränken werden. Tatsächlich zeichnet sich genau dies spätestens mit der geplanten, systematischen Löschung der Informationen auf der elektronischen Gesundheitskarte ab[20].
Die nächsten Schritte versucht das 2021 vorgestellte Gutachten[21] des Sachverständigenrats „Gesundheit“ eilfertig vorzubereiten, in dem er eine zwangsweise zentrale Datenspeicherung

18 P. Haas: „Elektronische Patientenakten“, Bertelsmann Stiftung (Hrsg.), 2017

19 A. Beich: „DSAM: Fortrolighed mellem laege og patient er vigtigere end andre interesser“ („Dänische Gesellschaft für Allgemeinmedizin: Vertraulichkeit zwischen Arzt und Patient ist wichtiger als andere Interessen“), Altinget (2018) *www.altinget.dk*/sundhed/artikel/selskab-fortrolighed-mellem-laege-og-patient-er-vigtigere-end-and, zuletzt abgerufen: 27.02.2020); hier wie auch im Folgenden wurden fremdsprachliche Texte von mir selbst nach bestem Wissen und Gewissen übersetzt.

20 „Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur digitalen Modernisierung von Versorgung und Pflege“ (Januar 2021), S. 34

fordert, der man sich im Stil eines sogenannten „dark patterns“[22] aktiv widersetzen muss, sowie einen Zugriff auf medizinische Daten „*ohne Zustimmungserfordernis oder Opt-out-Möglichkeit“.* d.h. ohne Mitspracherecht des Patienten. Sie glauben, Ihre Daten sind Ihre Daten? Nicht, wenn es nach den Professorinnen und Professoren des Sachverständigenrats geht[23].

Interessant ist hier ein Blick zu unseren europäischen Nachbarn. Nachdem dort nur ein verschwindend geringer Anteil der Versicherten Interesse an einer virtuellen Patientenakte gezeigt hatte, stellte auch der französische Rechnungshof 2017 fest: „*Eine sichere Kommunikation im Gesundheitswesen […] und insbesondere die elektronische Patientenakte [dossier médical partagé], für die [...] nach ihrem kostspieligen Misserfolg seit dem 1. Januar 2017 zuständig ist, werden nicht wirklich effizient sein, wenn sie nicht nutzerfreundlich, flexibel und interoperabel sind und alle für die Behandlung der Patienten zweckdienlichen Informationen enthalten. Unter diesem Aspekt riskiert die elektronische Patientenakte, deren Einrichtung übrigens nicht verpflichtend ist, auf Zurückhaltung bei den Patienten zu treffen, die verlangen können, dass dort bestimmte Informationen nicht auftauchen [...]*“[24]. Die Lösung? Neben einer massiven Werbeoffensive wurde in Frankreich in den folgenden Jahren, 2019 und 2020, Gesetze verabschiedet, die die automatische Einrichtung einer virtuellen Patientenakte für alle ab 2022 vorsehen, sofern nicht einzeln und aktiv widersprochen wird[25].

Zentrale Daten-sammlun-gen als An-griffsziele

Hinzu käme, dass eine zentrale oder zentral zugängliche Sammlung, Speicherung und Verarbeitung sensibler Daten der Versicherten in einer virtuellen Patientenakte diese Sammlung, und damit auch die Daten jedes Einzelnen, erst zu einem attraktiven Angriffsziel professionell agierender Datendiebe machen würde. D.h. eine solche virtuelle „elektronische Patientenakte“ würde das Risiko einer irregulären Datenaneignung von katastrophalem Ausmaß massiv erhöhen. Es bedürfte einer sehr gründlichen Abwägung dieses Risikos gegenüber den durch sie plausiblerweise zu erwartenden Vorteilen. Diese Abwägung müsste zudem um so kritischer ausfallen, je größer die Wahrscheinlichkeit wäre, dass eine irreguläre Datenaneignung im Nachhinein nicht einmal sicher festgestellt und zugeordnet werden könnte. Ein Fall, der weiter unten noch betrachtet wird. Eine solche Abwägung hat nicht stattgefunden.

Ein zusätzlicher Aspekt ergäbe sich, wenn diese sensible Datensammlung in einer Infrastruktur verarbeitet und gespeichert würde, die als rein virtuelles „privates Netz“[26] physisch mit dem Internet verbunden bzw. in Teilen identisch wäre. Also mit einem globalen Netzwerk, auf das rund vier Milliarden Menschen Zugriff haben. Darunter eine unbekannte Zahl von Akteuren der Organisierten Kriminalität, der Privatwirtschaft, sowie die Nachrichtendienste aller Staaten dieser Erde. Tatsächlich gibt es wohl kaum einen verletzlicheren, unsichereren und damit weniger empfehlenswerten Ort für die Speicherung und den Austausch einer Sammlung sensibler Daten als eine mit dem Internet verbundene

21 „Digitalisierung für Gesundheit“, Gutachten des Sachverständigenrats zur Begutachtung der Entwicklung im Gesundheitswesen, Bonn/Berlin, 2021

22 Unter „dark patterns“ werden subtile psychologische Tricks bzw. das Ausnutzen menschlicher psychologischer Schwächen verstanden, die einem Nutzer das Gefühl von Wahlfreiheit geben, ihn aber tatsächlich zu einem vom Ersteller der „dark patterns“ vorher bestimmten Handeln veranlassen sollen (vgl. z.B. „Deceived by design – how tech companies use dark patterns to discourage us from exercising our rights to privacy, Forbrukerrådet (Norwegischer Verbraucherschutz), 27.06.2018).

23 Für eine ausführlichere Darstellung vgl. Kommentar im Anhang zu diesem Text.

24 Cour des comptes: „Rapport public thématique – l‘avenir de l‘assurance maladie“ (November 2017).

25 Code de la santé publique (ab 4. März 2021 gültige Fassung), Partie législative, 1ére partie, livre 1er, titre 1er, chapitre 1er, section 3: „Dossier médical partagé et dossier pharmaceutique“, art. L1111-14, sowie Code de la santé publique (ab 1. Januar 2022 gültige Fassung), Partie législative, 1ére partie, livre 1er, titre 1er, chapitre premier, section 3: „Espace numérique de santé, dossier médical partagé et dossier pharmaceutique“, art. L1111-13-1.

26 siehe z.B. M. Gramma: „Drei populäre VPN-Anbieter gehackt“, Inside IT, (Oktober/Dezember 2019; https://www.inside-it.ch/de/post/drei-populaere-vpn-anbieter-gehackt-20191022)

oder mit ihm physikalisch identische Netzwerkinfrastruktur. Dies bzw. eine gesetzliche Beauftragung hierzu auch nur temporär zu rechtfertigen bedürfte außerordentlicher Gründe wie das Bestehen einer unmittelbaren Not- und Ausnahmesituation, die anders nicht bewältigt werden könnte. Sonst wäre sie weder zweckmäßig noch angemessen. Eine solche rechtfertigende Not- und Ausnahmesituation liegt hier offensichtlich nicht vor[27].

Aber es würden doch sicherlich große Anstrengungen unternommen, um nach bestem Wissen und Gewissen und dem Stand der Technik die Sicherheit dieses Hochrisikosystems zu gewährleisten? Absolut.

Als im März 2017 die zuständige amerikanische Zulassungsstelle den Flugzeugtyp 737 MAX des Herstellers Boeing zuließ, war auch sie wie die Ingenieure des Herstellers zweifellos ehrlich überzeugt - und hatten alle ihr Bestes dafür getan -, dass das Flugzeug sicher ist. Zwei Jahre und zwei Abstürze auf zwei Kontinenten später waren dennoch fast 350 Menschen tot. Nicht aufgrund von Fahrlässigkeit oder Unfähigkeit, sondern weil es in dem komplexen System „Verkehrsflugzeug“ zu unerwarteten Wechselwirkungen gekommen war, die zu einem nicht mehr beherrschbaren Verhalten des Gesamtsystems führten. In die Katastrophe.

Würde man nun die medizinischen Daten der Versicherten zentral speichern, ergäbe sich ein Netzwerk mit ca. 200 000 zugriffsberechtigten und interagierenden Ärzten und Einrichtungen wie Krankenhäusern und ihrer technischen Dienstleister plus vielen weiteren Menschen in Heilberufen und im Pflegedienst[28], mit Millionen von Versicherten mit noch mehr Endgeräten, angeschlossen an das Internet mit Milliarden von Menschen und unzählbar vielen Zeilen Computercode. Im Vergleich dazu ist das außer Kontrolle geratene System „Boeing 737 MAX“ so simpel und durchschaubar wie ein Papierflieger...

Auch wäre nicht klar, worin im Interesse der Patientenversorgung der Vorteil einer potentiell lückenhaften virtuellen Patientenakte als „Front End“ zentraler Datenbanken liegen sollte gegenüber einer mitgeführten, vollständigen elektronischen Patientenakte im Besitz des Patienten. Auch nicht mit Blick z.B. auf Forschungsdaten wenn man die bestehenden Ansätze und Praktiken medizinischer Forschung bedenkt. Medizinischer Forschung wie die aus öffentlichen Mitteln finanzierte „Nationale Kohorte“[29] - eine repräsentative Langzeitstudie, die mit großem Aufwand eine gesicherte Datenqualität, detaillierte Aufklärung und Information der Teilnehmenden, eine durchgehende Pseudonymisierung ohne Hintertür, Freiheit von Interessenkonflikten, ein System persönlicher Verantwortung und die Diskussion ethischer Grundlagen sicherstellt.

Datenanhäufung und Profilerstellung als Geschäftsmodell

Zudem müssen die Bürgerinnen und Bürger bei einer gesetzlich beauftragten Sammlung ihrer medizinischen Daten z.B. durch die Krankenkassen natürlich darauf vertrauen können, dass der Gesetzgeber mit den Krankenkassen einen neutralen und vertrauenswürdigen Sachwalter eingesetzt hat. D.h. es sollte keine offensichtlichen Interessen des Datenverwalters an den

27 Auch nicht durch die aktuelle Covid-19-Pandemie, und auch nicht durch den von Interessenvertretern als Argument genannten „Digitalen Impfpass“, der ja keineswegs eine zentrale Speicherung erfordert. (vgl. https://www.tagesschau.de/inland/bitkom-corona-impfungen-101.html). Auch die Ende 2020 vom „Sachverständigenrats Gesundheit“ hoffnungsvoll vorgebrachte Vermutung, dass eine zwangsweise auf allen geeigneten Geräten installierte Corona-App, die zudem alle relevanten medizinischen Daten der Besitzer gesammelt hätte, zu einem Erkenntnisgewinn geführt hätte, durch den wiederum der generelle Lockdown im Herbst 2020 hätte umgangen werden können, geht wohlweislich nicht über eine allgemeine Mutmaßung hinaus und erscheint wenig stichhaltig. Abgesehen von der verfassungswidrigen Grundrechtsverletzung und dem damit einhergehenden politischen Erdbeben und Akzeptanzverlust jedweder Maßnahmen würde es wohl zu einem Ausweichverhalten kommen, das die zuvor gesammelten Daten operativ weitgehend nutzlos machen würde (vgl. „Digitalisierung für Gesundheit“, Gutachten 2021).

28 „Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur digitalen Modernisierung von Versorgung und Pflege“ (Januar 2021)

29 https://nako.de

von ihm verwalteten medizinischen Daten oder deren Weitergabe geben, insbesondere keine Interessen wirtschaftlicher Art an ihrer Verwertung. Würde der Gesetzgeber solchen Interessenkonflikten Vorschub leisten, würde er damit seine Fürsorgepflicht verletzen.

Der Staat kann sich dabei auch nicht die Geschäftspraktiken wirtschaftlich hoch erfolgreicher Datensammler und -verwerter wie Google oder Facebook zum Vorbild nehmen oder ihnen Vorschub leisten, ohne die Grundlagen der Verfassung zu gefährden.
Deren Geschäftsmodell einer vordergründig kostenlosen Nutzung zentraler Datensammlungen und -dienste wie z.B. bestimmter Suchmaschinen oder virtueller „sozialer Netzwerke“ bis hin zu einer Art parallelem Internet beruht ja im Kern auf einem Tauschhandel. In diesem Tauschhandel werden Bequemlichkeit und die Illusion von Autonomie, Nähe und Gemeinschaft wie billige Glasperlen bei uns „digital natives“ eingetauscht gegen den kostbaren, von den Meisten bisher aber als wertlos erachteten „Rohstoff“ Ihrer eigenen, personenbezogenen Daten. Dieser dient dann in einem zweiten Schritt dazu, aus ihm über Profilbildung die lukrative Handelsware Manipulierbarkeit zu erzeugen und kommerziell anzubieten[30]. Dieser Raubbau an den Grundlagen einer freiheitlichen Gesellschaft ist nicht nur sittenwidrig, er unterminiert auch den im Zeitalter der Aufklärung gesetzten Grundpfeiler des Grundgesetzes: den mündigen Bürger, der hier zum reinen Datenquell- und Manipulationsobjekt wird.

Würde der Staat diesen Tauschhandel, den man etwas spitz als „Digitalen Kolonialismus“ bezeichnen könnte, kopieren und ihn damit gutheißen und fördern, würde er ihn legitimieren und ihm Vorschub leisten. Mit allen Konsequenzen für die Gesellschaft.

Insofern wäre auch das Argument, man müsse durch eine staatlich beauftragte Sammlung der medizinischen Daten der Bürgerinnen und Bürger den Bestrebungen von Amazon, Google etc. zur Sammlung von medizinischen Daten zuvorkommen[31], ein leeres Argument. Zum einen könnten die genannten Firmen oder ihre Subunternehmen immer noch als Dienstleister der Krankenkassen fungieren und damit faktisch die personenbezogenen medizinischen Daten auf ihren Datenträgern sammeln. Zum anderen verhindert die Gesetzgebung in keiner Weise, dass die genannten Firmen auch weiterhin eigene, privatwirtschaftliche Sammelmöglichkeiten für medizinische Daten anbieten und zur Profilerstellung verwenden, dem würde eher noch Legitimität zugesprochen.

Der einzige wirksame Weg, eine Ansammlung personenbezogener medizinischer Daten zu verhindern, wäre ja die Aufklärung der Bürger über die damit verbundenen Gefahren und ihr grundsätzliches Verbot als das, was sie ist: sittenwidrig und existentiell bedrohlich für die freiheitliche Gesellschaft. So werden beispielsweise auch Banküberfall, Nötigung und Erpressung ja nicht gesetzlich reguliert oder mit bestimmten Rahmenbedingungen gesetzlich beauftragt, sondern schlicht verboten und bekämpft. Etwas Vergleichbares wird durch den Gesetzgeber hier in keiner Weise geleistet.

Schließlich gilt auch, dass der Versicherte sich darauf verlassen können muss, dass die vom Gesetzgeber genannten Ziele und Zwecke der Gesetzgebung im Wesentlichen tatsächlich die sind, die der Gesetzgeber durch die von ihm erlassenen Regelungen verfolgt. Wenn sich also

30 Das Geschäftsmodell wird manchmal als „werbegetrieben“ oder „werbebasiert“ bezeichnet. Das ist nicht ganz korrekt. Es werden keine Werbeanzeigen verkauft, sondern Zielgruppen. Der Käufer, der eine Botschaft verbreiten möchte, kann sich als Adressaten, die die Botschaften sehen werden, bequem bestimmte Personenprofile zusammenstellen („zusammenklicken“), die z.B. auf Alter, Wohnort, Interessen (interest based) oder Verhalten und Absichten (behaviour based) beruhen. Wenn die Anbieter entsprechender Dienste beteuern, sie würden keine (Roh-)Daten ihrer Nutzer verkaufen oder weitergeben ist das so korrekt wie irrelevant, da ihre Geschäftsmodell ja darauf beruht, die Daten selbst auszuwerten und zur Profilbildung zu verwenden.

31 „Die elektronische Patientenakte“, Bundesministerium für Gesundheit (https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/elekrtonische-patientenakte.html (zuletzt abgerufen: 07.03.2020)

beispielsweise aus dem Kontext der Gesetzgebung abzeichnen würde, dass der Gesetzgeber hier nicht patientenorientiert die „Verbesserung der Wirtschaftlichkeit, Transparenz und Qualität der Behandlung“ sondern eigentlich eine verdeckte Wirtschafts- oder Technologieförderung anstrebt, widerspräche dies den rechtsstaatlichen Grundsätzen der „Normenklarheit“ und „Normenbestimmtheit“. Und ganz einfach dem der Würde des Menschen geschuldeten Respekt des Staates vor seinen Bürgern, ihn ernst zu nehmen.

Datenautonomie

Wie steht es um die Datenautonomie, die Selbstbestimmung des Versicherten? Die oft zu findende Aussage, Krankenversicherung und Dienstleister könnten auf die medizinischen Daten einer virtuellen Patientenakte nicht zugreifen, wenn sie nur verschlüsselt seien, ist nicht ganz korrekt. Physisch können sie sehr wohl auf die bei ihnen gespeicherten oder über sie zugänglichen Daten zugreifen. Denn sonst könnten sie sie nicht verarbeiten bzw. ihre Dienstleistung nicht anbieten. Gemeint ist lediglich, dass sie nicht in der Lage sind, die Dateien, auf die sie eben sehr wohl physisch Zugriff haben, unmittelbar und ohne kriminelle Energie zu entschlüsseln. Dies bedeutet jedoch nicht, dass auch sonst keine interessierte Stelle in der Lage wäre, die Verschlüsselung unmittelbar oder später zu brechen oder zu umgehen, sobald sie einmal in den Besitz der Daten gelangt ist. Auf diesen Punkt werden wir noch zurückkommen.

Wenn also zum Beispiel unter der Überschrift „Gesundheitsakte TK-Safe geht in den erweiterten Anwendertest“[32] der Vorstandsvorsitzende der Techniker Krankenkasse mit den Worten zitiert wird, dass „*weder die TK noch IBM[33] auf die Daten des Versicherten zugreifen können“*, so ist diese Aussage falsch. Zumindest die Firma IBM als technischer Dienstleister kann technisch sehr wohl auf die Daten zugreifen. Gemeint ist, dass die TK und IBM nicht im Besitz des Schlüssels sind, um die Verschlüsselung der Daten aufzuheben. Das ist im Prinzip richtig, allerdings ist beispielsweise gerade IBM nun gleichzeitig auch einer der weltweit wenigen Hersteller von Supercomputern wie beispielsweise dem Rechner „Summit“ des US amerikanischen Oak Ridge National Laboratory, die grundsätzlich auch für das Brechen von Verschlüsselungen geeignet sind. D.h. selbst hierzu wäre IBM grundsätzlich in der Lage, zumal IBM aktiv an der Entwicklung sogenannter „Quantencomputer“ arbeitet, die bestimmte Verschlüsselungsverfahren („RSA“) bekanntermaßen effizient brechen können. Nicht ohne Grund ist IBM ja auch Partner der US amerikanischen Geheimdienste über Projekte der „*Intelligence Advanced Research Agency* (IARPA)“[34]. Und dabei geht es vermutlich nicht darum, mithilfe von Quantencomputern Verkehrswege zu optimieren oder den Klimawandel zu modellieren…

Aber die Frage ist nun: Was für eine Patientenakte wird nun durch die Gesetze des Bundesgesundheitsministers eingeführt? Sie ahnen es natürlich schon.

Die virtuelle Patientenakte

Tatsächlich hat das Gesundheitsministerium es aus gutem Grund lange Zeit vermieden, das klar zu benennen. Denken Sie an die eingangs erwähnten Zitate von der Website des Bundesgesundheitsministeriums die in der Hinsicht so aufrichtig sind wie die treuherzige Behauptung von Google, Facebook & Co. man sammle Daten ja nur für „ein besseres Nutzererlebnis“. Ich vermute, dass selbst vielen Bundestagsabgeordneten nicht klar war, dass es nicht um eine echte elektronische Patientenakte geht, als sie am 14. März 2019 dem „Terminservice- und Versorgungsgesetz (TSVG)“ und damit der Einführung der Spahn‘schen Version einer Patientenakte zustimmten: der virtuellen Patientenakte, in der die Daten tatsächlich zentral gespeichert werden.

32 https://www.heise.de/newsticker/meldung/Gesundheitsakte-TK-Safe-geht-in-den-erweiterten-Anwendertest-4312568.html (abgerufen 08.02.2020)

33 IBM ist der technische Dienstleister der Techniker Krankenkasse für den Betrieb der von ihr angebotenen virtuellen elektronischen Gesundheitsakte/Patientenakte.

34 Bundesamt für Sicherheit in der Informationstechnik: „Entwicklungsstand Quantencomputer“ (Juni 2020), S. 131

Doch der Gesetzgeber hat durch die Festlegung eines Zugriffs auch mittels mobiler Endgeräte faktisch dafür gesorgt, dass keine echte elektronische, physische Patientenakte in Hoheit des Versicherten eingeführt wird, sondern eine rein virtuelle Patientenakte als Teil einer von Dritten verwalteten Datenbank, auf die beispielsweise per Smartphone zugegriffen werden kann. Knapp zwei Jahre und einige Gesetze später, fühlt sich das Bundesgesundheitsministerium sicher genug, dies auch einigermaßen unverhohlen zuzugeben[35].

Damit trifft also alles zu, was wir oben für den Fall einer virtuellen Patientenakte und die mit ihr einhergehenden Widersprüchlichkeiten und Probleme gesehen hatten. Das Bundesgesundheitsministerium geht inzwischen sogar noch weiter, indem Ihre Versichertenkarte, liebe Leserin und lieber Leser, zukünftig auf keinen Fall mehr überhaupt eine Speicherfunktion besitzen, sondern letztlich wohl komplett abgeschafft und durch eine virtuelle „digitale Identität“ ersetzt werden soll[36]. Ein Albtraum der Datensicherheit.

Man kann sich des Eindrucks nicht erwehren, dass das Bundesgesundheitsministerium die Marketingsprüche von Google und Co. zu sehr für bare Münze genommen hat. Und so im Digitalen Raum ein Hochrisikosystem schafft - komplett vorbei am Bedarf der Bürgerinnen und Bürger.

Was ist seine Schlussfolgerung, wenn er merkt, dass der Bedarf nicht da und er den Weg sinnlos und allein gegangen ist? Selbstkritik und Kurskorrektur? Ganz im Gegenteil. Die Totalität des digitalen Hochrisikosystems soll weiter ausgebaut werden, so dass es möglichst keine „Schlupflöcher“ für die Bürgerinnen und Bürger mehr gibt, durch die sie diesem System entgehen könnten – bitte sehr, dann müssen Sie es doch einfach lieben! Mit dem jüngsten Gesetzentwurf soll sichergestellt werden, dass der Irrweg der zentralen Datenspeicherung für die Bürgerinnen und Bürger ein Weg ohne Wiederkehr wird. Ein Weg, auf dem es nur eine Richtung gibt: immer weiter. Oder, wie es bisher noch in jedem vorgelegten Gesetzentwurf so lapidar wie falsch heißt: „*Alternativen - Keine*.“[37]

Aber nur weil man die richtige Abzweigung verpasst und konsequent in die falsche Richtung gegangen ist, muss man es ja nicht unbedingt halten wie der Bergführer, der sich unversehens am Rand eines Abgrunds wiederfindet und meint: „Egal, jetzt sind wir so weit gegangen, jetzt gehen wir auch weiter.“ Tatsächlich ist es nie zu spät, einen falschen Weg zu verlassen.

Lassen Sie uns also erstmal einen Schritt zurücktreten und nachdenken. Mehrfach war bisher von einer zentralen oder zentral zugänglichen Datenbank die Sprache. Vielleicht stellen Sie sich die Frage: Stimmt das überhaupt? Denn man könnte ja durchaus einwenden, dass es sich aufgrund der relativ großen Zahl unterschiedlicher Krankenkassen in Deutschland nicht wirklich um zentrale oder zentral zugängliche Datensammlungen handelt.

Tatsächlich aber ist die Anzahl der Versicherten zwischen den Krankenkassen extrem ungleich verteilt: So versicherten die vier größten Krankenkassen (AOK (gesamt), Techniker Krankenkasse, DAK-Gesundheit, Barmer GEK) im Jahr 2018 insgesamt 51.640.644 Bundesbürgerinnen und Bundesbürger, also deutlich über 50% der Gesamtbevölkerung[38]. Wenn man statt der „Gesamt-AOK“ nur die größte AOK (AOK Bayern) berücksichtigen möchte, beträgt die Zahl der Versicherten der vier größten Krankenversicherungen immer noch 29.698.853, d.h. es handelt sich um mehr als jeden dritten Bundesbürger.

35 Siehe z.B. gematik GmbH: Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur (September 2020)

36 „Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur digitalen Modernisierung von Versorgung und Pflege“ (Januar 2021)

37 Z.B. ebd., S. 5

38 Zahlen Stand 12/2019 nach https://krankenkassen.net/gesetzliche-krankenversicherung/mitgliederzahlen-der-gesetzlichen-krankenkassen.html#anzahl-der-versicherten

Hinzu kommt, dass aufgrund des hohen technischen Aufwandes für Einrichtung und Betrieb einer virtuellen Patientenakte davon auszugehen ist, dass verschiedene Krankenkassen unter Umständen letztlich auf denselben IT-Dienstleister zurückgreifen werden, der dann die eigentliche Speicherung, Verarbeitung und Zusammenführung der Daten übernimmt. Dies ist tatsächlich der Fall.

So stellt zum Beispiel Ronald Fritz von IBM fest: *„Die elektronische Patientenakte ist die gesetzlich vorgeschriebene Akte, die jede gesetzliche Krankenversicherung ihren Versicherten zum 1. Januar 2021 anbieten muss. […] IBM stellt diese ePA unter anderem den fast 24 Millionen Versicherten der Techniker Krankenkasse (TK), Barmer, Knappschaft, Viactiv und HEK zur Verfügung. Sie wird einen sicheren, zentralen Datenspeicher bereitstellen […].“*[39] Die genannten „24 Millionen Versicherten“, deren Daten zentral durch IBM gespeichert werden sollen, entsprechen ca. 29,5 % der Gesamtbevölkerung. Damit würden durch die medizinisch ungerechtfertigte Einführung einer virtuellen Patientenakte potentiell die medizinischen Daten von fast jedem dritten Bundesbürger im Rechenzentrum des Unternehmens gespeichert[40].

Im Folgenden wollen wir uns etwas näher anschauen, wie es eigentlich zur gesetzlichen Einführung einer virtuellen Patientenakte gekommen ist. Sie sind kein Jurist? Kein Problem. Gesetze sind vielleicht keine Strandlektüre, aber glücklicherweise müssen Gesetze in einem Rechtsstaat so formuliert werden, dass die Bürgerinnen und Bürger sie verstehen können[41].

Gesetzgebung zur virtuellen Patientenakte

Sie können also ruhig einmal in die erwähnten Gesetze schauen, sie sind kein Geheimnis. Und das Gute ist: Mit Blick auf die virtuelle Patientenakte gab es in letzter Zeit so viele Gesetze, da ist sicher auch eins für Sie dabei...Halt, moment mal - mehrere Gesetze in kurzer Zeit rund um dasselbe Thema? Warum eigentlich?

Einige der jüngeren Gesetze zur virtuellen Patientenakte sind das „Terminservice- und Versorgungsgesetz (TSVG)“ vom 6.5.2019, das „Digitale-Versorgung-Gesetz (DVG)“ vom 9.12.2019 oder auch das Gesetz vom 14.10.2020 mit dem klangvollen Namen „Patientendaten-Schutz-Gesetz (PDSG)“. Drei Gesetze rund um dasselbe Thema in weniger als anderthalb Jahren – das klingt nach ziemlich viel. Oder ist Gesetzgebung ein so simpler Prozess?

Wie entsteht ein Gesetz[42]? Zunächst wird es Gesetz innerhalb eines Ministeriums als Entwurf geschrieben („Referentenentwurf“), anschließend folgt ggf. eine öffentliche Diskussion mit Möglichkeit zur Stellungnahme durch z.B. Berufs- und Interessensverbände und eine Abstimmung der betroffenen Ministerien untereinander („Ressortabstimmung“). Anschließend wird der Entwurf an den Bundestag übermittelt, der sich mehrfach und zum Teil in den Fachausschüssen damit befasst („Lesungen“). Stimmt der Bundestag zu, geht das Gesetz weiter in den Bundesrat, der sich nochmal mit dem Gesetzesvorhaben befasst und ihm ggf. zustimmen muss.

Man könnte sagen, die Gesetzgebung ist wohl doch eher ein aufwändiger Prozess. Und trotzdem hat das Gesundheitsministerium innerhalb kurzer Zeit so viele Gesetze mit Bezügen zur Sammlung medizinischer Daten auf den Weg gebracht?

Vielleicht lohnt es sich, hier einmal einen Ausschnitt der Zeitleiste jüngerer Gesetzgebung zu betrachten:

39 https://www.ibm.com/de-de/blogs/think/2019/12/13/elektronische-patientenakte/ (zuletzt abgerufen 07.02.2020)

40 Die Speicherung erfolgt ja nicht, wie manchmal irrtümlicherweise angenommen wird, „bei der gematik“.

41 Anders als z.B. in der VR China, in der Gesetze auch gerne mal geheimgehalten werden (vgl. Gesetzgebung mit Bezug auf Hongkong).

42 z.B. Bundeszentrale für politische Bildung: „Gesetzgebungsverfahren“ (www.bpb.de/nachschlagen/lexika/recht-a-z/22287/gesetzgebungsverfahren)

23. 07. 2018: Referentenentwurf des TSVG
06. 05. 2019: TSVG tritt in Kraft (Einführung der „elektronischen Patientenakte zum 1.1.2021)
16. 05. 2019: Referentenentwurf des DVG
09. 12. 2019: DVG tritt in Kraft
29. 01. 2020: Referentenentwurf des PDSG
14. 10. 2020: PDSG tritt in Kraft
15. 11. 2020: Referentenentwurf DVPMG[43]

Das heißt, kaum war ein Gesetz in Kraft getreten, tauchte plötzlich der fix und fertig formulierte, 80...190seitige Referentenentwurf des nächsten Gesetzes auf. Interessant.

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt.": Die Würde des Menschen kann durch den Staat bzw. den Gesetzgeber auf zwei Arten missachtet werden: Einerseits durch gesetzliche Regelungen, deren Inhalt oder Vollzug die Menschenwürde verletzt. Andererseits durch einen Gesetzgebungsprozess, der die Würde der Bürgerinnen und Bürger missachtet, indem der Gesetzgeber sie über die Hintergründe und den Zweck der Gesetzgebung in die Irre führt und diese verschleiert. Möglicherweise in der Überzeugung, er (der Gesetzgeber) wisse ohnehin besser als die Bürgerinnen und Bürger selbst, was gut und richtig für sie sei. Er dürfe seine wahren Absichten verschleiern, damit die lästige „unqualifizierte" Kritik der Bürgerinnen und Bürger, die sonst zu erwarten wäre, die Gesetzgebung und ihre zügige Umsetzung nicht behindere. Damit er statt dessen die Bürgerinnen und Bürger ungehindert zu ihrem Glück zwingen könne, gewissermaßen das Modell der Chinesischen Kommunistischen Partei. Dieses Bild des Bürgers hätte allerdings wenig mit dem eines mündigen Bürgers zu tun und widerspräche dem Grundsatz einer demokratischen Gesellschaftsordnung. Und eingangs hatten wir ja andererseits bereits festgestellt, dass eine virtuelle elektronische Patientenakte eine sowohl unverhältnismäßige als auch unzweckmäßige Realisierung einer Patientenakte darstellt.

Nun gut, aber das Bundesgesundheitsministerium hatte ja nur auf den riesigen Bedarf bei den Patientinnen und Patienten reagiert. Oder etwa nicht?

Motivation zur Einführung einer virtuellen Patientenakte

Eine konkrete Antwort gibt der Beitrag „Elektronische Patientenakte: Kontrolle über die eigenen Gesundheitsdaten" des Vizepräsidenten „Health Platform Leader, Insurance" Ronald Fritz von IBM vom 13.12.2019[44] zu der im April 2018 gestarteten persönlichen Gesundheitsakte der Techniker Krankenkasse: „*Bestes und prominentestes Beispiel: der TK Safe, der von der TK und IBM gemeinsam entwickelt wurde und mittlerweile rund 250.000 Anwender hat.*" Die Techniker Krankenkasse hatte zu dem Zeitpunkt 7.681.839 Mitglieder und 10.176.612 Versicherte (Stand 12/2019[45]). Das heißt mehr als anderthalb Jahre nach Einführung einer persönlichen virtuellen elektronischen Gesundheitsakte hatten nur rund 3 % der Mitglieder (2,5 % der Versicherten) von der Möglichkeit Gebrauch gemacht, während ähnlich wie in Frankreich 97 % der Mitglieder (97,5 % der Versicherten) offensichtlich kein Interesse an einer virtuellen persönlichen Gesundheitsakte hatten. Wobei fraglich ist, ob selbst diese geringe Teilnehmerzahl nicht auch Versicherte als „Anwender" beinhaltet, die sich zwar registriert hatten, das Angebot aber nie aktiv nutzten.

Offensichtlich gab es seitens der Versicherten praktisch keinen Bedarf an einer virtuellen „elektronischen Gesundheits- oder Patientenakte".

43 „Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz"
44 https://www.ibm.com/de-de/blogs/think/2019/12/13/elektronische-patientenakte/ (zuletzt abgerufen 07.02.2020)
45 https://krankenkassen.net/gesetzliche-krankenversicherung/mitgliederzahlen-der-gesetzlichen-krankenkassen.html#anzahl-der-versicherten (zuletzt abgerufen 08.02.2020)

Nun könnte man vermuten, dass es seitens der Ärzteschaft einen dringenden Bedarf gegeben habe, eine virtuelle Patientenakte einzuführen.

Ein Blick auf die im TSVG wie auch den diversen Folgegesetzen vorgesehenen Sanktionen gegen Ärzte bei Verweigerung an der Teilnahme selbst an der „Telematikinfrastruktur“ sowie auf die öffentlichen Meinungsäußerungen der Ärzteschaft, z.B. im Rahmen der Ärztetage, macht schnell deutlich, dass auch hier - vorsichtig ausgedrückt - die Skepsis zu überwiegen scheint bzw. die Idee einer virtuellen Patientenakte bisher vehement abgelehnt wurde.

Offensichtlich gab es auch seitens der Ärzteschaft keinen Bedarf an einer virtuellen Patientenakte.

Wenn nun aber ein Gesetz oder ein Abfolge von Gesetzen, die vorgeblich den Zweck einer besseren Versorgung hat, weder verhältnismäßig noch zweckmäßig ist und weder durch einen Bedarf der Versorgten noch durch einen Bedarf der Versorgenden hinterlegt ist, stellt sich die Frage, ob sie überhaupt erforderlich ist.

Und natürlich auch, welchen Grund es nun eigentlich für den mit hohem Aufwand betriebenen Gesetzgebungsprozess gibt.

Einige indirekte Hinweise liefert die Erläuterung zu § 336 SGB V[46], dessen Regelungen auf die genannten Gesetze zurückgehen. Der Paragraph ermöglicht den Zugriff auf die virtuelle „elektronische Patientenakte“ ohne Einsatz der elektronischen Gesundheitskarte. In der Begründung des TSVG heißt es zu dem Thema beispielsweise (S. 74, II.3.10. Telematik):
„*[…] Viele Menschen nutzen in ihrem Alltag mobile Endgeräte wie zum Beispiel Smartphones oder Tablets, um zu kommunizieren, sich zu informieren oder Geschäfte des alltäglichen Lebens zu tätigen. Diese Lebensrealität soll mit den gesetzlichen Änderungen aufgenommen werden […]. Da die aktuellen gesetzlichen Regelungen nur einen Zugriff unter Einsatz der elektronischen Gesundheitskarte und mit solchen Komponenten und Diensten vorsehen, die nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik sicherheitszertifiziert sind (z. B. Kartenlesegerät), ist eine Anpassung der gesetzlichen Regelungen notwendig. […] Die Regelung, die einen zusätzlichen Zugriffsweg ohne Einsatz der elektronischen Gesundheitskarte vorsieht, zielt darauf ab, den Versicherten einen selbständigen Zugriff mittels mobiler Endgeräte wie Smartphones oder Tablets auf ihre medizinischen Daten der elektronischen Patientenakte zu ermöglichen und verpflichtet die Gesellschaft für Telematik, die Voraussetzungen dafür zu schaffen.*“

Die Begründung ist in mehrfacher Hinsicht aufschlussreich.

Zum Einen liegt hier aus logischer Sicht ein sogenannter „naturalistischer Fehlschluss“ vor: Aus der Tatsache, dass die aktuelle gesellschaftliche Realität (vermeintlich) eine bestimmte Ausprägung hat, wird gefolgert, dass dies so gut und richtig sei und daher als gesetzliche Regel festgeschrieben werden müsse. Dem Gesetzgeber wird die rein beschreibende Rolle des Chronisten einer Alltagswelt zugeschrieben, die durch die Marketingabteilungen der Hersteller mobiler Endgeräte geprägt ist.
Dabei ist selbst dieser Fehlschluss in sich nicht konsequent zu Ende geführt. Denn das Kriterium, dass viele Menschen im Alltag bestimmte Klassen von Dingen verwenden, „*um zu kommunizieren, sich zu informieren oder Geschäfte des alltäglichen Lebens zu tätigen“* gilt im Moment durchaus auch für soziale Medien wie Facebook und dessen „Parallelinternet“, sowie die Dienste von Google, Microsoft und Amazon oder für Geräte wie Amazon Echo und Google Nest. Diesen Netzwerken, Diensten und Geräten müssten nach dieser Logik konsequenterweise ebenfalls der Zugriff auf die persönliche virtuelle Patientenakte ermöglicht werden. Was mit Blick auf den Schutz der medizinischen Daten nicht unbedingt erstrebenswert wäre.

46 Stand vom 18.01.2021; es ändert sich ja recht schnell, wie wir gesehen haben...

Doch auch so wurde durch Einbeziehung mobiler Endgeräte das Sicherheitsniveau der virtuellen „elektronischen Patientenakte“ offensichtlich nochmal massiv abgesenkt. Und das mit der Begründung, im Bezug auf die virtuelle „elektronische Patientenakte“ (für die es praktisch keinen Bedarf gibt) auf den (unbelegten) zusätzlichen Bedarf zu reagieren, von unterwegs mobil auf die virtuelle „Patientenakte“ zuzugreifen. Das ergibt eigentlich keinen Sinn. Aber zumindest ist das Ganze eine sichere Sache...oder nicht?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit Blick auf die mobile Nutzung digitaler Gesundheitsanwendungen nüchtern fest: „*Ein kompromittiertes Smartphone kann somit das gesamte digitale Leben des Nutzers ungewollt offenlegen.*“[47] - und das reale Leben, möchte man hinzufügen. Mit Blick auf Perrows Diskussion von Hochrisikosystemen ist bemerkenswert, dass das BSI unter der Überschrift „Restrisiken“ ebenso nüchtern feststellt: „*Der Betrieb digitaler Gesundheitsanwendungen hat besonders hohe Anforderungen, die mit bestehenden Endgeräten und Cloud-Lösungen nur unzureichend abzudecken sind. […] Die offene Architektur vieler Plattformen begünstigt den Einsatz von Malware. Installierte Apps können bestehende Schwachstellen ausnutzen. […] Der Betrieb des Backends bei Public Cloud-Anbietern beinhaltet besondere Risiken für die sensiblen Daten der Nutzer. Während hohe Entropie, sichere Kommunikations- und Verschlüsselungsverfahren Risiken abmildern, sind in der Cloud Daten während der Verarbeitung quasi ungeschützt .[...]*“.[48]

Es erscheint völlig unverhältnismäßig, eine derartige Bresche in die Sicherung sensibler medizinische Daten zu schlagen, nur um es den Versicherten vermeintlich bequemer zu machen. Und zwar auch schon aus der Perspektive des Referentenentwurfs von 2018: Bereits 2017, ein Jahr vor dem Referentenentwurf zum TSVG, wurden über WikiLeaks Dokumente der CIA veröffentlicht, aus denen klar hervorging, mit welcher Leichtigkeit und Totalität auf mobile Endgeräte durch professionelle Hacker zugegriffen werden kann[49]. Hierüber wurde öffentlich berichtet, d.h. es war dem Gesetzgeber früh, noch vor Erstellung des Referentenentwurfs bekannt. Sollte er davor die Augen verschlossen haben?

Mir erscheint schwer vorstellbar, dass jemand ein derart dringendes und unaufschiebbares Bedürfnis nach einem Zugriff auf seine virtuelle Patientenakte und die Details der letzten Warzen- oder Wurzelbehandlung haben sollte, dass es diese Absenkung des Sicherheitsniveaus rechtfertigen könnte. In der Summe lässt sich festhalten, dass die vom Gesetzgeber angeführten Gründe unter dem Strich eigentlich keinen Sinn ergeben.

Was allerdings einen Sinn ergäbe, wäre, wenn es dem Gesetzgeber eigentlich gar nicht so sehr um den Versicherten und dessen Versorgung geht, sondern vor allem darum, dass Sekundäranwendungen und „Apps“ auf mobilen Geräten auf Inhalte der Patientenakte zugreifen können. Um so beispielsweise für die Hersteller entsprechender Sekundäranwendungen und Apps einen Markt vorzubereiten. Denn aus Sicht der Anbieter von „Mehrwertdiensten“/Sekundäranwendungen und Apps würde sich hier ein neues, lukratives Marktsegment eröffnen, dessen technische Hürden aus wirtschaftlicher Sicht möglichst gering sein sollten. Im Licht einer solchen Agenda ergäben die Regelungen Sinn und würden insbesondere aus Sicht des Gesetzgebers den gesetzgeberischen Aufwand nachvollziehbar erscheinen lassen. Der Bundesgesundheitsminister als heimlicher Bundeswirtschaftsminister?

Um hier zu einem klaren Bild zu kommen, gibt es naturgemäß nur die Möglichkeit, den Kontext der betreffenden Gesetzgebung näher anzuschauen.

Hintergrund der Gesetzgebung zur virtuellen Patientenakte

„*Datenschutz ist was für Gesunde.*“ - dieses Zitat aus dem 2016 erschienen Buch „App vom Arzt“ des späteren Gesundheitsministers Jens Spahn liefert einen ersten Hinweis auf die

47 Bundesamt für Sicherheit in der Informationstechnik: „Sicherheitsanforderungen an digitale Gesundheitsanwendungen“, Technische Richtlinie (BSI TR-03161), Version 1.0 (2020), S. 4

48 Ebd. S. 11

49 z.B.: https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/ (zuletzt abgerufen: 08.02.2020)

generelle Motivation der Einführung einer virtuellen Patientenakte[50]. Unter der Überschrift „Daten sind der Rohstoff der Zukunft“ beklagt Jens Spahn den „verkrampften“ Umgang mit Daten in Deutschland und führt als positives Gegenbeispiel aus: „*Unternehmen in den USA können erst einmal Berge von Daten ihrer Kunden sammeln und auf der Grundlage von Datenauswertungen nach und nach neue Geschäftsmodelle oder ein neues Produkt entwickeln. Das deutsche Datenschutzrecht schreibt dagegen vor, dass man Daten nur mit der ausdrücklichen Zustimmung des Kunden zu einem bestimmten, vorher definierten Zweck sammeln darf. Nur für diesen Zweck dürfen sie gespeichert und verarbeitet werden und müssen unaufgefordert wieder gelöscht werden, wenn dieser Zweck erfüllt ist. Der deutsche Ansatz mag Datenpuristen besser gefallen. Wahr ist aber auch, dass er es unseren Unternehmen unendlich viel schwerer macht, mit ihren amerikanischen Wettbewerbern mitzuhalten. […] Und den meisten Kunden ist es am Ende egal – sie nutzen munter Facebook, Instagram, Google & Co, weil es so schön bequem ist und sie nicht ständig irgendwelche Datenschutzerklärungen akzeptieren müssen. […] In Zeiten der Digitalisierung wird eine gute Datengrundlage immer wichtiger.*“[51]

Diese und ähnliche Äußerungen wären nicht relevant und könnten einfach als private Meinungsäußerung betrachtet werden...wenn der Erstautor Jens Spahn nicht wenig später als Bundesgesundheitsminister die oben aufgeführten Gesetze vorgelegt hätte, die zufälligerweise den Aufbau einer zentral zugänglichen Sammlung medizinischer Daten in Form einer virtuellen Patientenakte gesetzlich beauftragen. Und die dabei wie beschrieben das Sicherheitsniveau massiv senken, um den Zugriff über mobile Endgeräte zu ermöglichen.

So liegt die Vermutung nahe, dass das eigentliche Ziel nicht eine bessere medizinische Versorgung sondern der Aufbau eines Markts für Sekundäranwendungen und Apps ist. Die oben wiedergegebenen Zitate werfen überdies die Frage auf, ob es auch um die Sammlung personenbezogener medizinischer Daten mit dem Ziel ihrer wirtschaftlichen Verwertung geht und im Rahmen der inkrementellen Kettengesetzgebung irgendwann auch ihre Weitergabe angestrebt wird, z.B. als „Forschungsdaten“. Denn insbesondere Software, die Methoden des maschinellen Lernens verwendet, benötigt geeignete „Trainingsdatensätze“[52]

Werfen wir an dieser Stelle auch einen Blick auf die neuen gesetzlichen Regelungen[53], in denen die Krankenkassen als Datenzuträger die Sozialdaten ihrer Versicherten an den Spitzenverband Bund der Krankenkassen als Datensammelstelle übermitteln, der sie wiederum in bearbeiteter Form für Forschungszwecke zur Verfügung stellt. Und „Forschung“ meint hier nicht unbedingt „Krebsforschung“. Sie bedeutet durchaus auch die Entwicklung neuer Algorithmen maschinellen Lernens anhand von umfangreichen Trainingsdatensätzen. Und falls die Forschungsabsicht einmal nur vorgetäuscht sein sollten? Nun ja, sind die Daten erst einmal im Umlauf, kann man sie leider nicht wieder „zurückholen“...sorry.

Die Absicht, einen Markt für Sekundäranwendungen und Apps zu schaffen, lässt sich noch deutlicher herausarbeiten. Nahezu zeitgleich mit dem Inkrafttreten des TSVG wurde der Referentenentwurf des „Digitale-Versorgung-Gesetzes“ (DVG) in Umlauf gebracht, das inzwischen in Kraft getreten ist. Dort sind nun tatsächlich „Apps vom Arzt“, d.h. die Erstattung der Kosten digitaler Gesundheitsanwendungen vorgesehen. In der Tat wird hier also in unmittelbarem zeitlichen Zusammenhang ein Markt für oben genannte Sekundäranwendungen und Apps geschaffen.

Die mit den Gesetzentwürfen verfolgte Absicht wird noch klarer, wenn man darüber hinaus den mit Art. 1 Abs. 29 DVG eingeführten §263a des „Fünften Buchs Sozialgesetzbuch“ (SGB V) betrachtet. Dort wird den Krankenkassen die Möglichkeit eingeräumt, mit bis zu 2% ihrer Finanzreserven in Investmentvermögen „zur Förderung der Entwicklung digitaler

50 J. Spahn, M. Müschenich und J. F. Debatin: „App vom Arzt“, Herder Verlag (Freiburg), 2016, S. 2
51 Ebd., S. 18
52 Wohl eine der Motivationen für kommerzielle Anbieter von Speicherplatz für Daten „in der Cloud“.
53 „Digitale-Versorgung-Gesetz“, §§303a-303f SGB V

Innovationen“ zu investieren. Das heißt: Hier wird in unmittelbarem zeitlichen Zusammenhang eine Wirtschafts- und Technologieförderung durch die Krankenkassen ermöglicht, u.a. genau für die genannten Sekundäranwendungen und Apps. Die Krankenkassen sollen mit dieser Regelung also zu einem wirtschaftlichen Nutznießer der Verwertung medizinischer Daten durch die „digitalen Gesundheitsanwendungen“ werden, z.B. über die Rendite der Investmentanlage. Damit verlieren sie nur wenige Monate nach Inkrafttreten des TSVG mit seinen Regelungen zur Einführung der virtuellen Patientenakte bereits ihre Rolle als neutraler Datenverwalter ohne eigenes Interesse. Und sehen sich plötzlich einem wirtschaftlichen Anreiz gegenüber, für die Weiterverwertung der ihnen anvertrauten Daten zu sorgen, z.B. indem sie ihre Versicherten zu einer „Datenspende“ drängen.

Die Rolle des ärztlichen Personals

Zudem kommt hinzu, dass sich die Ärztinnen und Ärzte einer Weitergabe der medizinischen Daten ihrer Patienten an die zentralen Datenbanken nicht verweigern dürfen, wenn der Patient sie dazu auffordert. Auch dann nicht, wenn die Weitergabe an Dritte nach ihrer Überzeugung in keiner Weise der Behandlung dient oder im Interesse des Patienten ist. Diese Aushöhlung der ärztlichen Verantwortung und Schweigepflicht und die Reduktion des ärztlichen Personals auf eine Rolle als Dienstleister für die Befüllung und Pflege einer zentralen Datenbank personenbezogener medizinischer Daten dient keinem erkennbaren medizinischen, dafür aber einem um so besser erkennbaren wirtschaftlichen Zweck. Diese Zwangsverpflichtung als „Makler“ und „Dienstleister“ einer Plattform zur Wirtschaftsförderung greift dabei tief in die Freiheit der ärztlichen Berufsausübung ein.

Als unabhängige Perspektive soll hier noch die Sicht eines technischen Dienstleisters wiedergegeben werden[54]. So schreibt der oben genannte Vizepräsident der Firma IBM im Dezember 2019: „*Die elektronische Gesundheitsakte war und ist Ausgangspunkt jedes zusätzlichen Nutzererlebnisses und innovativer Mehrwertdienste im Kontext Gesundheit. […] Oberhalb der ePA [Anmerkung: ePA: elektronische Patientenakte] werden diese ePA-Daten und historische Daten vergangener Gesundheits- und Krankheitsverläufe[55] an eGA-Mehrwertdienste [Anmerkung: eGA: elektronische Gesundheitsakte] übergeben, Ableitungen getroffen, sowie Analysen der Versicherten in ihrer Hoheit gestartet. Die eGA bietet damit den nötigen Raum für das „Feuerwerk an Ideen und Kreativität“ bei möglichen Zusatzfunktionen der ePA, von dem Bundesgesundheitsminister Jens Spahn sprach. Zudem erlaubt die eGA die wettbewerbliche Differenzierung der Kassen untereinander. […] Bürger können damit ihre lebenslangen Gesundheitsinformationen besser nutzen, etwa dank erprobter und prädiktiver Datenanalyse. […] Unsere klare Idee dabei: fragmentierte Datenhaltung irgendwo in der Welt vermeiden und stattdessen die persönliche Akte als zentralen, sicheren Datenspeicher etablieren, aus dem sich digitale Gesundheitsanwendungen bedienen und in die sie wiederum hinein speichern können.*“

Die erwähnte prädiktive Datenanalyse wird dabei typischerweise auf Methoden des maschinellen Lernens beruhen; das wiederum möglichst umfangreiche Datensätze zum „Anlernen“ benötigt.

Diese Wahrnehmung der mit der Einführung der virtuellen „elektronischen Patientenakte“ und ihrer Ausgestaltung verbundenen Absicht, nämlich die Verwendung von „*Mehrwertdiensten*“ und „digitalen Gesundheitsanwendungen“ zu ermöglichen, die sich „*aus der persönlichen Akte bedienen und in die sie wiederum speichern können*“ deckt sich offensichtlich mit der oben rekonstruierten Absicht des Gesetzgebers[56]. Der Aspekt einer verbesserten Transparenz, Wirtschaftlichkeit und Qualität der Versorgung spielt keine wesentliche Rolle, höchstens

54 https://www.ibm.com/de-de/blogs/think/2019/12/13/elektronische-patientenakte/ (zuletzt abgerufen 07.02.2020)

55 Die Terminologie des Autors bezüglich „Patientenakte“/„Gesundheitsakte“ ist hier etwas unklar, so wären z.B. historische Krankheitsverläufe ja ebenfalls Teil der Patientenakte.

56 s.a. „Die elektronische Patientenakte“, Bundesministerium für Gesundheit (https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/elekrtonische-patientenakte.html (zuletzt abgerufen: 07.03.2020)

nachrangig in Form eines impliziten, allgemeinen Deckmäntelchens für die eigentlich angestrebte Wirtschafts- und Technologieförderung, für die Ärzten und Patienten als Zuträger rekrutiert werden sollen.

Dieses Ziel einer Wirtschafts- und Technologieförderung wird mit jedem neuen Gesetz klarer und zeigt sich besonders deutlich in der bereits angedeuteten Rolle, die der Gesetzgeber für die Krankenkassen quasi neu schafft.

Die neue Rolle der Kranken-kassen

Eigentlich sind Krankenkassen ja Einrichtungen, die ohnehin Einiges über die Versicherten wissen und denen man vertrauen können möchte. In Art. 1 Nr. 6a PDSG räumt der Gesetzgeber den Krankenkassen nun aber das Recht ein, ihren Versicherten individualisierte „Versorgungsinnovationen“ oder „Versorgungsleistungen“ anzubieten[57]. Dahinter steht natürlich die Erwartung an die Krankenkassen, dieses Recht auch tatsächlich in Anspruch zu nehmen. Was bedeutet das?

Die Unterbreitung *individualisierter* Angebote durch die Krankenkassen setzt logisch voraus, dass diese erst einmal individuelle Profile ihrer Versicherten erstellen, die den Krankenkassen dann ja erst eine Individualisierung ihrer Angebote erlauben[58]. Es geht eben nicht um Angebote „für Handwerker“ oder „für Studenten“, sondern um *individualisierte* Angebote speziell für Sie, Max Mustermann aus Musterstadt, geschieden, zwei Kinder, Beruf ..., im Zeitraum X arbeitslos, in der Vergangenheit in Behandlung bei Hausärztin Y und Facharzt Z, wobei zu folgenden Zeitpunkten folgende diagnoseabhängige Leistungen abgerechnet wurden… Sie verstehen, worauf ich hinauswill. Und für Ihren Partner. Und Ihre Kinder.

Da es sich bei den angebotenen „Innovationen“ und „Leistungen“ im Kontext von Krankenkassen naturgemäß um solche mit medizinischem Bezug handeln wird, werden also auch die von den Krankenkassen erstellten Profile ihrer Versicherten vor allem medizinische Profile sein, basierend auf den Daten, auf denen die Krankenkassen als Einrichtungen in einer Vertrauensposition Zugriff haben.

Bei den „individuell geeigneten Versorgungsinnovationen“ wird es sich um digitale Anwendungen („Apps“) handeln, die bei ihrer Nutzung durch die Versicherten kontinuierlich Gesundheits- aber auch Metadaten der Versicherten erfassen. Diese Daten sind grundsätzlich wieder zur weiteren Profilbildung oder Verfeinerung von persönlichen Profilen geeignet.

Dies bedeutet, dass den Krankenkassen droht, selbst zum Profilersteller und -sammler zu werden: Sie erstellen medizinische Profile ihrer Versicherten und können diese zentral sammeln, auswerten, teilen – ggf. mit Entwicklern digitaler Anwendungen bis hin zu professionellen Datenhändlern – und können sie grundsätzlich zeitlich und inhaltlich unbegrenzt weiter bis hin zu „Totalabbildern der Persönlichkeit“ verfeinern, unter Umständen auch anhand von personenbezogenen Datenströmen, die gemäß des neuen § 345 SGB V aus den „individuell geeigneten Versorgungsinnovationen“ oder den „zusätzlichen Inhalten und Anwendungen“ zu den Krankenkassen fließen.

Indem die Krankenkassen auf Wunsch des Gesetzgebers damit auch noch selbst begännen, umfassende Sammlungen medizinischer Profile ihrer Versicherten anzulegen, stiege auch die Wahrscheinlichkeit einer irregulären Aneignung oder/und missbräuchlichen Verwendung medizinischer Profile der Bürgerinnen und Bürger.

Bezüglich der Krankenkassen entsteht also eine hochproblematische neue Rolle und Datenmacht durch Datenanhäufung und Anreize zur Profilbildung, die der Gesetzgeber den Krankenkassen bzw. ihren Dienstleistern im Zuge seiner inkrementellen Gesetzgebung überträgt, indem sie:

57 Zusätzlich gilt, dass die Versicherten dem erst im Nachhinein widersprechen können.

58 Dies ist völlig analog zur individualisierten Werbung auf der Grundlage von Persönlichkeitsprofilen z.B. durch virtuelle „Soziale Netzwerke“.

- die personenbezogenen medizinischen Daten ihrer Versicherten in einer virtuellen „elektronischen Patientenakte“ zentral speichern und verwalten dürfen (§ 342 SGB V), wenngleich sie keinen Zugriff auf die Daten haben dürfen (§ 343 Abs. 1 SGB V, § 344 Abs. 2 SGB V)

- diese Daten dem Forschungsdatenzentrum bei Einverständnis der Versicherten pseudonymisiert, verschlüsselt und unbefristet zur Verfügung stellen (§ 341 SGB V, § 363 SGB V),

- diese Daten und die anderer Versicherter vom Forschungsdatenzentrum in anonymisierter Form wieder abrufen können und dadurch volle inhaltliche Zugriffs- und Vervielfältigungsrechte bezüglich der Daten erhalten (§ 303e SGB V),

- sie gleichzeitig ermuntert werden zu einer Profilerstellung oder „Katalogisierung“ ihrer Versicherten, um ihnen „individuell geeignete Versorgungsinnovationen“ anzubieten (Art. 1 Nr. 6a PDSG), deren Entwicklung ja wiederum eine Datenabfrage nach § 303e SGB V rechtfertigt, wobei sie

- selbst als gewinnorientierter Investor auftreten und bis zu 2 % ihrer Finanzreserven in Investmentvermögen zur „Förderung der Entwicklung digitaler Innovation“ einbringen dürfen, sofern ein „angemessener Ertrag“ erzielt werde (§ 263a SGB V).

Der Gesundheitsminister höhlt die Vertrauensstellung der – nun nicht mehr ohne Eigeninteresse handelnden - Krankenkassen aus und erhöht weiter die Menge und Verbreitung von Datensätzen personenbezogener medizinischer Daten der Bürgerinnen und Bürger. Er erhöht dadurch signifikant die Wahrscheinlichkeit einer irregulären Datenaneignung und Verwendung zur Erstellung von Teil- oder Totalabbildern der Persönlichkeit der Bürgerinnen und Bürger. Durch den Aufbau zentraler Sammlungen macht er die Patienten und ihre Daten zum digitalen Angriffsziel. Durch die Zwangsverpflichtung des ärztlichen Personals zur Mitwirkung an der Erstellung zentraler Sammlungen medizinischer Daten fordert der Gesetzgeber zudem eine „Komplizenschaft“, die eigentlich nicht mit meinem Verständnis der ärztlichen Tätigkeit vereinbar ist.

Datensammlung am Forschungsdatenzentrum

Mit dem PDSG wurde neu auch die sogenannte „Datenspende“[59] eingeführt. Darin zeigt sich nun bereits die problematische Eigendynamik einer zentralen Sammlung personenbezogener medizinischer Daten in einer Datenbank, die zu immer neuen Begehrlichkeiten führen wird. Bei der „Datenspende“ geht es um die Möglichkeit zur weitgehend bedingungslosen, vollständigen oder teilweisen Freigabe personenbezogener medizinischer Daten aus der virtuellen Patientenakte zu Forschungszwecken.

Der Begriff „Datenspende“ suggeriert dabei eine Analogie beispielsweise zur Organ- oder Knochenmarkspende. Eine Analogie, die jedoch an wesentlichen Punkten nicht zutrifft.

Zum Einen sind anders als bei der lebensrettenden Spende eigener Organen oder eigenen Körpergewebes die „Eigentumsverhältnisse“ genetisch geteilter und mit Diagnosen verknüpfter medizinischer Daten weniger klar. Die Freigabe von genetisch geteilten Daten durch eine andere Person aufgrund der beabsichtigten Datenanalyse und der mit ihnen verbundenen Prognose- und Rekonstruktionsmöglichkeiten kann nach meinem Verständnis bereits das Recht auf informationelle Selbstbestimmung verletzen.

Zum andern können gespendete Organe oder gespendetes Knochenmarksgewebe - auch bei einer großen Zahl von Spendern - kaum zum Schaden Anderer oder zum Schaden einer

59 Z.B. in der Erläuterung des PDSG auf der Website des BMG (www.bundesgesundheitsministerium.de/patientendaten-schutz-gesetz.html, zuletzt abgerufen September 2020)

freiheitlich-demokratisch verfassten Gesellschaft führen. Dies verhält sich jedoch im Fall einer großen Sammlung personenbezogener medizinischer Daten[60] deutlich anders: Sie eignen sich offensichtlich ganz hervorragend zur – potentiell massenhaften – Erstellung von Persönlichkeitsprofilen, welche wiederum bereits gegen die freiheitlich-demokratischer Grundordnungen eingesetzt wurden, wie wir im zweiten Teil sehen werden.

Statt nun aber die umfassende Sammlung von Daten und deren Verwertung zur Profilerstellung einzudämmen, will sich der Gesetzgeber selbst daran beteiligen bzw. sie aktiv fördern.

Mit dem neuen § 363 SGB V wird die Möglichkeit geschaffen, an einem Forschungsdatenzentrum eine bundesweite, zentrale, inhaltlich, anzahlmäßig und zeitlich unbegrenzte, umfassende und fortlaufend aktualisierte Vorratsdatenspeicherung der personenbezogenen medizinischen Daten potentiell aller Bundesbürgerinnen und Bundesbürger durchzuführen, sobald die Versicherten der Preisgabe ihrer Daten einmal zustimmen und sie diese Freigabe nicht zu einem späteren Zeitpunkt widerrufen[61]. Wobei die Daten zu diesem Zeitpunkt vielleicht schon weitergegeben und unwiderruflich verwendet wurden.

Über die weitere Verwendung dieser – lediglich pseudonymisierten – Daten entscheidet dann das Forschungsdatenzentrum ohne weitere Mitwirkung der Versicherten oder der Öffentlichkeit, lediglich eingeschränkt durch die im neuen § 363 Abs. 1 SGB V genannten Forschungszwecke und die Vorgaben gemäß § 303e SGB V.

Dabei gilt, dass Patienten, auch wenn sie sich selbst als einzelne Versicherte gegen die entsprechende Speicherung und Freigabe der eigenen Daten entscheiden, um die Folgen einer massenhaften Profilerstellung zu vermeiden, sie den gesellschaftlichen Folgen einer potentiellen Massenspeicherung dennoch ausgeliefert sind.

Ein Fallbeispiel: Google

Gemäß § 303e SGB V Abs. 1 umfasst der Kreis der Nutzungsberechtigten der Forschungsdatenbank unter anderem „Hochschulen“ und „sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, sofern die Daten wissenschaftlichen Vorhaben dienen“.

Hier muss man auf den Fall „Aleksandr Kogan“ zu verweisen, auf den wir später noch zurückkommen. Dort war Ausgangspunkt einer massenhaften Datenaneignung ebenfalls eine vermeintlich wissenschaftliche Untersuchung, Aleksandr Kogan war dabei wissenschaftlicher Mitarbeiter an zwei Universitäten.

Zum Anderen gilt jedoch, dass Universitäten und Forschungseinrichtungen typischerweise in Kooperationen mit zahlreichen anderen nationalen oder internationalen Universitäten und Forschungseinrichtungen und Wirtschaftsunternehmen stehen, welche sich ihrer Kontrolle in der Praxis naturgemäß entziehen.

Als ein Beispiel sei die seit 2018 bestehende Forschungspartnerschaft zwischen der „*für die besonders intensive und intelligente Vernetzung der Ingenieurswissenschaften mit*

60 Wobei die Daten, wie früher bereits ausgeführt, nicht auf Befunde, Therapien etc. zu beispielsweise Blinddarmbeschwerden oder eingewachsenen Fußnägeln o.ä. beschränkt sind, sondern auch intimste Dinge wie traumatisierende Erfahrungen, Drogenmissbrauch, persönliche Schicksalsschläge, psychologische Auffälligkeiten etc. umfassen können und damit unter Umständen auf die verletzlichsten Punkte der Persönlichkeit verweisen. Gleichzeitig sind es gerade die verletzlichsten Mitbürger, die die geringsten Ressourcen und Energien haben, um den Überblick über die Nutzung ihrer einmal in einer Datenbank gespeicherten Daten behalten oder sich mit ihr auseinandersetzen und ihr ggf. widersprechen zu können, vielleicht sogar gegen Anraten ihres Arztes, der für die Befüllung der virtuellen „elektronischen Patientenakte“ eine Vergütung erhält.

61 Wobei für mich eine offene Frage ist, was nach dem Tod des Betreffenden mit dessen Daten geschieht.

Naturwissenschaften und Medizin“[62] bekannten Technischen Universität München und dem Konzern „Google“ im Bereich Künstliche Intelligenz und Maschinelles Lernen genannt. Die insbesondere auf Anwendungsfälle Künstlicher Intelligenz zielt und „*personelle Unterstützung*“[63] beinhaltet.

Tatsächlich scheint die Beziehung zwischen dem amerikanischen Konzern „Google“ und Stadt und Technischer Universität München besonders heiß und innig zu sein.

So findet sich in der in München erscheinenden „*Süddeutschen Zeitung*“ regelmäßig eine Werbebeilage des Unternehmens, die in Format, Aufmachung und Titel („Aufbruch – Mensch und Gesellschaft im digitalen Wandel“) den Eindruck einer seriösen Veröffentlichung erweckt und sich erst bei genauerem Hinsehen als Firmenbroschüre entpuppt.

Mit der Werbebeilage schlägt der Konzern mehrere Fliegen mit einer Klappe. Er profitiert vom guten Ruf der renommierten Zeitung, erreicht bundesweit Personen des öffentlichen Lebens, wird durch die Werbegebühren zu einem Geldgeber einer potentiell kritischen und investigativ arbeitenden Zeitung, und - weil es sich um eine Beilage handelt - das Unternehmen „Google“ kommt um die deutliche Kennzeichnung als Anzeige herum. Tatsächlich findet sich erst auf Seite 2 unten in mikroskopisch kleiner Schrift der Hinweis, dass es sich um eine Anzeigenveröffentlichung des Unternehmens handelt.

Dennoch ist die Lektüre nicht ohne Erkenntnisgewinn.

Im Januar 2021 konnte man z.B. auf der Titelseite der Werbeschrift die doch etwas überraschende Schlagzeile lesen: „*Für die Privatsphäre: Daran arbeitet das Google-Team in München*“[64]. Blättert man nach hinten, um mehr über dieses phänomenale Münchner Google-Team zu erfahren, stößt man - neben dem Münchner „Google Safety Engineering Center“ und dessen Ausbau der Nutzerbindung an das Google Benutzerkonto zur Umgehung der „Cookie-Richtlinie“ bei der Profilerstellung - auf die Professorin Dr. Alena Buyx von der Technischen Universität München. In einem ausführlichen „Interview“ mit dem offensichtlichen Ziel, die für den Datensammler und -verwerter Google lästigen Datenschutzregeln als überholt und vermeintlich innovationsfeindlich darzustellen.

Das pseudo-journalistische Frage-Antwort-Spiel mündet konsequenterweise in die (praktisch neutrale) Frage, was denn „*guten von schlechtem Datenschutz*“ unterscheide[65]. Na gut, vielleicht ist sie doch irgendwie suggestiv. Und die Professorin der TU München antwortet brav: „*Von schlechtem […] Datenschutz spreche ich, wenn er nicht mehr zu den Gegebenheiten passt oder wenn er wichtige soziale Güter unmöglich macht. Dann ist Datenschutz auch ein Innovationshemmer.*“[66]

Ist Professor Buyx von der Technischen Universität München also vielleicht einfach eine medien-unerfahrene Informatikerin? Ein Nerd, der einen schlechten Tag hatte und nicht verstanden hat, dass sie als Wissenschaftlerin gerade die Rolle eines sogenannten „Mietmauls“ für einen Konzern spielt[67]? Ähm, nein. Wohl leider nicht.

---

62 "Google investiert in Wissenschaft ‚Made in Germany‘“ (Pressemitteilung der TU München, 16.02.2018, https://www.tum.de/nc/die tum/aktuelles/pressemitteilungen/details/34489, zuletzt abgerufen 22.09.2020)

63 Ebd.

64 Google*: „Aufbruch – Mensch und Gesellschaft im digitalen Wandel, Ausgabe Nr. 22*“ , Anzeigenveröffentlichung, (2021)

65 Ja, Sie haben richtig gelesen, kein Scherz.

66 Ebd., S. 27

67 Wobei sich dies nicht auf Wissenschaftler/innen beschränkt. So findet sich auf der letzten Seite der Werbebroschüre ein isoliert betrachtet scheinbar harmloses, pseudo-journalistisches Interview mit einer verantwortlichen Juristin des Statistischen Bundesamtes, also einer Bundesbehörde. Könnte das im Kontext einer Google-Broschüre vielleicht als Feigenblatt oder gar dazu dienen, die Normalität der hemmungslosen Datensammlung kommerzieller „Datenkraken“ und Profilersteller zu suggerieren, indem

Die approbierte Ärztin Professor Buyx ist Direktorin des Instituts für Geschichte und Ethik der Medizin an der TU München und seit 2020 Vorsitzende des Deutschen Ethikrats. Also medienerfahrene Vorsitzende genau des Gremiums, das die Bundesregierung berät, wenn es um ethische Fragen bezüglich Ihrer medizinischen Daten geht. Und das in der Vergangenheit auch schon getan hat. Zum Beispiel mit der Stellungnahme „*Big Data und Gesundheit*“[68]. In der es unter anderem heißt: „*Wo sich tradierte Instrumente – wie die bislang gängige strikte Orientierung an Datensparsamkeit und enger Zweckbindung – als dysfunktional erweisen, müssen deshalb andere Möglichkeiten […] in den Vordergrund treten. […] Um die Potenziale von Big Data im Gesundheitsbereich zu realisieren, ist eine möglichst reibungsfreie Kooperation zwischen zahlreichen Akteuren aus der klinischen Praxis, medizinbezogener Grundlagenforschung, in gesundheitsrelevanten Feldern tätigen Unternehmen und individuellen Datengebern nötig.[...]*“.

Auch beim weiteren Lesen der verklausulierten Empfehlungen dieser Stellungnahme kann man sich der Frage nicht erwehren, ob womöglich der Weihnachtsmann auf dem Weg zum Nordpol den Wunschzettel von Datenverwertern wie Facebook oder Google versehentlich in den Briefkasten des Deutschen Ethikrats gelegt hat[69].

Als einziges Mitglied des Ethikrates stellte sich übrigens eine andere Ärztin offen und unmissverständlich gegen die Empfehlungen: Dr. Christiane Fischer, u.a. Gründungsmitglied der gegen Korruption im Gesundheitswesen gerichteten Initiative „MEZIS“.

Die „Big Data“-Stellungnahme des Deutschen Ethikrates entstand, wie die TU München betont, unter intensiver Mitarbeit von Professor Bruyx und wurde nach längerer Vorarbeit im Jahr 2018 veröffentlicht. Also zwei Jahre nachdem der spätere Gesundheitsminister Jens Spahn in seinem Buch „App vom Arzt“ mit der frei erfundenen Behauptung „*Datenschutz ist was für Gesunde*“ den Schutz Ihrer medizinischen Daten, liebe Leserinnen und Leser, als Luxus für die Glücklichen unter Ihnen reserviert hat, die nie krank werden...

Beginnen Sie, sich Sorgen um Ihre medizinischen Daten zu machen? Das sollten Sie auch.

Aber bleiben wir noch kurz in München. Das Unternehmen Google ist nämlich nicht das einzige, das seine Liebe zur Technischen Universität München entdeckt hat. So gibt es an der Münchner Universität gewissermaßen das Digital-Äquivalent zu einem „Donald Trump-Institut für Ethik in der Politik“, nämlich ein vom Unternehmen Facebook finanziertes „Institut für Ethik in der Künstlichen Intelligenz“[70]. Kritikern dieser Liaison hält der frischgebackene Institutsleiter und Unternehmensethiker entgegen, dass er es wesentlich vertrauenswürdiger finde, „Geld von einem Unternehmen zu nehmen als von einer Einzelperson“[71] Hm. Da könnte man natürlich fragen, ob z.B. der Friedensnobelpreis wirklich ethisch vertrauenswürdiger wäre, wenn er nicht von Alfred Nobel gestiftet worden wäre sondern von Rheinmetall oder Heckler&Koch.

---

sie mit der gesetzlich klar reglementierten, kontrollierten und umgrenzten Datenerhebung öffentlicher Stellen gleichgesetzt und dadurch verharmlost wird? Hm...

68 Deutscher Ethikrat: „Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestalung, Stellungnahme vom 30.11.2017“, Berlin (2018).

69 Ebd. S. 262ff.; die Stellungnahme enthält allerdings als abweichende Einzelstimme auch ein sehr kritisches „Sondervotum“ der Ärztin Christiane Fischer, das u.a. einen deutlich größeren Schwerpunkt auf Datenschutz und -autonomie legt.

70 Technische Universität München: „Facebook fördert die TU München – Neues Forschungsinstitut für Ethik in der Künstlichen Intelligenz, Pressemitteilung vom 20.01.2019

71 S. Buchwald: „TU München und Facebook: Zweifel an Unabhängigkeit“, 13.12.2019, Süddeutsche Zeitung, (online: https://www.sueddeutsche.de/muenchen/muenchen-tu-finanzierung-facebook-1.4723566, zuletzt abgerufen März 2021)

Vielleicht könnte man sagen: Es kommt immer darauf an, wer das andere Ende des Geldscheins in der Hand hält. Und warum. Na schön, man kann das ruhig auch mal positiv sehen: Es ist doch ein wunderbarer Beleg für die unvorhersehbaren Wendungen des Lebens und damit ein schöner Zufall, dass ausgerechnet kurz nach Bekanntwerden der Machenschaften von „Cambridge Analytica“ und der zentralen Rolle von Facebook und seines Geschäftsmodells[72] das Unternehmen öffentlichkeitswirksam eine Universität gesucht und gefunden (oder sie sich angedient[73]) hat, an der es die Gründung eines Ethik-Instituts inszenieren konnte.

Und es ist doch ebenfalls ein sehr schöner Zufall, dass ausgerechnet ein Wirtschafts- und Unternehmensethiker, der Professor der Technischen Universtität München ist, Leiter des neuen Instituts wird. Nein, moment, das war jetzt kein Zufall sondern von Facebook vertraglich gefordert[74]. Aber trotzdem: Das ist doch schön.

Und es ist doch nur natürlich, dass der Münchner Professor dem Unternehmen reinen Herzens und gerne bescheinigt, dass dort ein Umdenken einsetze. Nun erscheint diese Einschätzung rückblickend vielleicht ein klein wenig optimistisch - aber bitte, wer hat sich noch nie geirrt? Oder wollen Sie vielleicht behaupten, dass der neue Institutsleiter irgendeinen Grund haben sollte, seinem Gönner und Forschungsgeldgeber irgendwie unkritisch gegenüber zu stehen? Welcher Grund sollte das sein?

Er ist im Gegenteil ein kritischer Geist. Zum Beispiel kritisiert er gerne die Fokussierung von ethischen Debatten auf gesetzliche Regulierung und Bürgerrechte, wie Datenschutz oder Privatsphäre. Während die Unternehmensperspektive und die Bedeutung von klaren ethischen Regeln und Business Ethik - also freiwilliger Selbstverpflichtungen - viel zu kurz kommen[75]. Wobei man sich natürlich fragen kann, wie gut Selbstverpflichtungen gerade bei Tech-Firmen funktionieren.

Und die Technische Universität München wehrt sich doch völlig zu Recht dagegen, dass das Teilen ihres guten Rufs mit dem absolut seriösen Datenausbeuter und Profilersteller Facebook unter Generalverdacht gestellt wird[76]. Es gebe schließlich keinerlei Auflagen oder Erwartungen, und die akademische Freiheit sei natürlich gewährleistet[77] [78]. Alles gut.

Schön, man *könnte* vielleicht einwenden, dass jemand, der sich beruflich mit Unternehmen und Ethik beschäftigt, da etwas stärker sensibilisiert sein und sich seine Geldgeber genauer

72 Wir werden in Teil 2 darauf zurückkommen.

73 Das war zumindest mein spontaner Gedanke angesichts einer drei Absätze langen juristischen Absicherung von Facebook und Ermahnung der TU München im Vertrag, sich an geltendes Recht und Regeln zu halten , vgl.: C. Köver/I. Dachwitz: „Ein Geschenk auf Raten“, 18.12.2019, netzpolitik.org (https://netzpolitik.org/2019/ein-geschenk-auf-raten/#Schenkungsvertrag)

74 S. Buchwald: „TU München und Facebook: Zweifel an Unabhängigkeit“, 13.12.2019, Süddeutsche Zeitung, (online: https://www.sueddeutsche.de/muenchen/muenchen-tu-finanzierung-facebook-1.4723566, zuletzt abgerufen März 2021)

75 C. Lütge: „There ist not enoough business ethics in the ethics of digitization“, in Ciulla/Scharding: „Ethical Business Leadership in Troubling Times“, Edward Elgar Publishing, 2019.

76 I. Dachwitz: „Verhaltensbasierte Werbung: Facebook identifiziert emotional verletzliche Jugendliche“, 2.5.2017, netzpolitik.org (https://netzpolitik.org/2017/verhaltensbasierte-werbung-facebook-australien-analysiert-emotionen-und-aengste-von-jugendlichen, zuletzt abgeufen März 2021)

77 S. Buchwald: „Eine Frage der Ethik“, 7.10.2019, Süddeutsche Zeitung (online: https://www.sueddeutsche.de/muenchen/muenchen-tum-facebook-institut-ethik-1.4630292, zuletzt abgerufen März 2021)

78 M. Hauck: „TU München verteidigt Kooperation mit Facebook“, 21.01.2019, Süddeutsche Zeitung

ansehen sollte[79]. Er sich vielleicht sogar Gedanken über die Ethik des eigenen Handelns und seine Implikationen machen könnte.

Man könnte vielleicht auch vermuten, dass korrumpierende Prozesse selten „transparent“ mit offen ausgesprochenen Auflagen und Erwartungen einhergehen. Also, überspitzt formuliert: Wenn Ihnen der lokale Mafioso eine Finanzspritze für die Eröffnung Ihrer Pizzeria gewährt, möchte er auch nicht mit Ihnen über Kochrezepte oder die Speisekarte diskutieren. Er will ja nicht Ihren Laden kaufen, sondern Ihre Loyalität.

Er will Ihnen einfach nur einen Gefallen tun. Und es Sie wissen lassen. Damit Sie in seiner Schuld stehen. Und ihm später vielleicht auch einmal einen Gefallen tun, wenn der Bedarf da ist. Und Sie auf keinen Fall gegen seine Interessen handeln. Korruption beginnt mit Gefälligkeiten. Ganz ohne Auflagen und Erwartungen. Einfach so. Also sollte man vielleicht ein wenig aufpassen, von wem man Geschenke annimmt...

Das gilt übrigens auch für das Gesundheitswesen. Der Name des oben erwähnten Anti-Korruptions-Vereins „MEZIS“ beispielsweise ist eine Abkürzung für: „Mein Essen zahle ich selbst“. Dahinter steht die übliche Praxis, dass Pharmaunternehmen Ärzten hochkarätige Fortbildungen anbieten, gerne kostenlos oder günstig in teuren Hotelsmit exquisiter Küche. Auch das ist ja nicht einfach eine Butterfahrt,bei der das Unternehmen stundenlang plump seine eigenen Medikamente anpreist. Es geht weniger um die Inhalte, sondern um den Rahmen und die Einbettung, die aus der Veranstaltung eine einzige große Gefälligkeit machen. Natürlich ganz ohne Auflagen oder Erwartungen.

Einfach so.

Ach, Sie wollen die Inhalte Ihres Gesundheitsport gerne ganz oben in den Suchergebnissen haben, liebes Ministerium[80]? Den kleinen Gefallen tun wir Ihnen gerne. Sehr gerne sogar. Kein Problem, machen wir einfach über den kurzen Draht. Natürlich ganz ohne Auflagen oder Erwartungen. Einfach so.
Die Idee einer virtuellen digitalen Patientenakte finden wir übrigens prima. Hatten wir auch schon.

Der Leiter des Facebook-finanzierten Instituts der Technischen Universität München hatte seine Kontakte zu dem Unternehmen übrigens als Mitglied internationaler Ethikkommissionen geknüpft[81], und hier schließt sich ein Kreis: Unter dem Personal des Facebook-finanzierten Instituts findet sich wiederum die Vorsitzende des Deutschen Ethikrats, Frau Professor Buyx als eine Projektleiterin eines – dann wohl auch von Facebook finanzierten – Forschungsprojekts („METHAD“), das mit Gründung des Instituts im Oktober 2019 startete[82]. Ziel des Gründungsprojektes ist die Entwicklung eines automatisierten medizinischen ethischen Ratgebers für Ärzte in der Patientenversorgung, basierend auf Methoden des maschinellen Lernens[83], also auf der Statistik fremder und eigener Entscheidungen in der Vergangenheit[84]

79 Man muss fairerweise sagen, dass die Fördermittel für Geisteswissenschaften oft geringer sind als z.B. die Fördertöpfe für naturwiasenschaftliche Themen. Aber das ließe sich ja vielleicht auch anders und aus neutralen Steuermitteln lösen, z.B. durch die bayrische Landesregierung; auch Geisteswissenschaftler/innen werfen für Fördergelder typischerweise nicht alle Skrupel über Bord.

80 „Spahn stellt Kooperation vor – Gesundheitsinfos prominent bei Google“. 10.11.2020, Tagesschau online (https://www.tagesschau.de/inland/google-bundesgesundheitsministerium-101.html, zuletzt abgerufen März 2021)

81 M. Hauck: „TU München verteidigt Kooperation mit Facebook“, 21.01.2019, Süddeutsche Zeitung

82 https://ieai.mcts.tum.de/research/methad-toward-a-medical-ethical-advisor-systtem.for.ethical-decisions, zuletzt abgerufen März 2021

83 Typischerweise unter dem publikumswirksamen Schlagwort „Künstliche Intelligenz“ gefasst, wobei aus meiner Sicht die Bezeichnung „Imitierte Intelligenz“ oder „Simulierte Intelligenz“ korrekter wäre.

Womit wir letzlich wieder beim Unternehmen Google wären, das als offizieller „Exzellenzpartner“ diskret eine Million Euro in das Stiftungsvermögen der Technischen Universität München steckt[85]. Aber das ist ja nun keine große Sache. Jedenfalls nicht für Google, für das der Betrag wohl allenfalls einen mikroskopischen Bruchteil der in Deutschland und Europa nicht gezahlten Steuern ausmacht. Aber dafür so sinnvoll und gezielt investiert. Natürlich ganz ohne Auflagen und Erwartungen. Einfach so.

Lassen Sie und an dieser Stelle die internationale „Spezlwirtschaft“ der Technischen Universtität München verlassen und uns wieder dem Unternehmen Google zuwenden. Das auf Profilerstellung spezialisierte Unternehmen „ist ja auch ein illustratives Beispiel für das Datenumfeld mit Blick auf Unternehmen, deren Kern und Geschäftsgrundlage die massenhafte Erstellung von Persönlichkeitsprofilen ist. Unternehmen, deren Interessen sich zunehmend auf den Bereich medizinischer Daten erstrecken. Lassen Sie uns einen näheren Blick darauf werfen.

Tatsächlich hat das Unternehmen einen eigenen Geschäftsbereich im Bereich Gesundheit, „*Google Health*“[86]. In der Vergangenheit hatte das Unternehmen bereits versucht, eine Art virtueller Patientenakte zur zentralen Speicherung medizinischer Daten einzuführen[87], wobei vorgesehen war, „*dass externe Dienstleister gegen Bezahlung Zugriff auf bestimmte Datensätze erhalten sollten*.“[88] Das Projekt wurde zum 1.1.2012 wieder eingestellt, da die Akzeptanz bzw. der Markt kein ausreichendes Volumen aufwiesen[89]. Dies ist durchaus konsistent mit den oben beschriebenen Erfahrungen der Techniker Krankenkasse, die mit einem ähnlichen Projekt ja ebenfalls auf ein minimales Interesse traf[90]. Die Situation hat sich in Deutschland jetzt jedoch infolge der Gesetzgebung insofern verändert, als der Gesetzgeber mit der Verpflichtung zur Einführung einer virtuellen Patientenakte künstlich einen Markt schafft und das Gesundheitsministerium faktisch für diesen wirbt. Es werden zudem die technischen Voraussetzung und Datenformate geschaffen, um virtuelle Patientenakten oder medizinische Datenbanken jeder Art - und jeden Anbieters - leicht füllen zu können.

Das Unternehmen Google seinerseits hat seit 2018 den Geschäftsbereich „Health“ umorganisiert und massiv „wiederbelebt“, unter anderem mit dem Ziel einer Verbesserung von Suchfunktionen in medizinischen Aufzeichnungen und virtuellen Patientenakten (*electronic health records*)[91] und der Erleichterung des Zugangs zu/Austauschs von Patientendaten durch Standardisierung - gemeinsam mit den Unternehmen Apple, Amazon und Microsoft[92]: „*2019 wurde angekündigt, dass [Google] die Anzahl von medizinischen Daten erhöhen wolle, die für Suchalgorithmen zugänglich sind [*searchable medical records*] und die ‚Qualität gesundheitsbasierter Suchergebnisse bei Google und Youtube erhöhen wolle‘. Google Health scheint sich auch auf die Erforschung Künstlicher Intelligenz mit Bezug auf den Gesundheitssektor, klinische Werkzeuge und Kooperationen für andere Instrumente und Dienstleistungen im Gesundheitssektor zu konzentrieren.*“[93] Damit im Einklang stehen

84 Wobei man sich fragen könnte, ob das aus philosophischer Sicht nicht von vornherein ein klassischer naturalistischer Fehlschluss ist, zumal aus meiner Sicht ethische Dilemmata gerade dadurch gekennzeichnet sind, dass es kein „Gewohnheitsrecht“ gibt und individuelle und fortschreitende Gewissensbildung erfordert, die einem autonomen Subjekt nicht abgenommen werden kann.

85 "Google investiert in Wissenschaft ‚Made in Germany‘“ (Pressemitteilung der TU München, 16.02.2018, https://www.tum.de/nc/die tum/aktuelles/pressemitteilungen/details/34489, zuletzt abgerufen 22.09.2020)

86 https://health.google/

87 https://de.wikipedia.org/wiki/Google_Health (zuletzt abgerufen 23.09.2020)

88 Ebd.

89 https://en.wikipedia.org/wiki/Google_Health (englischsprachiger Artikel und Referenzen darin, zuletzt abgerufen 23.09.2020)

90 s.o.

91 https://en.wikipedia.org/wiki/Google_Health

92 https://thenextweb.com/digital-life/2019/07/31/apple-google-and-microsoft-partner-to-provide-digital-access-to-patients-health-records/ (zuletzt abgerufen 23.09.2020)

93 https://en.wikipedia.org/wiki/Google_Health

Kooperationen des Unternehmens mit und massive Investitionen in Anbieter von Telemedizin (Amwell)[94], Firmen im Bereich Künstlicher Intelligenz (DeepMind) sowie auch im Bereich Fitness-Tracker/Activity-Tracker (FitBit), die mit einem Zugang zu deren personenbezogenen Datensätzen verbunden sind[95]. Datensätzen, die sich entweder direkt aus virtuellen Patientenakten speisen oder aus personenbezogenen Daten, die mithilfe von Fitnesstrackern generiert werden[96]. Das Unternehmen zielt also exakt auf die Daten, die der Gesetzgeber in einer virtuellen „elektronischen Patientenakte“ direkt oder indirekt über „durch den Versicherten zur Verfügung gestellten Gesundheitsdaten“ bereitstellen und miteinander verknüpfen will. Gleichzeitig ist das Unternehmen in den USA spätestens seit 2019 mit dem „Projekt Nightingale“[97] aktiv an der – zunächst nicht öffentlich gemachten - zentralen Speicherung und Auswertung der Daten von Millionen Patienten beteiligt, mit dem Ziel der Entwicklung von Google-basierten Funktionen in elektronischen Patientenakten[98]. Dabei geht es neben der Integration einer Google-Suchleiste auch um Methodenentwicklung für die inhaltliche medizinische Auswertung mit Methoden des Maschinellen Lernens (Imitierte Intelligenz). Tatsächlich gehen entsprechende Versuche noch weiter zurück. So veröffentlichte das Unternehmen bereits Anfang 2018 in der Fachzeitschrift „Digital Medicine“ Ergebnisse der automatisierten inhaltlichen Auswertung der individuellen medizinischen Datensätze von rund 216.000 Patienten; wobei das Modell für jeden Patienten Zugang zu „Zehntausenden von Prädiktoren“ hatte[99]. Darunter Freitext-Einträge der behandelnden Ärzte, demographische Angaben (Alter, Geschlcht etc.), Diagnosen, Therapien, Medikationen, Laborwerte[100]...also praktisch alle Inhalte eine elektronischen Patientenakte. Insgesamt hatte das Unternehmen Google dabei offenbar Zugriff auf alle Patientendaten der Universitätskliniken in San Francisco und Chicago aus dem Zeitraum 2021-2016 bzw. 2009 bis 2016, Die betroffenen Patienten, deren persönliche medizinische Daten dem Unternehmen Google zugänglich gemacht wurden, wurden hier allerdings ebensowenig informiert, wie beim „Projekt Nightingale“. Nach US-Recht ist das juristisch erlaubt, wenn die Daten zuvor pseudonymisiert („*de-identified*“) werden. Wir kommen auf die trügerische Sicherheit von Pseudonymisierung und Anonymisierung im Informationszeitalter noch zurück. In diesem konkreten Fall gab es ein besonderes Problem, das vor Gericht führte: Die Datensätze aus Chicago enthielten das Behandlungsdatum, so dass das Unternehmen Google sie „*mit anderen Informationen kombinieren konnte, über die es bereits verfügte, wie zum Beispiel den Standortdaten von Handys mit Google Android Betriebssystem, Google Maps oder dem Google Routenplaner Waze,*“[101] und so zumindest im Prinzip die Datensätze wieder persönlich zuordnen konnte.

Um es klar zu sagen: Es geht hier nicht um vermeintliche „finstere Absichten“ des Unternehmens oder Ähnliches, die Absichten und Wünsche können so rein sein wie ein Gebirgsbach oder das Herz von Facebook-Chef Mark Zuckerberg.

94 „Google Cloud Invests $100 Million in Amwell and Announces New Cloud Partnership“, HealthCare IT TODAY, Meldung vom 24.08.2020 (https://www.healthcareittoday.com/2020/08/24/google-cloud-invests-100-million-in-amwell-and-announces-new-cloud-partnership/, zuletzt abgerufen 23.09.2020)

95 Thomas Macaulay: „What will Google’s healthcare expansion mean for UK data protection?“, Computerworld, 10.01.2020 (https://www.computerworld.com/article/3558678/what-will-google-s-healthcare-expansion-mean-for-uk-data-protection.html, zuletzt abgerufen 23.09.2020)

96 Ebd.

97 E. Pilkington: „Google‘s secret cache of medical data includes names and full details of millions – whistleblower“, 12.11.2019, The Guardian

98 N. Singer/D. Wakabyashi: „Google to store and analyze millions of health records“, 11.09.2019, The New York Times (https://ww.nytimes.com/2019/11/11/business/google-ascension-health-data.html, zuletzt abgerufen April 2021)

99 A. Rajkomar et al.: „Scalable and accurate deep learning with electronic health records“. npj Digital Medicine, 18, S. 1ff. (2018).

100 Ebd.

101 D. Wakabayashi: „Google and the University of Chicago are sued over data sharing“, 26.6.2019, The New York Times

Es geht halt nicht um Absicht und Wunsch sondern um Wirklichkeit. Und das Problem ist aus meiner Sicht ganz nüchtern - ähnlich wie im eingangs zitierten „Volkszählungsurteil“ - die immer stärkere, ungesunde Machtkonzentration als zwangsläufige Folge einer immer umfassenderen und vollständigeren Datensammlung, die ebenso zwangsläufig mit einer immer stärkeren Abhängigkeit der betroffenen Menschen und ganzer Gesellschaften und Staaten einhergeht.

Zum Beispiel der Abhängigkeit, dass die Daten niemals gegen Ihre Interessen verwendet werden, dass die Überzeugungen und Interessen des Unternehmens sich mit Ihren decken, dass nichts schief geht, dass die Daten nicht manipulativ verwendet werden, um Ihre Überzeugungen und Interessen zu ändern, dass die Daten sich nicht weiterverbreiten, dass Daten nicht verändert werden, dass das Unternehmen ehrlich ist, dass Dritte es nicht hacken oder anderweitig Zugriff erlangen, dass auch alle Einzelpersonen im Unternehmen integer sind und in Ihrem Interesse und entsprechend Ihrer Überzeugungen handeln…würden Sie das alles unterschreiben?

Ich nicht.

Mit anderen Worten: Das Ganze ist ein immer weiter um sich greifendes Hochrisikosystem, das logisch zur Unmündigkeit der Bürgerinnen und Bürger führt, die wie im 18. Jahrhundert auf einen gütigen Landesvater hoffen und ihm bedingungslos vertrauen müssen. Zum Beispiel darauf, dass er sie nicht wie weiland Landgraf von Hessen-Kassel verkauft, um seine Kasse aufzubessern. Und ehrlich gesagt: Dass das Unternehmen mit den USA in einem Land beheimatet ist, dass datenschutzmäßig Entwicklungsland ist und den Ländern der Europäischen Union um Jahrzehnte hinterherhinkt, macht es nicht gerade besser.

Was bedeutet das für medizinischen Daten? Ein auf die massenhafte Erstellung von Persönlichkeitsprofilen spezialisiertes Unternehmen hat - über eigene Subunternehmen oder die seines Mutterkonzerns oder Anwendungen aus dem „Google Playstore“ - auch in Deutschland direkten Zugriff auf personenbezogene Gesundheitsdaten beispielsweise via Fitness-Apps oder Fitness-Trackern und auf Diagnosen anhand der Zielgruppe der jeweiligen App.

Bei eigenen Apps kann es hier auch eigene Identifikatoren setzen. Diese Daten können gegebenenfalls als „zusätzliche Inhalte“ in die virtuelle Patientenakte aufgenommen werden (§ 345 SGB V)[102]. Sobald die Inhalte der virtuellen Patientenakte über das Forschungszentrum „gespendet“ werden, kann das Unternehmen über Forschungskooperationen wiederum auf dieselben Daten zugreifen, wobei sie diesmal potentiell mit allen anderen medizinischen Daten des Versicherten verknüpft sind.

Die Daten sind dann zwar „anonymisiert“. Aber die Deanonymisierung von Daten, die man entweder selbst zuvor mit Identifikatoren oder digitalen Wasserzeichen versehen hat[103] oder die einem zum Teil bereits „im Klartext“ vorliegen, dürfte eine leichte Übung sein. Sofern sich die eigenen Anwendungen nicht ohnehin schon direkt aus der virtuellen Patientenakte „bedienen“, wie im obigen Zitat ausgeführt. Tatsächlich reicht es schon, wenn Fitness- und Gesundheits-Apps die Messwerte auf einen Firmenserver des Anbieters speichern und verarbeiten. Praktisch jede Zeitserie von Messdaten von Körperfunktionen dürfte ebenso eindeutig zuzuordnen zu sein wie ein Fingerabdruck.

---

102 Vgl. a. „Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur digitalen Modernisierung von Versorgung und Pflege“ (Januar 2021), z.B. S. 3

103 z.B. in Form von Pseudozufallszahlen im „Rauschen“ der Messwerte; beispielsweise können Werte für die Herzfrequenz, die ganzzahlig angezeigt werden, in einem Datenformat abgespeichert werden, dass Nachkommastellen umfasst, in denen sich dann „im Rauschen“ leicht eine identifizierende Zahlenkombination unterbringen ließe.

Hinzu kommt, dass das Unternehmen „auf Nummer sicher gehen“ und die Versicherten direkt auffordern kann, die Inhalte ihrer virtuellen „elektronischen Patientenakte“, die ja praktischerweise bereits einheitlich formatiert, digitalisiert, zentral gesammelt und „fertig zum Abholen“ vorliegen, herunterzuladen, sofern diese Möglichkeit besteht. Und sie idealerweise selbst mit anderen Datensätzen zu verknüpfen und beispielsweise in einer „Google Health Cloud“ abzulegen. Dies „schmackhaft“ gemacht mit dem Versprechen, dort von besonderen Algorithmen oder Rechenkapazitäten oder auch einer direkten Verknüpfung mit Google Android Smartphones zu „profitieren“.

Technisch ist alles bereit. In ähnlicher Weise bietet das Unternehmen dies ja bereits an für möglichst alle Fotos, die Smartphone-Nutzer machen, als „Google Photos“-App: „*Kostenloser Speicherplatz mit automatischer Sortierung für alle Deine Erinnerungen*“[104] Fotos, die auch gerne mit genauen Standortinformationen versehen und durch den Nutzer selbst mit den Bildern anderer Nutzer verknüpft werden können: „*Erstelle geteilte Alben, die auch deine Freunde und Familienmitglieder mitgestalten können. So entgeht dir nie wieder, wenn jemand etwas hinzufügt, ganz egal über welches Gerät.*“[105] und mittels Algorithmen zur automatisierten Erfassung von Bildinhalten für Suchalgorithmen zugänglich sind: „*Deine Fotos werden geordnet und können nach Orten und Inhalten durchsucht werden – Taggen ist nicht nötig. Wenn Du Dir beispielsweise die Fotos deines süßen Hundes ansehen möchtest, suche einfach nach ‚Hund‘*“[106].
Sie denken sich vielleicht: OK, gut zu wissen, dann gebe ich meine Diagnosen nicht mehr bei Googles Suchmaschine ein und verwende auch keine FitBit-Apps und -Tracker. Und um ganz sicherzugehen benutze ich nur noch die „Digitalen Gesundheitsanwendungen“, die vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) geprüft und zugelassen sind[107].

Das können Sie machen, eine gute Idee. Sie leiden unter Sozialen Phobien oder eine Panikstörung? Dann laden Sie sich einfach die zugelassene Anwendung „Invirto“ aus dem Google Play Store herunter, nachdem Sie sich mit Ihrem Google Konto angemeldet haben. Oder leiden Sie an einer Depression? Prima, laden Sie sich die zugelassene Anwendung „Selfapy“ aus dem Google Play Store herunter. Ach so, Sie leiden an Schlaflosigkeit? Kein Problem, dann laden Sie sich doch einfach die zugelassene Anwendung „somnio“ aus dem Google Play Store herunter auf Ihr Smartphone mit Google Android Betriebssystem.

Oder schreiben Sie einfach direkt eine E-Mail mit Ihrer Diagnose an Google (alternativ Apple). Das kommt auf das Gleiche heraus.

Sollte es wirklich die Absicht des Gesetzgebers gewesen sein, die Datenautonomie und den Datenschutz der Versicherten zu schützen und zu stärken, bewirkt er tatsächlich das Gegenteil. Sollte es sein Ziel sein, Unternehmen wie Google „in die Schranken zu weisen“ oder ihnen „Konkurrenz“ zu machen, verfehlt er es vollständig – die Unternehmen hätten sich wohl keine bessere gesetzliche Begleitung und Unterstützung seiner weiteren, auf immer umfassendere Datenerfassung und Profilerstellung zielende Geschäftsentwicklung wünschen können.

Tatsächlich kann man sich des Eindrucks nicht erwehren, dass sich zwischen dem Bundesministerium für Gesundheit und der Unternehmen Google der Beginn einer symbiotischen Beziehung anbahnt, in der eine Hand die andere wäscht. Wobei es manchmal schwierig ist, zuzuordnen, welche Hand zu wem gehört.

So verkündete der Bundesgesundheitsminister Ende 2020 überraschend eine Kooperation des Ministeriums mit dem Konzern – und nur mit diesem – in deren Rahmen Inhalte des Nationalen Gesundheitsportals von Google bei medizinischen Suchanfragen hervorgehoben

104 https://www.google.com/intl/de/photos/about/
105 Ebd.
106 Ebd.
107 https://diga.bfarm.de

als exklusives „Knowledge Panel“ auf der Ergebnisseite präsentiert werden[108]. Dabei würden „die üblichen Datenschutzstandards von Google gelten“[109] Also einfach nur ein netter Gefallen im Schatten der Pandemie.

Allerdings regte sich schnell Widerspruch von Medienvertretern und von Betreibern privater Gesundheitsportale, die das Vorgehen als unzulässigen staatlichen Eingriff in die Medienlandschaft kritisierten[110], und schließlich bei Gericht Klage einreichten, der im Wesentlichen stattgegeben wurde[111]. Interessant ist der weitere Verlauf.

Insgesamt wurden vier Klagen bzw. Anträge gegen die Kooperation eingereicht[112]. Zum einen eine Klage generell gegen das Nationale Gesundheitsportal, die zurückgezogen wurde. Zum Zweiten eine Klage direkt gegen Google wegen marktmissbräuchlichen Verhaltens, die abgewiesen wurde. Stattgegeben wurde dagegen einer Doppelklage gegen das Bundesgesundheitsministerium und das Unternehmen Google, die auf die Benachteiligung kommerzieller Gesundheitsportale mit der Folge einer Einschränkung des Wettbewerbs und der Medien- und Meinungsvielfalt verwies, da die werbefinanzierten Portale mit substantiellen Einnahmeverlusten und Finanzierungsproblemen rechnen müssten.

Nun würde man denken, dass für das werbefinanzierte Unternehmen Google gerade dieser letzte Punkt selbst einleuchtend und von Interesse und es ihm zudem egal ist, auf welches Gesundheitsportal es zurückgreift, solange es seriös ist. Während dagegen das Bundesgesundheitsministerium mit seinem Projekt des Nationalen Gesundheitsportals guten Grund hätte, gegen das Urteil vorzugehen. Interessanterweise geschah genau das Gegenteil: Das Unternehmen Google legte Berufung ein[113] und handelte damit scheinbar im Interesse des Bundesgesundheitsministeriums. Warum eigentlich? Ein netter Gefallen, damit es sich nicht „die Hände schmutzig“ machen musste, einfach so? Oder handelte das Bundesgesundheitministerium zuvor – bewusst oder unbewusst - im Interesse des Unternehmens? Das das strategische Ziel verfolgt, in den Bereich „Medizinische Daten und Gesundheitswesen“ zu expandieren, und dafür als ersten, einfachen Schritt eine Qualitätssicherung seiner medizinischen Suchergebnisse anstrebt, bevor es dann übergeht zur Implementierung von Google Suchfunktionen in virtuellen Patientenakten und digitalen Gesundheitsanwendungen[114]. Allerdings braucht es dafür Vertrauen, und dafür eignet sich – ähnlich wie im Fall von Facebook und der Technischen Universität München – eine öffentliche, als neutral wahrgenommene Stelle natürlich besser als ein kommerzieller Anbieter (der zudem potentieller Konkurrent ist). Wer hier wem wann einen Gefallen tut – das finde ich so schwer zu durchschauen wie die Quelle des steten Stroms von Gesetzes- und Referentenentwürfen aus dem Bundesministerium für Gesundheit. Es ist aber sicher eines genaueren Blickes wert. In jedem Fall scheint gegenseitige Zurückhaltung nicht das Problem zu sein.

108 „Kooprerstion mit Ministerium – Dr. Google wird akkurater“, 10.11.2021, Frankfurter Allgemeine Zeitung (https://www.faz.net/aktuell/wirtschaft/digitec/durch-gesundheitsministerium-dr-google-wird-akkurater-17045468.html)

109 „Spahn stellt Kooperation vor – Gesundheitsinfos prominent bei Google“, 10.11.2020, tagesschau online (https://www.tagesschau.de/inland/google-bundesgesundheitsministerium-101.html)

110 M. Hanfeld: „Spahns Pakt mit dem Digitalkonzern – Fragen Sie Dr. Google!“, 12.11.2020, Frankfurter Allgemeine Zeitung (https://www.faz.net/aktuell/feuilleton/jens-spahns-pakt-mit-dem-digital-konzern-google-17047684.html)

111 „Kooperation zwischen Spahn-Ministerium und Google untersagt“, 10.02.2021, dpa/Süddeutsche Zeitung (https://www.sueddeutsche.de/politik/bundesregierung-kooperation-zwischen-spahn-ministerium-und-google-untersagt-dpa.urn-newsml-dpa-com-20090101-210210-99-382266)

112 Pressemitteilung 06 des Landgerichts München I vom 10.02.2021: „Netdoktor gegen BRD und Google: Vereinbarung über Knowledge Panels kartellrechtswidrig“

113 „Google geht rechtlich gegen Urteil zu Gesundheitsportal des Bundes vor“, 17.03.2021, ärzteblatt.de (https://www.aerzteblatt.de/nachrichten/122125/Google-geht-rechtlich-gegen-Urteil-zu-Gesundheitsportal-des-Bundes-vor)

114 B. Frist: „Googllng our way to better health: insights from my conversation with Dr. David Feinberg“, 11.03.2021, Forbes (https://www.forbes.com/sites/billfrist/2021/03/11/googling-our-way-to-better-health-insights-from-my-conversation-with-dr-david-feinberg/)

Das Unternehmen Google ist übrigens nicht der einzige große Tech-Konzern, der ein kommerzielles Interesse an medizinischen Daten entwickelt. So übernahm das Unternehmen Microsoft Anfang 2021 die Firma „Nuance Communications“[115], die sich sich auf Simulierte Intelligenz und Cloud Computing spezialisiert hat, insbesondere auch im Gesundheitssektor. Die beiden Unternehmen kooperierten bereits seit Ende 2019 mit dem Ziel „ambient clinical intelligence“ in das Arzt-Patientengespräch zu bringen, d.h. die automatische Erfassung und Verarbeitung des Patientengesprächs mit Methoden des Maschinellen Lernens und die Anbindung an elektronische Patientenakten[116], wobei das Unternehmen Nuance seine Produkte in die Microsoft-Cloud verschoben habe.
Ein interessantes Detail dabei ist die Kaufsumme von gut 16 Milliarden Euro, was nur etwas über dem Quartalsgewinn des Google-Mutterkonzerns Alphabet liegt[117] oder dem 390-fachen der Investitionsmittel des Bundesgesundheitsministeriums im Jahr 2019 bzw. dem Gesamthaushalt des Gesundheits- oder des Bundesministeriums für Bildung und Forschung in dem Jahr entspricht. Dies weist darauf hin, dass die Hoffnung, ein deutsches Start-up könne auf diesem Mark nicht nur bestehen sondern ihn „aufrollen“ oder das Gesundheitsministerium durch Wirtschaftsförderung die Spielregeln festlegen die Wahrscheinlichkeit nicht auf oihrer Seite hat. Realistischer ist, dass die Spielregeln des Marktes auf absehbare Zeit von den finanzstarken Quasi-Monopolisten und „Platzhirschen“ festgelegt werden. Selbst wirtschaftlich sinnvoller wäre es also vielleicht, durch Technologie-Entwicklung einen neuen Markt zu eröffnen, z.B. mit einem Kartenchip mit mehr Speicherplatz für eine elektronische Patientenakte in der Hand des Patienten.

Unternehmen und Drittstaaten

Es ist nun mit Blick auf das Anhäufen personenbezogener medizinischer Daten kein Trost, wollte man behaupten, es sei ja alles unproblematisch, solange es „nur“ Unternehmen sind und nicht etwa autoritäre Staaten mit einer gegen die freiheitliche Demokratie gerichtete Agenda.
Zum Einen ist die Barriere zwischen Staat und Wirtschaft je nach Land mehr als durchlässig[118] oder praktisch nicht existent. So ist laut Verfassungsschutzbericht „w*egen der engen Verflechtung von Staat und Wirtschaft in China [...] es im Einzelfall kaum möglich, zwischen staatlich betriebener Wirtschaftsspionage und Ausspähung durch konkurrierende Unternehmen zu unterscheiden.“*[119] Dem pflichtet das Lagebild 2021 des estnischen Auslandsnachrichtendienstes bei, der am Beispiel des Unternehmens „Huawei“ bemerkt: „*Die Kommunistische Partei Chinas und chinesische Privatunternehmen sind oft direkt oder indirekt miteinander verbunden.*“[120]
Zum Anderen können aber auch einzelne Unternehmer oder Wirtschaftsakteure eine Agenda vertreten, deren Konformität mit einer freiheitlich-demokratischen Grundordnung mehr als fraglich ist[121]. Generell ist die Machtkonzentration von Datenverwertern hochproblematisch, wie das Erpressungspotential von Firmen wie Facebook und Google zeigt, das sie angesichts

115 „Microsoft kauft KI-Unternehmen Nuance“, tagesschau online, 12.04.2021 (https://www.tagesschau.de/wirtschaft/microsoft-nuance-101.html, zuletzt abgerufen April 2021)
116 F. Lück: „Microsoft und Nuance kooperieren im Helthcare-Geschäft“, 17.10.2019, mednic (https://mednic.de/microsoft-und-nuance-kooperieren-im-healthcare-geschaeft, zuletzt abgerufen April 2021)
117 „Google-Mutter Alphabet steigert Quartalsgewinn um 43 Prozent“, Redaktionsnetzwerk Deutschland, 03.02.2021
118 Zu den USA vgl. z.B. die früher vorgetragenen Ausführungen Edward Snowdens oder auch das EuGH Urteil vom 16.07.2020 zum „Privacy Shield“-Abkommen.
119 Bundesministerium des Innern, für Bau und Heimat: „Verfassungsschutzbericht 2019“, S. 294.
120 Lagebild 2021 des estnischen Auslandsnachrichtendienstes Välisluureamet: „International Security and Estonia 2021“ (2021), S. 77
121 Vgl. z.B. die Rolle des Robert Mercers bei der Gründung von SCL/Cambridge Analytica und als Unterstützer von Stephen Bannon oder die Rolle Henning Conles im Rahmen der verschleierten Finanzierung der Partei „Alternative für Deutschland“ im Bundestagswahlkampf 2017 (z.B. https://www.tagesschau.de/investigativ/report-mainz/afd-spenden-127.html, zuletzt abgerufen 26.09.2020)

unliebsamer Gesetzgebung in Australien versuchten auszuspielen[122][123]. Auch hochproblematische personellen Verquickungen wie die oben genannte zeigen[124], dass Datenverwerter wohl keine Hemmungen vor der Schaffung von Abhängigkeiten und politischer Einflussnahme haben, deren Grenze sie selbst nach eigenem Gutdünken definieren wollen. Deren Wohlwollen und Absichten sollte der Staat sich und seine Bürger nicht ausliefern. Ein weiteren pikanten Hinweis darauf liefert der Umstand, dass Unternehmen wie Google und Amazon ohne Bedenken durch Transferzahlungen und das „Anmieten" von Flächen zur Platzierung von Online-Werbung faktisch auch solche Websites finanzieren, die massiv politische Desinformation verbreiten[125].

Mit anderen Worten: Der Gesetzgeber kann hier nicht nach dem „Prinzip Hoffnung" ein Vabanque-Spiel betreiben. Der Schutz der Grundrechte kann keine Unterscheidung machen zwischen der Bedrohung durch staatliche oder wirtschaftliche Akteure.

Deanonymisierung, Depseudonymisierung, Proliferation

Es ist ja auch völlig unklar, wie eine unkontrollierte Verbreitung und Proliferation der anonymisierten Daten und ihre Nutzung zur Erstellung oder Verfeinerung von Persönlichkeitsprofilen in der Realität tatsächlich verhindert werden kann. Wobei dies ja außer durch Unternehmen mit primär kommerziellen Interessenten auch direkt durch nachrichtendienstlich geführte „menschliche Quellen" aus dem Wissenschaftsbereich[126] als Zulieferer möglich ist. Der „Datenspender" selbst hat hier keine Einflussmöglichkeit mehr.

Der Gesetzgeber versucht nun, Missbrauch vorzubeugen[127], indem beispielsweise die Nutzung zur Deanonymisierung/Depseudonymisierung („Herstellung eines Personenbezugs") untersagt wird. Zudem seien Daten nur für die Zwecke zu verwenden, für die sie zugänglich gemacht worden seien.

Doch hier ergibt sich, abgesehen von der Frage nach einer Datenproliferation, sofort die Frage nach der Nachweisbarkeit eines Verstoßes und danach, ob das Verbot im Licht der aktuellen Gesetzgebung mehr als ein „frommer Wunsch" ist. Auch der Frage nach der tatsächlichen Anonymität anonymisierter medizinischer Daten muss sich der Gesetzgeber stellen.

Wie unten ausgeführt, erfordert die Katalogisierung von Persönlichkeitstypen und selbst die Erstellung von Persönlichkeitsprofilen nicht notwendigerweise einen expliziten Personenbezug im Sinne der De-Pseudonymisierung oder De-Anonymisierung durch Kenntnis von z.B. Name und Adresse des Betreffenden.

Das Unternehmen „Google" würde beispielsweise argumentieren, das es ja nie über eine Pseudonymisierung mithilfe von Identifikatoren hinausgehe - denn mehr ist für eine selbst massenhafte Profilerstellung zur Katalogisierung von Persönlichkeitstypen und der Einteilung des Betreffenden zur weiteren Verwendung ja auch nicht erforderlich. Wie weiter unten ausgeführt, ist es auch für die Manipulation demokratischer Prozesse völlig ausreichend, wenn bestimmte „Persönlichkeitstypen" kohärent identifiziert und adressiert werden können. Es ist nicht erforderlich zu wissen, welche konkreten Personen sich in der entsprechenden

122 Deutsche Welle: „Google droht Australien mit leeren Bildschirmen" (22.01.2021, https://www.dw.com/de/google-droht-australien-mit-leerem-bildschirm/a-56309021 , zuletzt abgerufen Februar 2021)

123 Deutsche Welle: „Facebook schränkt Nutzung in Australien ein" (18.02.2021, https://www.dw.com/de/facebook-schr%C3%A4nkt-nutzung-in-australien-ein/a-56606433 , zuletzt abgerufen Februar 2021)

124 J. Kliss: „Vom Kanzleramt zu Facebook", Tagesschau Online vom 24.02.2021 (https://www.tagesschau.de/inland/innenpolitik/facebook-wechsel-reuss-101.html)

125 Vgl. z.B. https://disinformationindex.org oder auch „the mondetization of disinformation through Amazon: La verdadera Izquierda", Bericht veröffentlicht auf (veröffentlicht auf https://www.disinfo.eu)

126 Siehe z.B. Bundesministerium des Innern, für Bau und Heimat: „Verfassungsschutzbericht 2019", S. 293ff.

127 § 303e SGB V

„Schublade“ der Katalogisierung befinden, solange sie nur kohärent eingeordnet und adressiert werden können.

Selbst wenn man argumentieren wollte, dass auch die Erstellung von solchen „pseudonymen“ oder „statistischen“ Persönlichkeitsprofilen durch die gesetzlichen Regelungen (§ 303e SGB V) bereits untersagt sei, stellt sich sofort die Frage, wie und ob dieses Verbot auch tatsächlich durchgesetzt werden kann oder eben lediglich ein „frommer Wunsch“ bleibe. Sanktionen wie ein vorübergehender Ausschluss vom Zugang zu den am Forschungsdatenzentrum gespeicherten Daten sind ein stumpfes Instrument, insbesondere gegenüber breit aufgestellten wirtschaftlichen Unternehmen oder gar Akteuren aus dem Bereich geheimdienstlicher Tätigkeit oder auch der organisierten Kriminalität.

Die Aufhebung von Anonymisierung ist zudem durch die Kombination von Daten aus verschiedenen Quellen möglich. Bereits im Jahr 2017 konnten Forscher der Universität Melbourne zeigen, dass personenbezogene medizinische Daten von 2,9 Millionen Menschen, die im Jahr zuvor von der australischen Regierung anonymisiert veröffentlicht worden waren, durch Kombination mit Daten aus anderen, öffentlich zugänglichen Quellen de-anonymisiert werden konnten[128]. Als die Daten daraufhin zurückgezogen wurden, waren sie bereits über 1500mal heruntergeladen worden. Für Deutschland wurde in demselben Jahr die Deanonymisierung von Internetnutzern anhand - kommerziell erhältlicher - Historien von besuchten Seiten im Internet („clickstreams“) demonstriert[129]. Hierzu konnten die Forscher, getarnt als Marketing-Firma, die Internethistorie von drei Millionen deutschen Nutzern kommerziell erwerben und auswerten. Diese Daten können ebenso mit anonymisierten medizinischen Daten kombiniert werden, z.B. über Gerätekennungen, um diese zu de-anonymisieren.

Da medizinische Daten untrennbar und dauerhaft mit der betreffenden Person verbunden sind, ist der Schaden eines kriminellen Zugriffs und irregulären Datenabflusses schon nach dem ersten Mal nicht mehr zu heilen.

Na gut, aber im Ernst - wie sieht die Realität des informationellen Kontexts mit Blick auf die Organisierte Datenkriminalität aus? Ist das überhaupt ein signifikantes Problem?

Datenumfeld: Organisierte Kriminalität

Das ist der Fall.

Bezüglich der Gefahrenlage durch Datenkriminalität als Teilbereich der organisierten Kriminalität spricht das Bundeslagebild „Cybercrime 2019“ des Bundeskriminalamtes eine deutliche Sprache. Das BKA beziffert dort allein für das Jahr 2019 die Zahl neuer Malware-Varianten auf mehr als 100.000.000 (hundert Millionen)[130]. Für den Bereich von auf mobile Endgeräte spezialisierten Schadprogrammen - die also spezifisch sind für Geräte, mit denen nach dem Willen des Gesetzgebers auf die virtuelle „elektronische Patientenakte“ zugegriffen werden kann - wird allein die Anzahl *neuer* Sorten von Schadprogrammen für das eine Jahr auf mehr als vier Millionen beziffert[131]. Offensichtlich sind die kriminellen Aktivitäten hier hoch signifikant, und sie wuchsen im Jahr 2020 weiter[132] Kritische Selbstreflexion der Strategen im Bundesgesundheitsministerium? Leider Fehlanzeige.

128 Olivia Solon: „‘Data is a fingerprint‘: why you aren‘t as anonymous as you think online“, The Guardian, 13.07.2018 (online unter: https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy , zuletzt abgerufen 06.03.2020).

129 Alex Hern: „‘Anonymous‘ browsing data can be easily exposed, researchers reveal“, The Guardian, 01.08.2017 (https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers , zuletzt abgerufen 06.03.2020).

130 „Cybercrime – Bundeslagebild 2019“, Bundeskriminalamt , Wiesbaden (2020), S. 13

131 Ebd., S. 15, wobei das BKA selbst von einer hohen Dunkelziffer ausgeht.

132 „Cybercrime – Bundeslagebild 2020“, Bundeskriminalamt , Wiesbaden (2021), S. 10, 19

Der Bundesgesundheitsminister bzw. sein Ministerium treiben das Spiel munter weiter und fordern mit dem Entwurf des „Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz“ von den Krankenkassen ultimativ, eine „sichere“ digitale Identität einzuführen, also eine Art Benutzerkonto, mit der alleine sich Versicherte im Gesundheitssystem bewegen und für alle Zwecke online ihre Berechtigungen und Zugriffsrechte nachweisen können. Das Bundeslagebild „Cybercrime 2020“ des Bundeskriminalamtes führt Digitale Identitäten im Rahmen der Schattenwirtschaft organisierter Kriminalität als „*Beliebte Handelsware*“ auf und berichtet von 10000000000...12000000000 digitalen Identitäten/Benutzerkonten, die zu dem Zeitpunkt als gehackt bekannt waren[133]. Man muss kein Hellseher sein, um vorherzusagen, dass digitale Identitäten, die Zugang zu personenbezogenen medizinischen Daten erlauben, eine noch sehr viel stärker beliebte Handelsware sein werden als Benutzerkonten bei Internethändlern o.ä.. Sollte das Bundesgesundheitsministerium mit seinem Gesetzesvorhaben „Erfolg“ haben, wird es damit vor allem eine neue Angriffsfläche für das Hacken der zentral gespeicherten medizinischen Daten schaffen.

Forschungs-datenbank: Eigenverant-wortung oder pauschale Da-tenpreisgabe?

Jenseits der strafrechtlich relevanten Organisierten Kriminalität stellt sich aber auch die Frage, inwieweit nicht beispielsweise ein Forschungszweck, der auf die Entwicklung von Algorithmen für die Zurverfügungstellung individualisierter, „individuell geeigneter“ Leistungen und Innovationen abzielt (vgl. § 68b SGB V), gerade dazu dienen kann, unter dem Hinweis auf die Priorität von Forschungszwecken das Verbot zur Herstellung eines Personenbezugs zu umgehen. Ein solches Forschungsvorhaben hätte ja gerade zum Ziel, anhand der Daten die Möglichkeit zur Profilerstellung zu untersuchen und zu implementieren.

Die Forschungszwecke nach § 363 Abs. 1 SGB V, also z.B. die „Verbesserung der Qualität der Versorgung“, sind zudem - notwendigerweise - sehr weitgefasste Zwecke. Sie lassen zum Zeitpunkt der Datenpreisgabe durch den Versicherten keinen Rückschluss auf die tatsächlichen, konkreten Inhalte und Motivationen oder gar die Durchführenden der Forschungsvorhaben zu, für die die Daten später verwendet werden.

Anders als bei der Teilnahme an wissenschaftlichen, medizinischen Studien üblich findet damit auch keine individuelle Aufklärung des Versicherten mehr über Inhalte, Ablauf und Ziele der einzelnen Forschungsvorhaben statt, zu denen er mit der Preisgabe seiner persönlichen medizinischen Daten beiträgt. Der Versicherte stellt dagegen dem Forschungsdatenzentrum einen pauschalen „Blanko-Scheck“ zur Verwendung seiner persönlichsten, eigentlich untrennbar mit ihm verbundenen Daten aus.

Indem der Gesetzgeber diese Möglichkeit zulässt, ermöglicht er eine Art „massenhafter Selbst-Entmündigung“ von Versicherten hinsichtlich ihrer persönlichen medizinischen Daten. Dies widerspricht aber grundsätzlich dem Prinzip einer freiheitlichen, demokratisch organisierten Gesellschaft mit dem mündigen Bürger als Subjekt seiner bewussten Handlungen: Mit der Freiheit des Einzelnen (zu handeln) geht zwingend auch die Verantwortung des Einzelnen (für die Konsequenzen seines Handelns) einher.

Diese Verbindung kann der Gesetzgeber nicht per Gesetz lösen. Schon gar nicht, ohne gegen die Grundprinzipien einer freiheitlichen Gesellschaft zu verstoßen. Dies ist ebenso undenkbar, wie der Gesetzgeber beispielsweise die Möglichkeit einführen könnte, freiwillig das persönliche Wahlrecht an ein „Wahlstimmenzentrum“ abzugeben, damit es die Stimmen der Wählerinnen und Wähler zentral verwaltet und sie – vielleicht in noch so gut gemeinter Absicht – zentral auf Parteien verteilt und bei Abstimmungen einsetzt.

Die persönliche Verantwortung für sein Handeln und dessen Folgen kann der mündige Bürger jedoch nicht delegieren. Damit der Einzelne die Verantwortung für die Nutzung seiner personenbezogenen Daten wahrnehmen kann, muss ihm aber der konkrete Verwendungszweck seiner Daten jeweils bekannt sein[134].

133 Ebd., S. 20

134 Vgl. hierzu Absatz 8 des neuen § 363 SGB V.

Es wäre vielleicht denkbar, dass das Forschungsdatenzentrum eine Art Aufsichtsfunktion wahrnimmt, indem es eine „Zertifizierung“ von Forschungsvorhaben unterstützt und kontrolliert, dass es zu keinem Zeitpunkt zu einer kritischen Datenakkumulation kommt. Eine bundesweite zentrale, umfassende und inhaltlich wie zeitlich grundsätzlich unbegrenzte Vorratsdatenbank personenbezogener medizinischer Daten ohne konkreten Anlass ist dagegen völlig unverhältnismäßig.

Sie stellt zudem erneut ein naheliegendes und höchst lohnenswertes Ziel für hochprofessionelle Versuchen einer irregulären Datenaneignung zum Schaden der freiheitlich-demokratischen Grundordnung dar.

Maschinelles Lernen, Datensätze, wissenschaftliche Forschung

Hier könnte man kritisch einwenden, ob denn nicht beispielsweise die Entwicklung medizinischer Software zur automatisierten Anwendung von Erfahrungswissen („Künstliche Intelligenz“/“Deep Learning“/“Künstliche Neuronale Netze“[135]) nun einmal notwendigerweise einen möglichst umfassenden und großen Datensatz voraussetzten?

Dies ist nicht der Fall.

Im Bereich Data Science hat man traditionell gezwungenermaßen mit unspezifischen Datensätzen oder deren Zusammenführung gearbeitet, die in anderen Zusammenhängen oder als Nebenprodukt angefallen sind, z.B. als Metadaten. Hier musste man dann automatisiert nach potentiell interessanten Zusammenhängen oder relevanten Daten „schürfen“ (*data mining*) und dafür insbesondere die Daten zuvor noch aufbereiten.

Daraus den Umkehrschluss zu ziehen, wissenschaftliche Data Science Projekte würden zwingend unspezifische, beliebig große Datensätze erfordern, die daher „ohne Rücksicht auf Verluste“ zu erzeugen und vorzuhalten seien, ist ein Fehlschluss. Im Gegenteil stellt die fehlende Spezifität von Datensätzen in Data Science-Projekten oft eher ein lästiges Problem dar, da so ein wesentlicher und mühseliger Teil der Arbeit, oft der größte Teil, in einer nachträglichen Anpassung und Aufbereitung von für die Aufgabe eigentlich „ungeeigneten“, unspezifischen Datensätzen besteht.

Dabei ist es auch im Bereich medizinischer informationeller Forschung im Rahmen echter wissenschaftlicher Arbeit wichtig und zumutbar, These, Ziel und Methodik der Forschungsarbeit im Vorhinein klar zu umreißen und dafür, wie bei medizinischen Studien üblich, gezielt und beschränkt auf das statistisch und personenbezogen Notwendige Daten zu erheben und dafür den einzelnen Patienten individuell und studienbezogen aufzuklären. Ein

135 Sehr rechenintensive Algorithmen (z.B. „logistische Regression“) basierend auf neurowissenschaftlich inspirierten Konzepten aus den 1940er und 1950er Jahren, die eine Vielzahl von extrem einfachen Unterprogrammen miteinander verknüpfen. Mit Hilfe z.B. von durch Experten - oder Nutzer - vorklassifizierten „Trainingsdaten“ können die Algorithmen automatisch interne Parameter so optimieren, dass möglichst zuverlässig zur jeweiligen Eingabe die gewünschte Ausgabe erfolgt. Da für den Nutzer und Programmierer typischerweise nicht nachvollziehbar ist, wie der Algorithmus zu seiner Ausgabe kommt, ist seine Anwendung aus wissenschaftlicher Sicht allerdings gerade nicht mit einem Erkenntnisgewinn verbunden: Man geht letztlich nicht über das in den Trainingsdaten hinterlegte Expertenwissen hinaus. Dies wird deutlich selbst bei aktuellen datenintensiven Projekten wie z.B. dem Sprachprojekt „GPT 3“ der Firma OpenAI, das durch die Verarbeitung riesiger, nicht mehr überschaubarer Mengen an Texten als Trainingsmaterial praktisch zu beliebigen Themen längere, z.T. glaubhaft wirkende Aufsätze in englischer Sprache generieren kann. Während solche zunächst überraschenden und faszinierenden Effekte zwar u.a. zukünftige Gefahren für die Redlichkeit und Integrität des gesellschaftlichen Diskurses als Folge ungehemmter Datenakkumulation („*deep fakes*“) illustrieren, wäre die Vorstellung nicht zutreffend, dass ein entsprechender Algorithmus als „Künstliche Intelligenz“ einen Datensatz durchforstet und dabei „auf magische Art und Weise“ neue wissenschaftliche Erkenntnisse gewinnt. Ebensowenig, wie eine Maschine für mich essen und trinken kann, kann sie „für mich“ denken, erkennen und den Wissenshorizont erweitern.

gutes Beispiel ist die vom Bundesgesundheitsministerium geförderte „Nationale Kohorte“, eine großskalige Langzeit-Gesundheitsstudie mit ca. 200.000 Teilnehmenden.

Dies gilt auch für die Entwicklung von krankheitsbezogenen Algorithmen unter Verwendung von Methoden des Maschinellen Lernens[136]. Gerade die Entwicklung und das Training von Algorithmen, die eine Art neuronale Netze simulieren („Künstliche Intelligenz“/“Supervised Deep Learning“), erfordert qualitativ hochwertige, spezifische und klar klassifizierte Daten. Hier wäre beispielsweise eine feste Sammlung von 200.000 Datensätzen sicher mehr als ausreichend, um als Trainings- und Testdaten zu dienen.

Eine umfassende, zeitlich und inhaltlich unbegrenzte Vorratsdatenspeicherung zu wissenschaftlichen Zwecken ist dagegen weder gerechtfertigt noch erforderlich. Auch nicht die Existenz eines umfassenden und beliebig großen „Vorratsdatensatzes“, um sich dort „auf gut Glück“ auf die ungezielte Suche z.B. nach etwaigen Korrelationen machen zu können, in der Hoffnung, dass diese dann auch relevant seien.

Es kann also auch nicht beispielsweise im Rahmen einer Güterabwägung argumentiert werden, dass ein Ignorieren des informationellen Kontexts durch den Gesetzgeber, die Risiken einer massenhaften Erstellung von Persönlichkeitsprofilen oder eine Beschädigung der freiheitlich-demokratischen Grundordnung im Interesse eines erhofften medizinischen Fortschritts in Kauf zu nehmen seien. Dessen Prämisse ist schon ein Fehlschluss.

Wie wir schon gesehen hatte, hält auch die Behauptung eines vorgeblichen Gewinns an Datenautonomie einer kritischen Betrachtung nicht Stand. Tatsächlich werden durch die Gesetzgebung der Verlust an Kontrolle von und Übersicht des Patienten über seine intimsten Daten beschleunigt und dem Verlust der Datenautonomie der Versicherten faktisch Vorschub geleistet. Zumal die Gesetzgebung in keiner erkennbaren Weise auf Datensparsamkeit abzielt.

Internationales Ranking als Argumentationshilfe

Hinsichtlich der Diskussion einer Güterabwägung darf jedoch ein wichtiges Argument für die Einführung virtueller Patientenakten und zentraler Datensätze nicht vergessen werden, das nach meinem Eindruck in den Überlegungen, die zu der aktuellen Gesetzgebung geführt haben, eine zentrale Rolle spielt: Die Sorge, Deutschland werde andernfalls wirtschaftlich oder entwicklungsmäßig „abgehängt“, so dass geradezu ein alternativloser Sachzwang zur - schnellstmöglichen - Einführung virtueller Patientenakten und zentraler Sammlungen personenbezogener medizinischer Daten bestehe.

Die eher diffuse - und historisch vielleicht nicht *ganz* originelle - Sorge, den Anschluss zu verlieren oder zu kurz zu kommen, zeigt sich beispielsweise in der Heranziehung einer aufwändigen Studie der Bertelsmann-Stiftung: „*#SmartHealthSystems – Digitalisierungsstrategien im internationalen Vergleich*“[137].

Diese definiert einen „Digital Health Index“ und erstellt daraus in einer eindrücklichen Graphik eine Rangfolge von 17 betrachteten Ländern gemäß des Index‘, in der Deutschland den vorletzten Platz einnimmt[138]. Oje... Die scheinbare Offensichtlichkeit und psychologische Dramatik dieser Darstellung wird jedoch schnell relativiert, wenn man sich nüchtern vor Augen führt, dass eine bloße Rangfolge und eine Bewertung derselben sehr unterschiedliche Dinge

136 Methoden, die sich auch zur automatisierten Deanonymisierung zusammengeführter Datensätze eignen.

137 empirica/Bertelsmann-Stiftung: „#SmartHealthSystems – Digitalisierungsstrategien im internationalen Vergleich“ (November 2018); eine ältere Arbeit, die wohl ein ähnliches Gefühl von Dringlichkeit zum Ziel hatte, war die ‚Studie‘ zur elektronischen Patientenakte der Münch-Stiftung und eines privaten Instituts aus dem Jahr 2016, siehe z.B. https://www.stiftung-muench.org/studie-zur-elektronischen-patientenakte-im-ausland-klare-vorgaben-des-gesetzgebers-sind-voraussetzung-fuer-erfolgreiche-implementierung-2/ (zuletzt abgerufen 23.09.2020)

138 Ebd., S. 225; in der Diskussion gerne mit dem (ebenso dramatischen wie überheblichen) Hinweis versehen, dass „nur Polen“ noch dahinterliege...

sind und sich nicht automatisch das eine aus dem anderen ergibt. Ein Platz „auf den hinteren Rängen“ kann grundsätzlich ebenso negativ wie positiv oder völlig irrelevant sein.

So könnte man beispielsweise auch eine Rangfolge von Ländern nach Fällen häuslicher Gewalt oder Korruptionsfällen pro 100000 Einwohner erstellen. In der Deutschland vermutlich ebenfalls einen der hinteren Plätze einnähme - ohne, dass man daraus schließen sollte, dass hierzulande „Nachholbedarf“ hinsichtlich häuslicher Gewalt oder Korruption besteht.
Ebenso könnte man einen „Elephanten-in-freier-Wildbahn“-Index erstellen, in dem Deutschland wohl ebenfalls vergleichsweise schlecht abschneiden würde. Nur wäre das halt völlig irrelevant.

Der „Digital Health Index“ ist tatsächlich eine bloße Zustandsbeschreibung der politischen Strategie und der technischen Implementierung und Reife hinsichtlich digitaler Verfahren im Gesundheitswesen, sowie der „tatsächlichen Nutzung von Daten“[139]. Dies ist im Sinne einer technischen Zustandsbeschreibung völlig berechtigt und hilfreich. Aber es taugt nicht als Argument der politischen und gesellschaftlichen Debatte über den tatsächlichen, messbaren Nutzen für den Patienten, mögliche Risiken oder das gesellschaftlich Wünschenswerte.

Es lohnt sich, nochmal einen genaueren Blick darauf zu werfen. Tatsächlich zeigt sich, dass die Studie einfach als Prämisse, als Vorannahme, davon ausgeht, dass nicht näher definierte „digitale Innovationen“ und „internationale Trends“ im Gesundheitssystem per se vorteilhaft und für den medizinischen Fortschritt praktisch unabdingbar und daher anzustreben seien:
„*Digitale Innovationen im Gesundheitssystem können einen entscheidenden Beitrag zur Verbesserung der Gesundheitsversorgung leisten. Digitale Lösungen können die Patientensicherheit verbessern, die Qualität der Behandlungsergebnisse erhöhen und die wirtschaftliche Effizienz und Nachhaltigkeit eines Gesundheitssystems steigern. Vermehrt ergeben die internationale Studienlage sowie Ergebnisse aus nationalen und regionalen Implementierungsevaluationen, dass eine Digitalisierung des Gesundheitssektors in der Tat zu einer verbesserten Qualität von und zu einem besseren Zugang zu Gesundheitsdienstleitungen führen kann, wenn die Rahmenbedingungen dies begünstigen. Zudem zeigen internationale Trends, dass die zeitnahe Umsetzung von neuem medizinischen Wissen in ergebnisorientierte Versorgung und Qualitätssteigerung ohne die Vernetzung und Digitalisierung des Gesundheitswesens nicht erreichbar ist.*“[140]

„Internationale Trends“ als Messlatte. Hm. Dabei ist anzuerkennen, dass die Autoren der Studie dies vorsichtig als Potential formulieren. In einer aktuellen Nachfolgearbeit zur „Sekundärnutzung von Daten in elektronischen Patientenakten“[141] werden zudem die - potentiellen – Vorteile zumindest in einem Punkt konkretisiert:

„*Potenziale der Sekundärnutzung von Daten*
› Identifizierung kleinster Nebenwirkungen durch Analyse größerer Patientengruppen (> 100.000)
› Verbesserte Diagnose seltener Krankheiten
› Erhöhte Therapiesicherheit und personalisierte Medizin
› Schnellere Bewertung von Qualität und Nutzen neuer Behandlungsmethoden
› Zielgerichtete Präventionsmaßnahmen und frühzeitigere Eindämmung von Epidemien“[142]

Während auch hier wieder die meisten Punkte als Prämisse völlig allgemein und ohne Quantifizierung als erstrebenswerte „Potenziale“ in den Raum gestellt werden, ist zumindest in puncto Identifizierung „kleinster“ Nebenwirkungen eine konkrete Zahl von mindestens 100.000 Patienten genannt. Gemeint ist hier vermutlich nicht „kleinste Nebenwirkungen“ sondern

139 Ebd. S. 17
140 Ebd. S. 6
141 empirica/Bertelsmann-Stiftung: #SmartHealthSystems -Sekundärnutzung von Daten in elektronischen Patientenakten“, September 2020.
142 Ebd., S. 5

„seltene Nebenwirkungen“: Geringe Nebenwirkungen werden ja weder größer noch bedeutender, wenn man eine größere Zahl von Patienten betrachtet. Allerdings umfasst die bereits erwähnte Nationale Kohorte sogar 200.000 Patienten, so dass sich auch nach dieser Argumentation kein Bedarf an einer virtuellen Patientenakte oder einer zentralen Sammlung potentiell aller medizinischer Daten potentieller aller Bürgerinnen und Bürger ableiten lässt.

Nichtsdestotrotz verweist dieser Punkt, auch wenn er in der Studie ungenau formuliert ist, auf das einzige Argument, das meines Erachtens für eine Vorratssammlung der personenbezogenen medizinischen Daten ins Feld geführt werden kann: Wird eine maximale Vorratsdatensammlung und -speicherung gerechtfertigt durch die Hoffnung, selbst die letzten und allerseltensten Nebenwirkungen, Krankheiten oder deren Ursachen besser untersuchen zu können?

In gewisser Weise liefern die Covid-19-Pandemie und die mit ihr einhergehende bewundernswert schnelle Impfstoffentwicklung hier wie unter einem Brennglas hilfreiche Hinweise. Und damit sind nicht die Platitüden des deutschen Sachverständigenrats „Gesundheit“ gemeint, der digitale Verwaltungsprozesse in Gesundheitsämtern mit zentraler Datenspeicherung durcheinanderwirft, um eine vorgefasste Meinung begründen[143].

Gemeint ist, dass die rasche und dennoch gründliche Impfstoffentwicklung und die breite Verabreichung des Impfstoffs innerhalb kurzer Zeit an viele Bürgerinnen und Bürger in unterschiedlichen Gesundheitssystemen ein wohl einmaliges Nebeneinander von klinischen Studien vor und nach der Zulassung und datenbankbasierten Studien in zentralisierten Gesundheitssystemen bewirkt hat. Es ist zweifellos interessant, einen kurzen Blick darauf zu werfen. Dies kann nur schlaglichtartig geschehen, da hier keine umfassende „Meta-Studie“ geleistet werden kann.

So erschien im Dezember die klinische Studie zur Sicherheit und Wirksamkeit des mRNA-Wirkstoffs BNT162b2 von BionTech[144], die eine Wirksamkeit des Impfstoffs nach der zweiten Dosis zwischen 90,3 % und 97,6 % feststellte und Nebenwirkungen vergleichbar denen anderer Impfstoffe feststellte. Die Autoren weisen dabei darauf hin, dass sehr seltene Nebenwirkungen aufgrund der begrenzten Teilnehmerzahl unter Umständen statistisch nicht erfasst werden können.

Im April 2021 erschien eine vorläufige Studie, die sich der Frage widmete, wie sicher der mRNA-Impfstoff für Schwangere ist[145]. Dabei kamen zwei Methoden zum Einsatz: das freiwillige Ausfüllen von Online-Fragebögen über einen gewissen Zeitraum nach der Impfung im Rahmen eines strukturierten Programm, sowie ein Register, in das im Gesundheitswesen Impfreaktionen gemeldet werden. Die Autoren weisen darauf hin, dass aufgrund der Impfpriorisierung und Freiwilligkeit Auswahleffekte eine Rolle spielen können.

Ebenfalls im April 2021 wurde vorab eine noch nicht begutachtete, datenbankbasierte Studie veröffentlicht, die anhand von Daten aus dem englischen Gesundheitssystem die Frage untersuchte, wie sich die Impfung älterer Menschen mit dem mRNA-Impfstoff BNT162b2 auf positive Testraten und die Wahrscheinlichkeit eines Krankenhausaufenthalts auswirkte[146].

143 F. Gerlach et al.: „Digitalisierung für Gesundheit“, Gutachten 2021 des Sachverständigenrats zur Begutachtung der Entwicklung im Gesundheitswesen, Bonn/Berlin, März 2021; vgl. auch Kommentar im Anhang zu diesem Text

144 F. P. Polack et al.: „Safety and Efficacy of the BNT162b2 mRNA Covid-19 vaccine“, N. Engl. J. Med. 383, 2603 (2020).

145 T. T. Shimabukuro et al.: „Preliminary Findings of mRNA Covid-19 Vaccine Safety in Pregnant Persons“, N. Engl. J. Med., 21.04.2021 (DOI: 10.1056/NEJMoa2104983)

146 T. Mason et al, „Effects of BNT162b2 mRNA vaccine on Covid-19 infection and hospitalization among older people: matched case control study for England. 22.04.2021, *medRxiv*, 2021. doi: https://doi.org/10.1101/2021.04.19.21255461.

Innerhalb sehr großer statistischer Unsicherheitsbereiche ergaben sich laut Autoren Ergebnisse, die konsistent mit denen aus früheren Studien waren.

Im Mai 2021 wurde eine datenbankbasierte Studie veröffentlicht, die die Auswirkungen der ersten Impfdosis auf die Wahrscheinlichkeit eines Krankenhausaufenthalts für die Impfstoffe von BionTech und AstraZeneca in Schottland untersuchte[147] und dabei eine Wirksamkeit von 91 % (85 %...94%) bzw. 88 % (75%...94%) fand. Die Autoren weisen darauf hin, dass andere Effekte als die Wahrscheinlichkeit eines Krankenhausaufenthalts relevant sein könnten, und dass die beiden Impfstoffe nicht direkt miteinander verglichen werden konnten, da es sich nicht um eine kontrollierte Studie [*experimental study*] handle und zudem unterschiedliche Personengruppen die jeweiligen Impfstoffe erhielten.

Als letztes Beispiel soll hier noch auf die Entdeckung der seltenen aber schweren Nebenwirkung des Impfstoffs von AstraZeneca verwiesen werden (Sinusvenenthrombose), die trotz umfassender Datensammlung und -verarbeitung und einer massiven Impfkampagne in Großbritannien mit seinem umfassenden Zugriff auf Patientendaten gerade *nicht* dort gefunden und aufgeklärt wurde, sondern u.a. in Dänemark und in Deutschland. In Dänemark wurde im März 2021 über aufsehenerregende Einzelfälle berichtet[148]. In Deutschland führt das Paul Ehrlich-Institut im Rahmen der Arzneimittelüberwachung („Pharmakovigilanz“) ein entsprechendes Register.
Ein Grund dafür, dass die Nebenwirkungen in Großbritannien nicht auffielen, könnten unterschiedliche Altersempfehlungen für den Impfstoff sein. Andererseits zeigt der Fall, dass in funktionierenden Gesundheitssystemen schwere Nebenwirkungen auch in extrem seltenen Fällen praktisch sofort entdeckt werden, auch ohne zentrale Datenakkumulation und -verarbeitung.

Zusammenfassend gab es in den hier geschilderten Fällen im Wesentlichen drei Methoden: Strukturierte Studien mit konkret für die Studie erhobenen Daten; Register, in denen systematisch bestimmte Fälle und ihre Umstände anlassbezogen gesammelt werden; datenbankbasierte Studien, in denen unspezifische Datensammlungen herangezogen wurden.

Die datenbankbasierten Studien konnten die Ergebnisse der strukturierten Studien anhand einer großen erfassten Personenzahl bestätigen und relativ flexibel politisch interessante Fragen beantworten, wie die nach der Wirksamkeit der ersten Dosis. Gleichzeitig ist keine unmittelbare neue Erkenntnis erkennbar, die über die strukturierten Studien hinausgeht oder mit ihr nicht hätte beantwortet werden können. Tatsächlich streben solche Studien ja auch immer an, repräsentativ zu sein.
Gleichzeitig wurden zumindest schwere Nebenwirkungen ohne die Notwendigkeit einer unspezifischen Datensammlung schnell und zuverlässig entdeckt[149].

Tatsächlich wird in der Berichterstattung bezüglich der datenbankbasierten Studien mit unspezifischen Datensätzen zum Teil eher mit dem „Bauchgefühl“ argumentiert, dass man in der Realität noch einmal die Gewissheit und ein besseres Gefühl bekommen habe, dass die repräsentativen Studien auch wirklich repräsentativ sind. Gleichzeitig ist es für Forschende natürlich angenehm und praktisch für viele schnelle Veröffentlichungen, wenn einfach fertige Datensätze ausgewertet werden können, auch wenn sie vielleicht nicht optimal sind. Beides sind allerdings keine besonders starken Argumente in der Abwägung, welchem Risiko man personenbezogene medizinische Daten aussetzen möchte.

147 E. Vasileiou et al., „Interim findings from first-dose mass COVID-19 vaccination roll-out and COVID-19 hospital admissions in Scotland: a national prospective cohort study“, The Lancet, 397, 1646 (2021)
148 C. Guldberg und A. Tørring: „Indberetter nyt dødsfald: Mistanke im vaccinebivirkninger“, EkstraBladet, 20.03.2021
149 Bei leichten Nebenwirkungen oder solchen, die nach langer Zeit auftreten, wird allerdings eine statistische Analyse an Bedeutung gewinnen.

In der Summe kann man sich immer die Fragen stellen: Welche Alternativen gibt es? Worin liegt wirklich, „unter dem Strich“ und ehrlich der Mehrwert einer unspezifischen Sammlung persönlichster Daten gegenüber Alternativen wie strukturierten Studien oder anlassbezogenen Registern? Gibt es sogar Nachteile?

Ich bin mir sicher, dass es Vorteile/Mehrwerte gibt, und einige wurden ja auch schon genannt. Aber sind sie konkret und groß genug, um das Risiko eines massenhaften und nie mehr zu heilenden Datenmissbrauchs aufzuwiegen, der die Grundlagen unserer freiheitlich-demokratischen Gesellschaftsordnung erschüttern oder zum Einsturz bringen würde? Was wiegt schwerer?

Im Grunde ist es eine ähnliche Frage wie in anderen Fällen der Vorratsdatenspeicherung: Darf man - sei es als Staat, als beauftragte Einrichtung oder als Unternehmen - die Kommunikationsdaten und Bewegungsprofile potentiell aller Bundesbürgerinnen und Bundesbürger umfassend und unbegrenzt auf Vorrat erfassen und speichern? Wird dies gerechtfertigt durch die Hoffnung, in der Zukunft auch das letzte und seltenste Verbrechen wie z.B. einen Terroranschlag lückenlos aufklären oder gar verhindern zu können? Wird dies gerechtfertigt durch wirtschaftliche Interessen? Darf der Staat das in einer Kettengesetzgebung „durch die Hintertür“ implementieren? Darf er alle Bundesbürgerinnen und Bundesbürger dazu auffordern oder dazu verführen, einer solchen Vorratsspeicherung, Datenakkumulation und Profilbildung „freiwillig“ zuzustimmen? Darf dies ein Unternehmen wie Google? Was wiegt schwerer: Die Unversehrtheit der verfassungsmäßigen Ordnung und das Grundrecht auf Freiheit auch gegenüber der Freiheit der Anderen? Oder die Hoffnung, auch extrem seltene Ereignisse oder Krankheiten eines Tages aufklären bzw. heilen zu können? Oder unternehmerische Freiheit und wirtschaftliche Interessen? Das wäre mal eine sinnvolle Frage, die eine gesellschaftliche Diskussion lohnen würde.

Datensparsame Alternative

Hinsichtlich medizinischer Daten und seltener Nebenwirkungen oder Krankheiten ließe sich dieses Dilemma allerdings leicht auflösen. Nämlich durch internationale Kooperation, wie sie in der Forschung völlig üblich ist. Da die Physiologie des menschlichen Körpers keine Grenzen kennt, wäre es ohne weiteres möglich, in jedem Land, das eine politische Einheit bildet, einen Datensatz von einer festen, begrenzten Personenzahl ähnlich der Nationalen Kohorte zu erstellen und diese Datensätze dann über politische Grenzen hinweg bei Bedarf zu kombinieren. Auf diese Weise wäre einerseits sichergestellt, dass nie eine politisch „kritische Masse“ von Bürgerinnen und Bürgern eines freiheitlich-demokratisch verfassten Staates erfasst wird, während man andererseits für Forschungszwecke durch Kombination der verschiedenen nationalen Datensätze zu großen Patientenzahlen und repräsentativen Daten gelangt.

Ein Antrieb zu solchen Überlegungen setzt allerdings erstmal ein Problembewusstsein für Ausmaß und Gefahren unbegrenzter Datensammlung, Datenkonzentration und der Teil- oder Totalabbildung der Persönlichkeit voraus. Den Willen, der Wirklichkeit ins Auge zu sehen. Neben der internationalen Perspektive wird in der genannten Studie jedoch insbesondere auch das Datenumfeld, der informationelle Kontext, konsequent ausgeklammert. Auch die dort angestellten Überlegungen hinsichtlich einer „Sekundärnutzung“ der Daten, die vielleicht eines nicht allzu fernen Tages in eine monetäre „Tertiärnutzung“ übergeht, sind nicht unproblematisch, wie ein Blick nach Großbritannien zeigt.

Virtuelle Patientenakte im Vereinigten Königreich

Dort existieren seit Langem sowohl eine virtuelle Patientenakte[150] als auch eine umfassende zentrale Datenbank der personenbezogenen medizinischen Daten „zu Forschungszwecken“, der *Clinical Practice Research Datalink* (CPRD)[151]. Hier hat sich das Unternehmen Google über das Forschungs- und Entwicklungsunternehmen „DeepMind“ bereits den Zugriff auf Millionen Patientendaten verschafft. Die Zeitung „The Observer“ berichtete am 8. Februar

150 Sie ist im dortigen Gesundheitssystem allerdings mit einer Widerspruchslösung verknüpft, d.h. Daten werden nur dann nicht darin gespeichert, wenn der Patient dem explizit widerspricht.

151 https://www.cprd.com/

2020 zudem unter der Überschrift „*Enthüllt: Wie Pharmariesen Zugriff auf Ihre Gesundheitsdaten [health records] erhalten*“[152], dass die CPRD die medizinischen Daten von Millionen Versicherten „zu Forschungszwecken“ an US amerikanische Pharmafirmen verkauft habe. Die Daten waren zwar anonymisiert, wie es ja auch für das Forschungsdatenzentrum vorgesehen ist. Es stellte sich jedoch heraus, dass die Pharmafirmen in der Lage waren, die Daten deanonymisieren, und dass sie damit sogar warben[153].

Eine Datenschützerin wird in dem Artikel mit den Worten zitiert: „*Wirklich anonyme Daten, die auf keinen Fall auf eine bestimmte Person zurückgeführt werden können, sind sehr schwierig zu realisieren angesichts des Umstands, dass so viele Informationen von uns im Umlauf und im Besitz von Firmen wie Facebook und Google sind* […].“[154], ein IT-Forscher der Universität Leicester wird zudem mit den Worten zitiert, dass „*wenn es sich um umfangreiche personenbezogene medizinische Daten handelt, gilt, dass je umfangreicher sie sind, desto einfacher ist es für Experten sie zu rekonstruieren und einzelnen Personen zuzuordnen.*“[155], wobei ein ebenfalls dort zitierter Datenschutz-Aktivist das Problem auf den Punkt bringt: „*Ihre medizinischen Daten sind wie ein Fingerabdruck Ihres gesamten Lebens.*“[156]

Auch diese Vorgänge in einem informationellen System, das sehr vergleichbar zu dem vom Gesetzgeber eingeführten ist, und die möglicherweise Anlass zu einer eher kritischen Sicht auf zentrale Datensammlungen medizinischer Daten geben könnten, werden vom Gesetzgeber geflissentlich und konsequent ignoriert.

Neben dieser „Tertiärnutzung“, also der Reduktion auf einen monetären Wert verbunden mit einer immer freizügigeren Verwendung und Verbreitung personenbezogener medizinischer Daten zu kommerziellen Zwecken, lässt sich aber auch die euphorische Hoffnung auf die hohe und direkte Dividende einer Sekundärnutzung hinterfragen.

So beschreibt eine Veröffentlichung in der zur Nature Gruppe gehörenden Fachzeitschrift „Digital Medicine“ die Evaluierung einer „digitalen Innovation“ zum Management akuter Nierenschäden im klinischen Umfeld[157]. Dabei ging es im Wesentlichen um die Anwendung „Streams“ des bereits erwähnten Unternehmens DeepMind. Dort stellen die Autoren fest, dass die Anwendung zwar Vorteile hinsichtlich der Effizienz der Abläufe gebracht habe, aber zu keiner messbaren Verbesserung des Behandlungserfolgs (*clinical outcome*) geführt habe. Dies unterstreicht nochmals, dass die Einführung einer virtuellen Patientenakte nach aktuellem Stand keinen quantifizierbaren medizinischen Vorteil für die Patienten bringt; insbesondere keinen, der die genannten Risiken und den gegebenen informationellen Kontext aufwiegen könnte.

Mit diesem Beispiel soll nicht gesagt werden, dass die Anwendung digitaler Verfahren und von Algorithmen, die auf maschinellem Lernen basieren, sich niemals in einer messbaren Verbesserung des Behandlungserfolgs äußern wird. Das wäre sicher falsch. Aber es unterstreicht, dass euphorische Zukunftsvisionen sich schnell als substanzlos entpuppen, wenn man nach dem tatsächlichen, messbaren Nutzen fragt[158]. Denn dessen Existenz und

152 Toby Helm: „Revealed: how drugs giants can access your health records“, The Observer, 08.02.2020 (https://www.theguardian.com/technology/2020/feb/08/fears-over-sale-anonymous-nhs-patient-data, zuletzt abgerufen 23.09.2020)

153 Ebd.

154 Ebd.

155 Ebd.

156 Ebd.

157 Connell et al.: „Evaluation of a digitally-enabled care pathway for acute kidney injury management in hospital emergency admissions“, NPJ/Digital Medicine, 31.07.2019.

158 Zwar muss beispielsweise Grundlagenforschung nicht immer einen unmittelbaren Nutzen vorweisen können, aber zum Einen ist hier der Grundlagencharakter stark zu bezweifeln, zum Anderen verringert ein fehlender Nutzen das Gewicht im Fall einer Güterabwägung, vor allem wenn eine Gefährdung der freiheitlich-demokratischen Grundordnung oder eine Verletzung von Grundrechten gerechtfertigt werden

Relevanz ist weder selbsterklärend noch evident. Forschung ist kein geradliniger Weg und keine Maschine, die auf Knopfdruck die gewünschten Ergebnisse liefert.

Das Beispiel illustriert vielmehr, dass bei nüchterner Betrachtung der Weg wohl länger und steiniger ist und der tatsächliche Mehrwert und Nutzen an seinem Ende vielleicht bodenständiger und begrenzter sind, als es in einer mit missionarischem Eifer betriebenen Debatte mit ihren unmittelbaren Heilsversprechen nahegelegt wird. Eine Debatte, die oft eher einem Monolog gleicht und die geprägt ist von sich überbietenden Schlagworten wie „disruptiver digitaler Innovation“ oder „innovativer digitaler medizinischer Versorgung“[159]. Bitte was?

Ein missionarisch geprägter Monolog, der in die selbst gestellte psychologische Falle führt durch den Zirkelschluss, dass jedwede Kritik unqualifiziert und daher unberechtigt sei. In dieser Logik müssen „Zweiflern“ die Augen für die großartigen Verheißungen „der Digitalisierung“ geöffnet werden, damit sie deren alles rechtfertigende Vorteile endlich „einsehen“. Und die ganz „Verstockten“? Die muss man notfalls zu ihrem Glück „zwingen“.

Und das ist leider, wie eingangs beschrieben, ein probater Katastrophenmechanismus.

Diese nicht hinnehmbare Haltung scheint sich nun leider auch in der verwirrenden und inkrementellen Gesetzgebung wiederzufinden, die quasi durch die Hintertür und im Nebel einander ablösender Gesetze versucht, unterhalb der Wahrnehmungsschwelle Fakten zu schaffen.

Tatsächlich aber sind sowohl Dringlichkeit als auch die vermeintliche Alternativlosigkeit und „Sachzwänge“ in der Realität wohl deutlich weniger dramatisch und ausgeprägt als der Aktivismus des Bundesministers für Gesundheit nahelegt.

Was dagegen meiner Ansicht nach äußerst dringlich wäre, wäre die Benennung von und Auseinandersetzung mit der Sitten- und Verfassungswidrigkeit der massenhaften, täglich fortschreitenden Profilerstellung der Bürgerinnen und Bürger durch Unternehmen. Und zwar möglichst bevor der freie und mündige Bürger und mit ihm der demokratisch legitimierte freiheitliche Staat und seine Institutionen verblassen zu sinnentleerten, schattenhaften Erinnerungen einer Gesellschaft, in der datengetriebene Akteure die Bürgerinnen und Bürger in allen, selbst den intimsten Lebensbereichen beobachten, erfassen, kontrollieren, einordnen und bewerten[160].

Mit Blick auf das Gesundheitswesen ist es nun lehrreich, einen näheren Blick auf die Versuche des „Augen-Öffnens“ zu werfen, da sie ungewollt einen weiteren Fehlschluss offenbaren. Ein beliebtes Mittel, einer vermeintlich „unaufgeklärten“ Öffentlichkeit die Verheißungen der unbegrenzten Datensammlung im Rahmen von *Digital Health* vor Augen zu führen, sind kurze, völlig fiktive Filme, die aus Sicht ihrer Macher erstrebenswerte Zukunftsszenarien darstellen, in denen beispielsweise der persönliche, zwischenmenschliche Kontakt zwischen Arzt und Patient ganz oder teilweise durch einen „digitalen Assistenten“ ersetzt ist, mit dem man seinen Gesundheitszustand am Bildschirm effizient „besprechen“ kann[161].

Unterschied zum Gesundheitssystem USA,VK

Einmal abgesehen von der Frage, ob es sich dabei eher um eine Utopie oder eher um eine Dystopie handelt, illustriert dieses Beispiel, wie unkritisch und unreflektiert Motivationen und

soll.

159 „Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur digitalen Modernisierung von Versorgung und Pflege“, S. 1

160 Vgl. hier auch die Versuche von Unternehmen wie z.B. Facebook, durch Einführung einer eigenen Währung in die globale Finanz- und Wirtschaftspolitik einzugreifen.

161 z.B. „Tim und der Avatar Dina – E-Health im Alltag im Jahr 2037“, IGES GmbH, 2017 (https://youtu.be/VcB6-JH2eJg, https://www.iges.com/themen/iges-future-script/index_ger.html, zuletzt abgerufen 24.09.2020)

Problemlösungsstrategien übernommen werden, die sich auf die spezifischen Eigenheiten und Unzulänglichkeiten von Gesundheitssystemen im englischsprachigen Raum beziehen. Dabei geht es insbesondere um die USA und das Vereinigte Königreich.

Da ist einerseits das praktisch vollständig privatisierte und auf Gewinnmaximierung ausgerichtete Gesundheitssystem der USA, das zwar einerseits Inseln der Spitzenmedizin aufweist, zu dem aber andererseits weite Teile der Bevölkerung aufgrund ihres sozialen Status‘, ihres Wohnorts, fehlenden Vermögens angesichts hoher Kosten und fehlender oder unzureichender Krankenversicherung keinen adäquaten Zugang haben.
Hieraus ergibt sich eine auf Gewinnmaximierung, aber auch eine auf Teilhabe zielende Argumentation, derzufolge ein Effizienzgewinn darauf zielt, mehr Menschen günstig eine bessere Versorgung zu ermöglichen. Dies klingt zwar gut und sinnvoll, bezieht sich aber auf die erhoffte Linderung ganz spezifischer Unzulänglichkeiten des US amerikanischen Gesundheitssystems.

Andererseits ist da das praktisch vollständig verstaatlichte, unterfinanzierte und zentralistisch organisierte Gesundheitssystem in Großbritannien (*National Health Service, NHS*)[162], das der allgemeinen Berichterstattung zufolge bereits durch eine stärkere Grippewelle an seine Belastungsgrenze geführt wird. Es ist zudem durch eine geringe Arzt- und Krankenhausdichte[163] und stark formalisierte Patientensteuerung geprägt und dadurch, dass selbst bei schwerer Erkrankung der Zugang zu einem Facharzt unsicher und oft erst nach langer Wartezeit oder gar nicht möglich ist.
Hier zielt die Argumentation hinsichtlich einer erhofften Effizienzsteigerung einerseits ebenfalls auf ökonomische Vorteile angesichts notorisch knapper Finanzierung, andererseits auf eine bessere Steuerung des Patienten durch das von Unterversorgung gezeichnete, zentralisierte und nicht eben effiziente System.

Es wird mit anderen Worten ohne nachzudenken und mit aller Macht versucht, Lösungen für Probleme auf Deutschland zu übertragen und weiterzuentwickeln, die es in dem wohl finanzierten, durch die Soziale Marktwirtschaft und ein Nebeneinander von Krankenhäusern und niedergelassenen Ärzten sowie freie Arztwahl geprägten dezentralen deutschen Gesundheitssystem mit seiner großen Versorgungsbreite und -tiefe so nicht gibt.
Einem Gesundheitssystem dessen Robustheit und Qualität sich – bei aller berechtigten Kritik und ihm eigenen Verbesserungsmöglichkeiten - auch im weltweiten Vergleich durchaus bewährt.

Hier stellt sich nicht allein die Frage, ob die entsprechenden finanziellen, technischen und legislativen Ressourcen daher nicht besser in die spezifischen Stärken und Entwicklungspotenziale des deutschen Gesundheitssystems investiert wären.

Äußerst relevant ist aber, dass dieses Vorgehen, unreflektiert Lösungen auf ein System zu übertragen für das sie nicht gedacht sind, mit Blick auf die Integrität der verfassungsmäßigen Ordnung die Gefahr birgt, durch das unkritische Übernehmen von unpassenden Lösungsansätzen und Strukturen auch die zugehörigen Probleme in das deutsche Gesundheitssystem einzuführen. Hierzu gehört z.B. ein problematischer Umgang mit und Zugang zu personenbezogenen medizinischen Daten und deren zentrale Zusammenführung und Vorratsspeicherung nach Vorbild der CPRD in Großbritannien bis hin zur Profilerstellung, und zwar unter Ignorierung des informationellen Kontexts.

---

162 Vgl. hier auch die unten vorgetragenen Erläuterungen zum erfolgreichen WannaCry-Angriff auf zahlreiche Einrichtungen des von zentralisierter Datenhaltung geprägten NHS.

163 z.B. T. Gerlinger und K. Mosebach: „*Versorgungsstrukturen des britischen Gesundheitssystems*“, Bundeszentrale für politische Bildung, 2014 (https://bpb.de/politik/innenpolitik/gesundheitspolitik/72931/versorgungsstrukturen, zuletzt abgerufen 26.09.2020)

Auch die Sorge vor wirtschaftlichen Nachteilen gegenüber anderen Ländern mit wenig entwickeltem Datenschutz und deren Firmen erscheint generell nur insofern berechtigt, als der Gesetzgeber Ansprüche an den Daten- und Grundrechtsschutz nicht aktiv vertritt. Und er sie nicht auf dem Markt durchsetzen und dort Verstöße auch sanktionieren will, im Extremfall bis hin zur Ausschließung von Marktteilnehmern. Denn es ist ja gerade die der Sozialen Marktwirtschaft zugrundeliegende Erkenntnis, dass der Markt zwar ein komplexes System aber keine übermächtige „Naturgewalt“ ist, deren Launen und erratischen Prozessen die Gesellschaft hilflos ausgeliefert ist. Keine Gesellschaft muss sich einen ruinösen Wettbewerb liefern, in dem in einer Abwärtsspirale immer mehr Ansprüche und Standards fallen gelassen werden, sei es im Umwelt-, Sozial- oder eben auch im informationellen Bereich mit Blick auf die Vermeidung massenhafter Profilerstellung. Die Gesellschaft muss sich dem Kampf nur stellen.

Dagegen lädt die Erstellung und Vorhaltung eines potentiell alle krankenversicherten Bürgerinnen und Bürger umfassenden, zentralen Datensatzes ihrer personenbezogenen medizinischen Daten (inklusive Therapien, Befunden etc.) geradezu ein zu einer legalen oder auch irregulären Datenaneignung (oder der Behauptung ihrer Aneignung) und der Verwendung zur massenhaften Erstellung von Persönlichkeitsprofilen oder deren Weiterentwicklung.

Gesetzgebung: Allgemeingültigkeit, Transparenz und Klarheit

Nun könnten der Gesundheitsminister oder der Gesetzgeber einwenden, dass es in der Vergangenheit ja ohnehin nur ein geringes Interesse an der Nutzung einer virtuellen „elektronischen Patientenakte“ gegeben habe, so dass man hoffen könne, dass auch in Zukunft nur ein minimaler Teil der Versicherten hier erfasst werden. Diese Argumentation ist jedoch nicht stichhaltig.

Dies wäre angesichts des betriebenen Aufwands zum Einen eine wenig glaubwürdige Haltung, zumal das „Prinzip Hoffnung“ einem inakzeptablen Lotterie-Spiel mit der Integrität der freiheitlich-demokratischen Grundordnung gleichen würde. Zum Anderen wurden, wie oben ausgeführt, durch die Gesetzgebung die Rahmenbedingungen massiv geändert und aktiv ein Markt geschaffen, der Weg für Unternehmen wie Google geebnet. Es werden wirtschaftliche Interessen bei Akteuren des Gesundheitssystems geweckt, die bisher ohne ausgeprägtes Eigeninteresse im Interesse des Versicherten handelten und daher bisher dessen Vertrauen genießen konnten. Nunmehr wird jedoch das Befüllen der Datenbank beispielsweise *en passant* „mit Zuckerbrot und Peitsche“ in die Behandlungssituation integriert, indem der Arzt einer Datenübertragung nicht widersprechen kann und gleichzeitig von der Übertragung der Daten durch eine Vergütung wirtschaftlich profitieren soll.

Um die Problematik der Argumentation nach dem „Prinzip Hoffnung“ in überspitzter Form zu illustrieren: Der Gesetzgeber könnte ja nach derselben Logik bewusst ein Rekrutierungs- und Logistikzentrum zur Unterstützung organisierter Kriminalität und verfassungsfeindlicher Akteure im Digitalen Raum schaffen nebst Auslobung einer Vermittlungsprämie, und dann seiner Vermutung Ausdruck verleihen, dass es wohl nicht in Anspruch genommen werde, da ja auch in der Vergangenheit nur ein geringer Teil der Bürgerinnen und Bürger in diesem Bereich aktiv gewesen sei.

Nein, dem Gesetzgeber muss vernünftigerweise unterstellt werden, dass er seine Rolle ernst nimmt und daher von seinen Zielen sowie der Effektivität seiner Maßnahmen zu ihrer Erreichung überzeugt ist. Ende des 18. Jahrhunderts formulierte der Philosoph Immanuel Kant in der preußischen Monarchie den theoretischen Anspruch an den Einzelnen: „Handle stets so, dass der Grundsatz Deiner Handlungen gleichzeitig ein Gesetz für alle sein könnte“[164]. Umgekehrt muss für den Gesetzgeber in der Demokratie ganz praktisch gelten: „Formuliere Deine Gesetze stets so, dass sie verallgemeinerbar und zur Grundlage des Handelns jedes Einzelnen werden können (ohne die freiheitlich-demokratische Grundordnung zu gefährden).“

164 Wörtlich: „Handle nur nach derjenigen Maxime, durch die zugleich wollen kannst, dass sie ein allgemeines Gesetz werde.“

Mit dem „Patientendaten-Schutz-Gesetz“ kristallisieren sich, wie oben dargestellt, zwei wesentliche Ziele heraus, die die häppchenweise Kettengesetzgebung wohl von vornherein anstrebte und für die die vorangegangenen Gesetze nach und nach die einzelnen Bausteine lieferten:

Zum Einen wird u.a. mit der Neuausrichtung der Krankenkassen eine Art deutsches „Profilerstellungs-Biotop“ von Datensammlern, -händlern und -verwertern im Gesundheitswesen nebst zugehörigem Markt geschaffen, die gestützt auf medizinische Daten und Profile der Versicherten digitale Anwendungen entwickeln und einsetzen[165].

Zum Anderen soll ein zentraler, möglichst umfassender und inhaltlich wie zeitlich unbegrenzter, gigantischer und fortwährend wachsender „Vorratsdatensatz“ der medizinischen Daten möglichst aller Bürgerinnen und Bürger aufgebaut und vorgehalten werden in der falschen Annahme, dies sei Voraussetzung für „digitale Innovationen“ in der Medizin und für die Entwicklung und Förderung eines entsprechenden Wirtschaftszweigs.

Sowohl das Eine als auch das Andere wie auch die Zwangsverpflichtung des ärztlichen Personals als Makler und Dienstleister dieser Ziele stehen im Widerspruch zu der besonderen Schutzwürdigkeit eines interessefreien Vertrauensverhältnisses zwischen Ärztin und Patient.

Zudem ist mein Eindruck, dass „lästige“ Datenschutzbestimmungen und -bedenken dabei gemäß der Maxime „*Datenschutz ist was für Gesunde*“[166] vermieden oder umgangen und ein unbequemer informationeller Kontext verdeckt werden. Beispielsweise durch eine Gesetzgebung in „Salamitaktik“, die möglichst spät – im „Idealfall“: zu spät - ein Gesamtbild ergibt.

Nun ist es in der politischen Debatte wohl nicht unzulässig und vielleicht auch nicht unüblich seine Ziele aus taktischen Gründen bis zu einem gewissen Grad zunächst zu „verschleiern“ und indirekt anzustreben, z.B. um Widerstände zu überwinden oder zunächst Gemeinsamkeiten zu suchen. Im Bereich der Gesetzgebung aber, die von der Klarheit ihrer Formulierungen und auch Intention, sowie von der Vielfältigkeit der vorangegangenen Diskussion lebt, ist dies nicht nur schlechter Stil, sondern hochproblematisch und allenfalls ein äußerst schmaler Grat, der begangen werden kann.

Und auch der wird spätestens dann verlassen, wenn die Schritte einer Kettengesetzgebung so gestaltet sind, dass der jeweils nächste geplante Schritt, in dessen Licht die Problematik bis hin zur Grundrechtsverletzung des vorigen Schrittes vielleicht erst deutlich wird, erst dann öffentlichkeitswirksam veröffentlicht wird oder in Kraft tritt, wenn die Frist zum Widerspruch gegen das vorhergehende Glied in der Gesetzeskette bereits abgelaufen ist. Und selbst wenn dies, wovon ich ausgehe, aus Sicht des Gesundheitsministers in bester Absicht geschieht, sollte es niemals Ziel oder auch nur Mittel der Gesetzgebung sein, die Bürgerinnen und Bürger bezüglich der Ausübung ihrer verfassungsmäßigen Rechte „auszutricksen“.

Wie stark die Überzeugung von der Überlegenheit der eigenen Absicht auch sein mag, keinesfalls darf dies dazu führen, dass ein wesentlicher Teil des Kontexts der Gesetzgebung, wie hier der informationelle Kontext, bewusst und konsequent ignoriert wird oder Schaden für die freiheitlich-demokratische Grundordnung oder Grundrechtsverletzungen in Kauf genommen werden. Genau das ist hier jedoch ebenfalls der Fall, und vor diesem Hintergrund und dem Hintergrund der wohl bewusst inkrementellen Kettengesetzgebung in Salamitaktik ist aus meiner Sicht die Verordnungsermächtigung des Bundesgesundheitsministers[167] ebenfalls problematisch: Hier gibt der Bundestag das Heft des Handelns unzulässigerweise völlig aus

165 Was konsistent mit den Überlegungen in dem bereits früher erwähnten Buch des derzeitigen Bundesministers für Gesundheit wäre, s.u..

166 J. Spahn, M. Müschenich und J. F. Debatin: „App vom Arzt“, Herder Verlag (Freiburg), 2016, S. 2

167 Art. 1 Nr. 31 „§ 363 Absatz (7)“ PDSG

der Hand, so dass das Gesundheitsministerium sich nicht einmal mehr gegenüber dem Gesetzgeber rechtfertigen und in der parlamentarischen Debatte mit kritischen Nachfragen auseinandersetzen muss, bevor es Fakten schafft.

Es ist kein Bestreben des Gesetzgebers zu erkennen, die Teil- oder Totalabbildung von Persönlichkeiten der Bürgerinnen und Bürgern einzudämmen oder zu verhindern. Durch den Gesetzgeber wird auch der Zugriff von Datenverwertern und Profilerstellern wie beispielsweise Google, VKontakte oder Facebook auf Gesundheitsdaten nicht erschwert, sondern im Gegenteil eine Ausweitung ihrer als Dienstleistung ausgegebenen Datensammlung und -verwertung eher noch erleichtert und unterstützt.

Mit der Erstellung immer mehr zentraler Datenbanken potentiell aller medizinischen Daten potentiell aller Bürgerinnen und Bürger flankiert von „individuell geeigneten Innovationen“ wird gezielt der Weg zu einer - als Individualisierung umschriebenen - Profilbildung geebnet. Der Gesetzgeber erleichtert es in der Profilbildung erfahrenen Unternehmen, über „digitale Innovationen“ oder auch als Dienstleister der Krankenkassen Zugriff auf immer mehr medizinische und andere personenbezogene Daten und Metadaten der Versicherten zu erhalten. Der Gesetzgeber weitet die massenhafte Profilerstellung gezielt aus auf den Bereich medizinischer Daten und das Gesundheitssystem.

Hinzu kommt, dass das Versprechen, die Versicherten könnten „selbst bestimmen“, wie die Daten verarbeitet werden und wer auf sie Zugriff habe, schon im Regelbetrieb und vor dem ersten Hackerangriff eine Illusion und damit ein leeres Versprechen ist.

Das „Administratoren-Dilemma“

In der Realität haben, anders als der Gesetzgeber nahelegt, keineswegs nur die Patienten und Berechtigte aus dem medizinischen Behandlungskontext Zugriff auf die gespeicherten Daten. In jedem Netzwerk und für jede Datenbank und Serverstrukturen gibt es, potentiell wechselnde, Administratoren mit umfassenden Rechten, die faktisch volle Zugriffsrechte auf alle gespeicherten und verarbeiteten Daten haben („Administratoren-Dilemma“).

Die Problematik dieses „blinden Flecks“ wurde u.a. durch einen massiven, erfolgreicher Hackerangriff auf das Unternehmen „Twitter“ ins Licht der Öffentlichkeit gerückt. Administratoren können Sicherheitsmaßnahmen umgehen oder außer Kraft setzen und haben grundsätzlich die Möglichkeit eines umfassenden Netzwerk- und Datenzugriffs.
Dies kann einerseits durch den oder die, mitunter wechselnde und für Außenstehende meist anonyme, Administratoren selbst geschehen. Alternativ ist es im Fall des Unternehmens „Twitter“ Dritten erfolgreich gelungen, sich Administratorenrechte anzueignen und somit beispielsweise die Möglichkeit, „*Passwörter von Nutzern [zu] ändern und zusätzliche Sicherheitsfunktionen wie die Zwei-Faktor-Authentifizierung aus[zu]schalten*“[168].

Dies unterstreicht, dass generell ein Verweis auf oder eine Forderung nach Datensicherheit „entsprechend dem Stand der Technik“ nur insofern ausreichend und angemessen ist, als der Stand der Technik ausreichend und angemessen ist. U.a. dieser Vorfall weist darauf hin, dass dies nicht der Fall ist, insbesondere nicht für umfassende Sammlungen personenbezogener medizinischer Daten. Bei einem solchen Verweis handelt es sich daher um eine selbst-referentielle Leerformel, d.h. einen Zirkelschluss.

Der Gesetzgeber hat durch die Pflicht zur Schaffung einer zentralen Datenbankstruktur für die Aufnahme potentiell aller medizinischen Daten der Versicherten neben dem behandelnden Arzt, zwischen dem und seinem Patienten neben berufsrechtlichen Vorschriften ein persönliches Bekanntschafts- und Vertrauensverhältnis und Gefühl persönlicher Verpflichtung besteht, eine zusätzliche Gruppe mit an den Tisch gesetzt. Eine Gruppe anonymer und potentiell wechselnder „Administratoren“ mit vollen Zugriffsmöglichkeiten auf die in einer virtuellen Patientenakte gespeicherten und verarbeiteten Datensätze.

168 M. Muth: „Angriff auf den Gott-Modus“, Süddeutsche Zeitung vom 17.07.2020

Die uneingeschränkte Verpflichtung des ärztlichen Personals zur Übertragung potentiell aller medizinischer Daten bedeutet, Daten, die durch die Schweigepflicht geschützt sind, unbekannten und beliebig wechselnden Dritten zwangsweise und auch entgegen der ärztlichen Fürsorgepflicht weiterzugeben. Die zudem kein berechtigtes medizinisches Interesse an den Daten vorweisen können, die aber die Möglichkeit hätten, die Daten zu kopieren, z.B. für eine spätere Entschlüsselung oder Weitergabe.

Verschlüsselung, Datensicherheit

Nun könnte man einwenden, dass ein Missbrauch der Daten aufgrund ihrer Verschlüsselung ausgeschlossen sei. Vielmehr seien die verschlüsselten Daten für den Angreifer, der sie sich irregulär angeeignet habe, ja wertlos. Das ist so nicht der Fall.

Es gibt im Wesentlichen zwei Arten von Verschlüsselungsverfahren (und deren Kombination)[169].

Zum Einen gibt es Verfahren, bei denen alle Beteiligten einen gemeinsamen, geheim gehaltenen Schlüssel besitzen, auf den sie sich vorher geeinigt haben. Diesen Schlüssel - letztlich eine Zahlenfolge – verwenden sie, um Daten z.B. vor dem Absenden oder dem Speichern zu verschlüsseln, und um sie wieder zu entschlüsseln, wenn die Daten empfangen werden, z.B. beim Herunterladen oder dem Empfang einer Nachricht. Da alle Parteien denselben Schlüssel besitzen und die Daten ver- und entschlüsseln können, spricht man hier von einem „symmetrischen“ Verfahren.

Entscheidend für die Sicherheit ist, dass der Schlüssel geheim ist und bleibt und auch nicht anderweitig erraten oder herausbekommen werden kann. Denn jeder, der den Schlüssel besitzt, kann die Daten entschlüsseln.

Zum Anderen gibt es Verfahren, bei denen zwei Schlüssel verwendet werden: ein öffentlicher und ein geheimer. Nur einer der Beteiligten besitzt dabei den geheimen Schlüssel. Damit andere ihm dennoch Daten verschlüsselt zuschicken können, gibt er den sogenannten „öffentlichen Schlüssel“ bekannt. Damit können Andere ihre Daten nach einer bestimmten Vorschrift verschlüsseln und ihm zusenden. Die Idee ist, dass aufgrund des verwendeten Verfahrens nur der Inhaber des geheimen Schlüssels in der Lage ist, die Verschlüsselung der Daten wieder aufzuheben. Der öffentliche Schlüssel reicht hierfür nicht aus. Hier spricht man von „asymmetrischen“ Verfahren.

Die Sicherheit der sogenannten „Telematik-Infrastruktur“, die zum Austausch und zur Speicherung medizinischer Daten dient, beruht im Kern auf Kryptographie, d.h. auf Verschlüsselung.

Für die virtuelle Patientenakte werden dabei aus technischer Sicht beide Verfahren, die asymmetrische und die symmetrische Verschlüsselung kombiniert[170]: Die medizinischen Daten werden mit einem symmetrischen Schlüssel verschlüsselt. Dieser Schlüssel selbst wird wiederum verschlüsselt und dann ebenfalls zentral gespeichert. Soll einem Anderen regulär Zugang gewährt werden, benötigt er natürlich den symmetrischen Schlüssel des Versicherten. Dafür wird der symmetrische Schlüssel ein weiteres Mal abgelegt aber (z.B. via Smartphone) neu verschlüsselt mit dem öffentlichen Schlüssel des Empfängers, so dass nun auch er ihn verwenden kann.

Entscheidend für die Sicherheit ist in jedem Fall dass der geheime Schlüssel geheim ist und bleibt und auch nicht anderweitig erraten oder herausbekommen werden kann. Denn jeder, der den Schlüssel besitzt, kann die Daten entschlüsseln. Hieraus ergeben sich sofort zwei

169 Siehe z.B. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: „Orientierungshilfe zum Einsatz kryptographischer Verfahren“ (2003)

170 Gematik GmbH: Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur (September 2020)

Schwachstellen, selbst wenn wir von einer großen Länge des Schlüssels ausgehen, der damit praktisch kaum zu „erraten“ ist.

Um auf die Daten zugreifen zu können, beispielsweise bei der Anzeige der Inhalte einer virtuellen Patientenakte, muss zum Einen auf dem verwendeten Gerät an irgendeiner Stelle der geheime Schlüssel gespeichert/vorhanden sein. Aufgrund der Gesetzgebung kann es sich bei dem Gerät um den PC zuhause, das Windows Tablet oder auch das Smartphone mit Google Android-Betriebssystem oder auch um alle drei Geräte handeln[171]. Zum Anderen liegen die Daten auf den Geräten in dem Moment unverschlüsselt vor. Kurz gesagt: Keines der Geräte darf gehackt werden.

Es ist aber davon auszugehen, dass es sich bei Angreifern auf eine medizinische Datenbank um staatliche oder in staatlichem Auftrag handelnde Akteure handelt oder/und um solche aus dem Bereich der Organisierten Kriminalität. Also um Angreifer, die hochprofessionell, kreativ und mit umfangreichen Ressourcen an Personal, Finanzmitteln und Ausstattung vorgehen.

Es ist kein Geheimnis, dass Akteure aus dem nachrichtendienstlichen Umfeld schon in der Vergangenheit in der Lage waren, Verschlüsselungen zu umgehen, z.B. indem sie sich Zugang zu mobilen Endgeräten verschafften. Wie oben genannt, sind Dokumente der CIA öffentlich geworden, aus denen klar hervorgeht, wie umfassend mobile Endgeräte durch professionelle Hacker gehackt werden können[172]. Hier sei auch an die Diskussionen und Berichterstattung rund um den „Bundes-Trojaner“ erinnert, sowie an die Enthüllungen des Hinweisgebers Edward Snowden[173]. Bekannt ist auch der Fall der kommerziellen Hacker-Software „Pegasus“ des Unternehmen „NSO Group“, mit der unter anderem Smartphones des Herstellers „Apple“ gehackt werden konnten, ohne dass dies für den Nutzer zu erkennen war[174], oder dass gewisse Staaten bei Grenzkontrollen gerne mal Spionagesoftware auf mobilen Geräten installieren[175].

Zudem ist bekannt, dass bereits in der Vergangenheit die Infrastruktur zur kryptographischen Absicherung, d.h. zur Verschlüsselung, nachrichtendienstlich unterwandert wurde. So berichtete die Tagesschau am 11.02.2020 unter dem Titel „CIA und BND hörten gemeinsam ab“ unter Verweis auf Medienberichte:
„*Der Bundesnachrichtendienst und der US-Auslandsgeheimdienst CIA haben nach Medienberichten mittels einer Verschlüsselungsfirma über Jahrzehnte hinweg mehr als 100 Staaten ausgespäht. Das bestätigten von führenden BND- und CIA-Mitarbeitern verfasste Akten, die das ZDF, die "Washington Post" und das Schweizer Fernsehen auswerteten. Den Berichten zufolge verließen sich Regierungen in aller Welt bei der Verschlüsselung ihrer Kommunikation auf die Schweizer Firma Crypto AG - im Unwissen darüber, dass diese seit 1970 in Besitz der CIA und des BND gewesen sei und die Geheimdienste in der Lage waren, die Verschlüsselung zu knacken.“*

Laut Washington Post[176] war neben dem Bundesnachrichtendienst und CIA auch die NSA beteiligt, wobei die CIA nach dem Ausscheiden des Bundesnachrichtendienstes Anfang der 1990er Jahre „*die deutschen Anteile übernahm und einfach weitermachte und die Crypto [AG] spionagetechnisch bis zum Verkauf 2018 weiternutzte*“, wobei sich die Relevanz

171 Sofern sie – nach aktuellem Stand – online registriert wurden.
172 z.B.: https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/ (zuletzt abgerufen: 08.02.2020)
173 s.u.
174 Siehe z.B. Alex Hern: „iPhones vulnerable to hacking tool for months, researchers say“, The Guardian, 20.12.2020 (https://www.theguardian.com/technology/2020/dec/20/iphones-vulnerable-to-hacking-tool-for-months-researchers-say , abgerufen 31.01.2021)
175 State Security Department of hte Republic of Lithuania/Defence Intelligence and Security Service: „National Threat Assessment 2021“, Vilnius (2021); S. 41ff
176 Greg Miller: „The intelligence coup of the century“, The Washington Post, 11.02.2020

kryptographischer Hardware durch die Prävalenz von Online-Verschlüsselungsverfahren ohnehin verringert habe. Grundsätzlich ist aber davon auszugehen, dass sich zum Einen die Aktivitäten nur auf andere Felder und Firmen verlagert haben und die Entwicklung von Methoden, um beispielsweise über das „Hacken“ von mobilen Endgeräten in den Besitz der privaten Schlüssel zu kommen[177]. Zum Anderen ist davon auszugehen, dass wohl nicht nur CIA und Bundesnachrichtendienst auf die Idee kommen können, Tarnfirmen zu betreiben und Verfahren der Kryptographie auf kreative Weise zu umgehen.

Eine logische Fortentwicklung mit Blick auf die virtuelle Patientenakte wäre beispielsweise die nachrichtendienstliche Unterwanderung oder Gründung von Firmen, die „ePA-Apps“, „Anwendungen des Versicherten“ oder Hardware wie die Konnektoren der „Telematik-Infrastruktur“ entwickeln[178].

Man muss davon ausgehen, dass Sicherheitsmaßnahmen und Verschlüsselung „auf dem Stand der Technik“ letztlich nicht ausreichen, um irreguläre Datenzugriffe durch Akteure aus dem nachrichtendienstlichen Bereich oder solchen, denen quasi-nachrichtendienstliche Mittel zur Verfügung stehen, ausschließen zu können.

Selbst in der Theorie[179] ist die Sicherheit klassischer Verschlüsselungsverfahren[180] nie absolut, sondern nur relativ zu dem Aufwand gegeben, den ein Angreifer betreiben will und kann. So verwendet beispielsweise ein weit verbreitetes asymmetrisches Verschlüsselungsverfahren, die ab 1978 entwickelte „RSA-Kryptographie“[181], eine Zahl als öffentlich kommunizierten Schlüssel, die sich aus dem Produkt zweier Primzahlen ergibt. Die theoretische Sicherheit des Verfahrens ergibt sich daraus, dass die Umkehrung der Rechnung, d.h. das Finden der beiden Primzahlen, deren Produkt die öffentlich bekannte Zahl ergibt, im Allgemeinen sehr rechenintensiv ist, besonders für große Zahlen.

Der zu erwartende Angreifer ist aber eben nicht ein jugendlicher Hacker an seinem Rechner im Kinderzimmer., sondern eine wohlorganisierte und hochprofessionelle Gruppe mit umfangreichen staatlichen Ressourcen. So wäre im ersten Schritt als einfachster Ansatz denkbar, dass zumindest für Schlüssel einer begrenzten Länge in den vergangenen 40 Jahren seit 1978 mithilfe leistungsfähiger Rechner und Netzwerke bereits eine Art umfangreiche Tabelle von Zahlen angelegt wurde, die als Produkt zweier Primzahlen berechnet wurden. Dann müsste der Angreifer im Idealfall die Rechnung nicht umkehren, sondern könnte zunächst einfach in der Tabelle nachschauen, ob die als Schlüssel dienende Zahl dort bereits enthalten ist. Dies ist umso realistischer, je kürzer der verwendete Schlüssel ist, d.h. je kleiner die als Schlüssel dienende Zahl ist, weshalb man tunlichst große Zahlen verwenden sollte.

Zudem ist seit Langem ein Algorithmus bekannt („Algorithmus nach Shor“), der prinzipiell in der Lage ist, das RSA-Verschlüsselungsverfahren effizient zu brechen, indem gezielt bestimmte Effekte quantenphysikalischer Systeme genutzt werden. Was sich für Manchen vielleicht wie Zukunftsmusik anhört, ist bereits Realität. So entwickeln und betreiben sowohl das Unternehmen IBM als auch das Unternehmen Google erste sog. „Quantencomputer“. Letzteres Unternehmen behauptet, mit seinem Quantensystem bereits die prinzipielle

177 Siehe z.B.: https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/ (zuletzt abgerufen: 08.02.2020)

178 Gematik GmbH: Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur (September 2020)

179 Oftmals ergeben sich Angriffspunkte durch Unvollkommenheiten der praktischen Realisierung.

180 „Klassisch“ meint hier Verfahren, die nicht, wie z.B. das BB84-Protokoll, Prinzipien der Quantenphysik nutzen.

181 Rivest/Shamir/Adleman: „A method for obtaining digital signatures and public-key cryptosystems“, Comm. ACM **21**, 120 (1978).

Überlegenheit über klassische Rechner demonstriert zu haben[182]. Weltweit wird intensiv an entsprechenden Systemen und ihrer Hochskalierung gearbeitet, in den USA ebenso wie in Russland[183], Europa[184] und anderen Weltregionen. Während in der öffentlichen Forschung noch an vergleichsweise kleinen Systemen gearbeitet wird, ist der Stand der Technik im nicht-öffentlichen Bereich naturgemäß unbekannt. Öffentlich bekannt ist aber, dass z.B. der US amerikanische Projektträger für nachrichtendienstliche Forschungsprojekte „IARPA“ sich intensiv mit dem Thema beschäftigt[185].

Dabei ist es keine Erleichterung, wollte man sich damit beruhigen, dass im besten Fall vielleicht noch einige Jahre vergehen mögen, bis hinreichend leistungsfähige Quantenrechner zur Verfügung stünden, oder dass es eines Tages noch sicherere Verschlüsselungsverfahren geben werde als heute: Sicherheit ist immer relativ und entsprechend der Ziele und Randbedingungen zu bewerten. Zum Beispiel mit Blick auf die erwartbare Dauer bis zum Brechen der Verschlüsselung relativ zur „Gültigkeitsdauer“ der betrachteten Daten.

Eine Verschlüsselung, deren „Haltbarkeitsdatum“ möglicherweise kürzer ist, als das der Relevanz der verschlüsselten Daten, ist faktisch nicht sicher. Das scheint mir hier aber der Fall zu sein.

Sensibilität, Intimität, dauerhafte Gültigkeit der Daten

Denn die hier betrachteten, personenbezogenen medizinischen Daten sind dauerhaft und unauslöschlich mit der betreffenden Person verbunden, ihre Relevanz ist je nach Lebensalter für Jahrzehnte gegeben und endet frühestens mit dem Tod. Sofern sich die Daten auf erbliche Merkmale beziehen, ist die Relevanz sogar noch für die nächste Generation gegeben. Demgegenüber stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Zuverlässigkeit von Prognosen zur Sicherheit kryptographischer Systeme fest: „*Grundlegende wissenschaftliche Fortschritte (entweder in Bezug auf Angriffsalgorithmen oder etwa die Entwicklung eines kryptographisch relevanten Quantencomputers) sind dagegen nicht vorherzusagen. Jede Vorhersage über einen Zeitraum von 6-7 Jahren hinaus ist schwierig, insbesondere bei asymmetrischen Verfahren, und selbst für diesen Zeitraum […] können sich die Prognosen aufgrund unvorhersehbarer Entwicklungen als falsch erweisen.*“[186]

Zu der Attraktivität dieses medizinischen Datensatzes trägt wesentlich bei, dass aufgrund der dauerhaften Relevanz der Daten das Anfertigen einer heimlichen Kopie des verschlüsselten Datensatzes problemlos zeitlich getrennt werden kann von seiner späteren Entschlüsselung. Die Entschlüsselung kann zu einem späteren Zeitpunkt erfolgen, wenn z.B. Verschlüsselungsverfahren, die nach dem aktuellen Stand der Technik als „sicher“ gelten, gebrochen werden können. Es „lohnt“ sich daher für Angreifer, große verschlüsselte Datensätze auch dann und „auf Vorrat“ zu erbeuten, wenn sie nicht unmittelbar entschlüsselt werden können. Und gerade medizinische Datensätze werden immer auch relevante Daten zu zukünftigen Personen des öffentlichen Lebens enthalten.

Die zeitlich begrenzte Sicherheit aktueller Verschlüsselungsverfahren ist nicht ausreichend, um die Risiken einer irregulären Datenaneignung und -verwendung von medizinischen Daten in zentralen Datenbanken auszugleichen. Das bedeutet, die einzigen dauerhaft wirksamen Sicherheitsmaßnahmen sind Datensparsamkeit durch das Vermeiden der Erzeugung sensibler Daten und in jedem Fall ihrer zentralen Speicherung wenn irgend möglich: „*Da ein*

182 E. Gibney: „Hello quantum world! Google publishes landmark quantum supremacy claim“, Nature **574**, 461-462 (2019)

183 Q. Schiermeier: „Russia joins race to make quantum dreams a reality“, Nature **577**, 14 (2020)

184 Ein Beispiel von vielen: „Quantum Valley Lower Saxony“ mit dem Ziel der Entwicklung eines skalierbaren Quantencomputer-Chips in Niedersachsen, www.qvls.de

185 Siehe z.B. https://www.iarpa.gov/index.php/research-programs/quantum-programs-at-iarpa

186 Bundesamt für Sicherheit in der Informationstechnik: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, BSI TR-02102-1, Version 2020-01 (2020), S. 16

Angreifer Daten speichern und später entschlüsseln kann, bleibt ein grundsätzliches Risiko für den langfristigen Schutz der Vertraulichkeit. […] Die Übertragung und die Speicherung vertraulicher Daten sollte auf das notwendige Maß beschränkt werden“.[187]

Es gibt keine Notwendigkeit für die Übertragung und Speicherung der medizinischen Daten der Bürgerinnen und Bürger in zentralen Datenbanken.

Ich habe nun bereits ziemlich oft behauptet, dass die personenbezogenen medizinischen Daten besonders sensible Daten sind. Stimmt das denn überhaupt? Wie steht es mit der oben behaupteten besonderen Sensibilität der personenbezogenen medizinischen Daten, die in der virtuellen „elektronischen Patientenakte“ auf die eine oder andere Weise zentral zugänglich sind?

Hier ist zunächst festzuhalten, dass im Gesetz als in der virtuellen Patientenakte zulässigerweise zu speichernde Daten unter anderem allgemein Daten über „Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte“ genannt sind. Eine inhaltliche Differenzierung, z.B. nach Art der Erkrankung oder Diagnose ist nicht vorgesehen, es wird lediglich die Forderung nach Sicherung der „semantischen und syntaktischen Interoperabilität“ erhoben.

Dies bedeutet, in die zentrale bzw. zentral zugängliche Sammlung personenbezogener medizinischer Daten können Daten im Zusammenhang mit Sportverletzungen oder Allergien ebenso aufgenommen werden wie Daten über Befunde, Diagnosen etc. im Zusammenhang mit sexuellen Störungen, Psychosen, Erbkrankheiten, Folgen von Vergewaltigungen und anderen Gewaltverbrechen, traumatischen Erlebnissen, Schwangerschaftsabbrüchen, Fehlgeburten, Depressionen, Verhaltens- und Angststörungen, Suizidversuchen, Suchtverhalten, sexuell übertragbaren Krankheiten, Wahnvorstellungen etc., sowie unter Umständen kontextuelle Informationen zum familiären oder kulturellen Umfeld oder persönlichen Wertvorstellungen und Persönlichkeitsmerkmale, soweit sie für Diagnose, Therapie oder Behandlung relevant sind. Weiterhin Daten zu verschriebenen Medikamenten (Medikationsplan) inklusive Psychopharmaka, aus denen auf die Diagnose und Persönlichkeitseigenschaften rückgeschlossen werden kann, wie z.B. Zwanghaftigkeit oder Neurotizismus, Depression, Schizophrenie, Geschlechtskrankheiten o.ä..

Medizinische Daten weisen im Vergleich zu anderen personenbezogenen, aber auch im Vergleich zu nicht personenbezogenen, besonderer Geheimhaltung unterliegenden Daten, einige signifikante Besonderheiten auf.

Die Relevanz von Daten wie beispielsweise Kreditkarteninformationen oder besonderer Geheimhaltung unterliegenden industriellen oder militärischen Plänen kann im Fall der Entdeckung eines „Datenlecks“ beeinflusst bzw. aufgehoben werden, z.B. durch Änderung der Datenzuordnung („Sperren der Kreditkarte“) oder Überarbeitung der betreffenden Pläne.

Bei medizinischen Daten funktioniert das nicht. Sie sind untrennbar und dauerhaft mit der Person oder den Personen verbunden, auf die sie sich beziehen. Medizinische Daten können im Fall eines „Datenlecks“ nicht im Nachhinein „gesperrt“ oder „unbrauchbar“ gemacht werden. Sie verlieren ihre Relevanz erst durch den Tod des Versicherten. Im Fall erblich bedingter Krankheiten nicht einmal dann. Der Schaden eines einmal entstandenen „Datenlecks“ ist nicht wieder gutzumachen. Im Fall erblich bedingter Krankheiten erstreckt sich dies auch auf zukünftige Generationen.

Medizinische Daten werden zudem in der Regel intimste Lebensbereiche berühren, und ihr Bekanntwerden zu schwerwiegenden, negativen sozialen und persönlichen Folgen führen, die eine freie Entfaltung der Persönlichkeit beeinträchtigen oder unmöglich machen. Tatsächlich kann die Kenntnis medizinischer Daten sogar gezielt dazu genutzt werden, durch Erpressung

187 Ebd.

oder Manipulation das Verhalten des/der Betroffenen entgegen seiner/ihrer originären Interessen zu lenken oder entscheidend zu beeinflussen. Wir werden weiter unten Beispiele kennenlernen.

Die Kombination von dauerhafter und unauflöslicher Relevanz medizinischer Daten und ihrer Intimität und damit Verwertbarkeit zur Verhaltenslenkung macht entsprechende Datensätze extrem attraktiv sowohl für Akteure aus dem Bereich der Organisierten Kriminalität als auch für extremistische politische und ausländische staatliche Akteure bzw. deren Geheimdienste[188].

Anders als die bisherige, durch Delokalisierung, Fragmentierung, Medienbrüche und isolierte Systeme[189] extrem sichere Speicherung und Nutzung medizinischer Daten, ist ein umfassender elektronischer, standardisierter und maschinell lesbarer Datensatz ein besonders lohnenswertes Ziel entsprechender Aktivitäten.

Eine Pseudonymisierung der Daten kann zudem durch persönlich zuzuordnende Inhalte der medizinischen Daten oder durch „vom Versicherten zur Verfügung gestellte Daten“ (z.B. aus Fitness-Apps), durch Metadaten, durch Zusammenführung mit anderen Datensätzen oder durch breit angelegte Angriffe auf mobile Endgeräte, mit denen zukünftig auf die Datenbank zugegriffen werden kann, aufgelöst werden.

Damit sind kopierte medizinische Datensätze hervorragend geeignet für eine „geheimdienstliche Vorratsdatenspeicherung“ durch ausländische staatliche Stellen und andere Akteure, die illegitimen Einfluss entweder einzeln auf zukünftige Personen des öffentlichen Lebens oder statistisch auf gesellschaftliche Prozesse wie demokratische Wahlen nehmen wollen.

Angriffe auf medizinische Datensammlungen

Nun werden Sie vielleicht kritisch einwenden: Mal langsam, wenn personenbezogene medizinische Daten angeblich so attraktive Angriffsziele sind - müssten entsprechende Angriffe dann nicht schon erfolgt sein? Also zum Beispiel in anderen Staaten die bereits zentrale Sammlungen bzw. Zugriffsmöglichkeiten über mit dem Internet verbundene Netzwerke haben?

Genau das ist der Fall.

Bereits im Februar 2015 erfolgte in den USA ein erfolgreichen Hackerangriff auf den US Krankenversicherer „Anthem“, der zu Zugriffen Daten von 80 Millionen Menschen führte[190]. Am 10. September 2015, ein Jahr vor den Präsidentschaftswahlen in den USA, berichtete die Zeitung „USA Today“ unter der Überschrift „10 Millionen Excellus Gesundheitskunden von Cyberattacke betroffen“ über eine ganze Reihe von Angriffen auf die personenbezogenen Daten bei Krankenkassen[191]: „*Excellus […] teilt mit, dass Daten von mehr als 10 Millionen seiner Kunden […] möglicherweise Ziel eines Angriffs im Jahr 2013 waren. […] Kriminelle Angriffe auf Computersysteme im Gesundheitswesen sind seit 2010 um 125 % gestiegen und sind inzwischen der häufigste Fall von Verletzungen der Datensicherheit [data breaches] […].*

188 Siehe z.B. A. E. Fotyga: „Report on EU strategic communication to counteract propaganda against it by third parties“, A8-0290/2016 (14.10.2016)

189 Vgl. dazu: Bundesgesundheitsministerium: „*Die Soft- und Hardware in Arztpraxen und Krankenhäusern sind meist inselartig umgesetzt. […] Mit dem DVG werden die Grundlagen […] geschaffen, so dass Informationen künftig leichter, schneller und auf Basis internationaler Standards ausgetauscht werden können.*“ (www.bundesgesundheitsministerium.de/digitale-versorgung-gesetz.html)

190 Siehe z.B. „Hackerangriff auf zweitgrössten US-Krankenversicherer Anthem“, 05.02.2015, Neue Zürcher Zeitung (https://www.nzz.ch/wirtschaft/newsticker/hackerangriff-auf-zweitgroessten-us-krankenversicherer-anthem-1.18476712 , zuletzt abgerufen 02.02.2021); nach Darstellung des dort zitierten Firmenchefs gebe es allerdings „*keine Hinweise, dass […] medizinische Daten betroffen sind.*“

191 Elizabeth Weise: „Cyber breach hits 10 million Excellus healthcare customers“, USA TODAY, 10. September 2015; online: https://eu.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-shield/72018150/ (zuletzt abgerufen: 10.02.2020)

Firmen im Bereich des Gesundheitswesens sind dabei besonders verlockende Ziele für Cyberangriffe, da ihre Dateien große Mengen persönlicher Daten der Nutzer enthalten. […] Excellus BlueCross BlueShield ist die dritte große Datenfirma im Bereich des Gesundheitswesens, die im vergangenen Jahr gehackt [breached] wurde. Bei Premera, einer […] Krankenversicherung in Alaska, waren bis zu 11 Millionen ihrer Kunden von einem Datenleck im März betroffen. Anthem gab im Februar bekannt, dass möglicherweise bis zu 80 Millionen ihrer Kundendatensätze gehackt wurden. […] Einbrüche in Datensysteme sind im Gesundheitswesen oft schlimmer, als es zunächst den Anschein hat, meint Arun Vishwanath, Professor an der Universität Buffalo […]. ‚In diesen Fällen, wenn man einmal Zugang zum Netzwerk hat, hört man nicht einfach auf, man versucht, so viel wie möglich zu erwischen. Das heißt, es wird nicht nur BlueCross[192] betreffen, sondern auch ihre Zulieferer, mit ihnen verbundenen Arztpraxen und mit ihnen vernetzte Partner [accessible affiliates] im ganzen Land.‘ "

Am 16. Januar 2018 berichtet der norwegische Staatssender NRK unter der Überschrift „Verdacht auf fremden Staat als Urheber von Hackerangriff"[193] über einen Angriff auf die medizinischen Daten von 2,8 Millionen norwegischer Bürgerinnen und Bürger: „*Professionelle Hacker sind in der vergangenen Woche in das Netzwerk des Gesundheitsverbundes Helse Sør-Øst eingedrungen. Der Polizei-Sicherheitsdienst[194] vermutet jetzt einen möglichen nachrichtendienstlichen Hintergrund eines fremden Staates. Helse Sør-Øst ist der größte Gesundheitsverbund des Landes, dem mehr als 2,8 Millionen Norwegerinnen und Norweger angehören. Alle sensiblen personenbezogenen Informationen jedes Einzelnen sind auf Servern gespeichert. Am Montag, dem 8. Januar wurde Helse Sør-Øst auf ungewöhnliche Aktivitäten im Zusammenhang mit den IT-Systemen in der Region hingewiesen. […] Die Art, wie der Einbruch in das System durchgeführt wurde, deutet auf hoch professionelle Täter hin.*"

Die genannte Zahl von 2,8 Millionen Norwegerinnen und Norwegern entspricht über 50 % der Gesamtbevölkerung.

In der Folgeberichterstattung von NRK wird knapp ein Jahr später unter dem Titel: „Bereitschaftspläne, Patientendaten und Forschungsergebnisse möglicherweise bei Helse Sør-Øst gestohlen"[195] über die Einstellung der vergeblichen Ermittlungsbemühungen berichtet: „*Der Sicherheitsdienst der Polizei stellt die Ermittlungen nach dem Urheber des Dateneinbruchs bei Helse Sør-Øst ein. Den Eindringlingen ist es gelungen, sich vollen Administratorzugang zum Netzwerk des Gesundheitsverbundes zu verschaffen. […] ‚Für uns ist der Fall jetzt abgeschlossen‘, teilt die Leiterein des PST, Benedicte Bjørnland NRK mit. ‚Sie hatten potentiell Zugang zum gesamten Netzwerk. Das bedeutet Patientendaten, Notfallpläne und Forschungsdaten. Wir können aber nicht mit Sicherheit sagen, dass entsprechende Daten abgeflossen sind.‘ […] Der Angriff soll über einen externen Server, der mit dem Internet verbunden war, erfolgt sein. Danach ist es gelungen, Zugang zu internen Servern zu erhalten und sich Administratorberechtigungen zu verschaffen. Die Ermittlungen haben gezeigt, dass die Eindringlinge ein besonderes Interesse an einem Lehrprogramm über das Netzwerk des Gesundheitsverbundes hatten, aber der Sicherheitsdienst der Polizei weiß nicht, wer hinter dem Angriff steckt. ‚Es gibt Grund zu der Annahme, dass es sich um einen professionellen Akteur handelt, aber wir können nicht mit Sicherheit sagen, dass es ein staatlicher Akteur ist‘, sagt Bjørnland.*"

192 Blue Cross / Blue Shield: Ein Verbund von Krankenversicherungen in den USA, der knapp 1/3 aller Bürgerinnen und Bürger versichert.

193 Kaja Staude Mikalsen: „Mistenker at en fremmed stat står bak hackerangrep" (NRK, 16./18.01.2018; online: https://www.nrk.no/osloogviken/mistenker-at-en-fremmed-stat-star-bak-hackerangrep-1.13869547, zuletzt abgerufen: 10.02.2020)

194 Politiets sikkerhetstjeneste (PST): Norwegischer Inlandsnachrichtendienst, u.a. zuständig für Spionageabwehr.

195 Maria Knoph Vigsnæs: „Beredskapplaner, pasientinformasjon og forskning kan være stjålet fra Helse Sør-Øst" (NRK, 05.12.2018, online: https://www.nrk.no/norge/beredskapsplaner_-pasientinformasjon-og-forskning-kan-vaere-stjalet-fra-helse-sor-ost-1.14325823, zuletzt abgerufen: 10.02.2020)

Hier wird ein weiterer Umstand deutlich, der eine zentrale bzw. zentral via Internet zugängliche Sammlung personenbezogener medizinischer Daten wie eingangs genannt zu einem ausgesprochenen attraktiven Angriffsziel macht: Es ist im allgemeinen praktisch unmöglich, den Urheber eines Dateneinbruchs festzustellen. Er bleibt anonym und muss faktische keine Konsequenzen befürchten. Praktisch. Und gefährlich.

Ein anderes Beispiel bezieht sich auf besonders sensible medizinische Daten aus dem Bereich der Psychotherapie, die dann für Erpressungen verwendet wurden. Wie unter anderem das Ärzteblatt[196], das Online-Portal „Heise“[197] und die Zeitung „The Guardian“[198] berichten, kam es in Finnland 2018/19 zur irregulären Aneignung intimer personenbezogener Daten bei einer Kette von Psychotherapiepraxen. Betroffen seien personenbezogene medizinische Daten von bis zu 40.000 Patienten, darunter auch Tagebücher und Diagnosen, auch von Minderjährigen. Zahlreiche Patienten hätten seitdem Erpressungsschreiben per E-Mail erhalten mit der Aufforderung, durch Zahlung einer Summe von 200 Euro eine Veröffentlichung ihrer Daten abzuwenden.
Gleichzeitig kursiere im Darknet jedoch bereits ein Datensatz von zehn Gigabyte, der 2.000 Patienten betreffe, d.h. hier ist es nachweislich bereits zu einer Datenproliferation gekommen. Laut „The Guardian“ wird von offizieller Seite generell von einer Kommunikation mit den Erpressern abgeraten, da „*die Daten mit hoher Wahrscheinlichkeit bereits anderweitig weitergegeben wurden*“[199].

Dieser Vorfall unterstreicht zum Einen, dass zentrale Sammlungen intimster medizinische Daten bereits heute im Visier von Hackern und einer professionell agierenden, kriminellen Schattenwirtschaft sind; zum Anderen, dass von einer unkontrollierten Verbreitung einmal irregulär angeeigneter Daten auszugehen ist (man kann sie nicht wie ein gestohlenes Gemälde „zurückgeben“ oder „zurückholen“, da immer noch eine gleichwertige Kopie existieren kann); zum Dritten, dass sie zur Manipulation des freien Willens verwendet werden wie hier zur Erpressung; zum Vierten, dass man auch nicht einfach argumentieren kann, man müsse die Daten einfach „sicher genug“ aufbewahren, und dies sei ja im Fall der virtuellen „elektronischen Patientenakte“ oder der Datensammlung des Forschungsdatenzentrums sicher der Fall und unproblematisch: Wie die finnische Seite „yle.fi“ berichtet, hat noch im Frühjahr 2019 eine externe Prüfung der IT im Rahmen einer Firmenübernahme der Praxiskette keine kritischen Punkte hinsichtlich der Datensicherheit gefunden[200] [201].
Dabei ist es kein Trost, wenn man feststellt, dass genau so ein Angriff auf die virtuelle Patientenakte vielleicht weniger erfolgreich sein würde. Denn der Angriff auf die virtuelle Patientenakte wird nicht genau so stattfinden wie im genannten Beispiel, sondern er wird auf die virtuelle Patientenakte und die konkrete Telematik-Infrastruktur angepasst sein[202] .

196 „Vertrauliche Psychotherapiedaten in Finnland gehackt“, Ärzteblatt, 27. 10. 2020 (online unter: https://www.aerzteblatt.de/nachrichten/117742/Vertrauliche-Psychotherapiedaten-in-Finnland-gehackt, zuletzt abgerufen am 28.10.2020)

197 Martin Holland: „Psychotherapeuten gehackt: Finnische Patienten und Praxen werden erpresst“, heise.de, 27.10.2020 (https://www.heise.de/news/Finnland-Psychotherapeuten-gehackt-Erpressung-von-Praxis-und-Patienten-4939533.html, zuletzt abgerufen am 28.10.2020)

198 „‘Shocking‘ hack of psychotherapy records in Finlanf affects thousands“, afp/The Guardian, 26.10.2020 (online unter: https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland, zuletzt abgerufen am 28.10.2020)

199 Ebd.

200 „Vastaamo board fires CEO, says he kept data breach secret for year and a half“, YLE, 26.10.2020 (online unter: https://yle.fi/uutiset/news/vastaamo_board_fires_ceo_says_he_kept_data_breach_secret_for_year_and_a_half/11614603, zuletzt abgerufen Oktober 2020)

201 Vgl. auch die eingangs zitierte Feststellung von Perrow.

202 Vgl. z.B. T. Maus: „Hinweise auf mögliche Verwundbarkeiten der Medizin-Telematik“, c‘t, 17.01.2020 (https://www.heise.de/ct/artikel/Hinweise-auf-moegliche-Verwundbarkeiten-der-Medizin-Telematik-4635791.html, zuletzt abgerufen Februar 2021), sowie z.T. die Artikelreihe „Digitales Infektionsrisiko“, c‘t 2021, Heft 1, S. 60ff.

Zielgerichtete, erfolgreiche Angriffe auf personenbezogene medizinische Daten und deren manipulative Verwendung sind offensichtlich eine Realität[203].

Hackerangriffe: Umfang, Zuordnung, Ziele

Gleichzeitig sind die bekannten Angriffe möglicherweise nur die Spitze des Eisbergs, unter der es außerdem noch unentdeckte Fälle und ganz „normale“ Datenlecks durch menschliches Versagen oder Datendiebstähle als „Beifang“ von Cyberkriminalität gibt, bei denen sich der Abnehmer der gestohlenen Daten nicht einmal die Mühe eines ausgefeilten Angriffs machen muss.

Auch hierfür sollen nur einige Beispiele genannt werden.

Eine aktuelle Meldung belegt, dass selbst Hacker-Angriffe, die scheinbar „nur“ die Verschlüsselung von Daten in erpresserischer Absicht zum Ziel haben, tatsächlich ohne Weiteres auch einen Abfluss der Daten involvieren können: So meldete die Tagesschau unter der Überschrift „Passdaten von 12.000 Deutschen im Netz“ am 18.09.2020, dass im Rahmen eines Hacker-Angriffs mit Verschlüsselungssoftware (ransomware) auf die argentinische Einwanderungsbehörde Daten nicht nur lokal verschlüsselt, sondern, wie sich zeigte, auch kopiert wurden, da sie im Internet veröffentlicht wurden, als auf Lösegeldforderungen nicht eingegangen wurde[204]. Dabei wird hier wiederum festgestellt: „Wer hinter dem Angriff steckt, ist unklar“. Und tatsächlich gibt es Cyberkriminelle, die im DarkNet eine eigene Enthüllungsplattform betreiben, auf der verschlüsselte Daten veröffentlicht werden, wenn kein Geld gezahlt wird („Erpressung-as-a-service“)[205]. Auch das Lagebild „Cybercrime 2020“ des Bundeskriminalamts berichtet über das Abfließen von Daten („Exfiltration“) im Rahmen von Verschlüsselungsattacken und dem weiteren und immer professionellern Ausbau krimineller Dienstleistungen, die weitere Attacken begünstigt („Cybercrime-as-a-service“)[206].

Schon im Mai 2017 wurde im Rahmen eines globalen Cyberangriffs mit dem Kryptotrojaner[207] „WannaCry“ auch das Gesundheitsnetzwerk N3 des britischen staatlichen Gesundheitssystems NHS infiziert, wobei in der Folge 34 Krankenhausverbünde („trusts“) und 595 angeschlossene Arztpraxen (general practitioners practises) akut betroffen waren[208]. Dem offiziellen Untersuchungsbericht zufolge wurde kein Lösegeld bezahlt[209], was impliziert, dass alle Systeme neu aufgesetzt wurden. Bezüglich der Frage eines Datenabflusses schreibt der Bericht: „*NHS England teilte uns mit, dass, wenn die WannaCry-Attacke zu Patientenschäden oder Datenverlusten geführt hätte, es erwarten würde, dass die Verbünde (trusts) entsprechende Fälle über bestehende Berichtswege berichten würden […]. NHS Digital teilte uns mit, dass die Analyse des WannaCry Kryptotrojaners darauf hinweise, dass der Cyberangriff nicht darauf ausgerichtet gewesen sei, auf Daten zuzugreifen oder diese zu stehlen, obwohl man nicht mit Sicherheit sagen könne, dass dies nicht der Fall sei.*“

Über einen ähnlichen Angriff mithilfe eines Kryptotrojaners auf das Rechenzentrum der Justus-Liebig-Universität Gießen im Dezember 2019, von dem in geringem Maß auch die Uniklinik betroffen war, berichtete unter anderem die Gießener Allgemeine Zeitung am 18./19.12.2019[210]. Das zweifellos professionell geführte Rechenzentrum musste komplett vom

203 Vgl. z.B. auch den Cyberangriff mit Kryptotrojanern auf die große US-Krankenhauskette Universal Health Services Ende 2020 (https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254, zuletzt abgerufen März 2021).

204 Vgl. auch: „Cybercrime – Bundeslagebild 2019“, Bundeskriminalamt , Wiesbaden (2020), S. 23 („double extortion“).

205 vgl. z.B. J. Schmidt: „Ist der König wirklich tot?“, c‘t 2021, Heft 5, S. 45 .

206 „Cybercrime – Bundeslagebild 2020“, Bundeskriminalamt , Wiesbaden (2021), z.B. S. 22ff.

207 Ein Schadprogramm, das die Daten auf einem Datenträger verschlüsselt und typischerweise anbietet, dem Betroffenen nach Zahlung eines Lösegeldes den Schlüssel zukommen zu lassen.

208 National Audit Office: „Investigation: WannaCry cyber attack and the NHS“, 25. April 2018

209 Ebd., S. 8

Internet getrennt werden und wieder neu aufgesetzt werden. Laut Berichterstattung handelte es sich bei dem Kryptotrojaner um die Schadsoftware mit dem Namen Ryuk.

Im Jahr 2020 wurde das Universitätsklinikum Düsseldorf Ziel eines erfolgreichen Hackerangriffs, in dem sich die Angreifer im Netzwerk der Klinik bewegen konnten[211], und der ab dem 10. September 2020 – wohl aufgrund einer Verschlüsselung der Daten - zu so weitreichenden Störungen des IT-Systems führte, dass das Klinikum zum Teil komplett von der Notfallversorgung abgemeldet werden musste[212]. Ende 2020 wurde in den USA die große Krankenhauskette „Universal Health Services“ mit mehr als 400 Häusern Ziel eines erfolgreichen Hackerangriffs mit Kryptotrojanern[213]. Im Mai 2021 wurde das zentralisierte irische Gesundheitssystem „HSE“ Ziel eines erfolgreichen Hackerangriffs mit Verschlüsselungssoftware[214]. Aufgrund des erforderlichen Herunterfahrens der Systeme mussten Krankenhäuser ihre Arbeit einschränken und konnten z.T. keine Bestrahlungstherapie mehr anbieten[215]. Die Irish Times meldete zudem, dass das HSE untersuche „*in welchem Ausmaß elektronische Patientenakten [patients‘ medical records] Teil der ‚kompromittierten‘ Daten waren*“, entsprechend der vermuteten Strategie der „*double extortion*“[216]

Die Relevanz dieser Beispiele besteht darin, dass das Aktivieren eines Kryptotrojaners unter Umständen eben nur den letzten, sichtbaren Schritt eines aus drei Schritten bestehenden Angriffs darstellt[217] [218]: Im ersten Schritt erfolgt die Öffnung des Systems z.B. über die Schadsoftware Emotet[219] mittels „Spearfishing“[220], im zweiten Schritt wird das System ausgespäht (beispielsweise Passwörter, Inhalte von Datenträgern etc.)[221] und erst im dritten

210 „Nach Hackerangriff auf Uni Gießen: Nun hat Schadsoftware einen Namen – Noch Schlimmeres verhindert?“, Gießener Allgemeine Zeitung, 19.12.2019 (online: https://www.giessener-allgemeine.de/giessen/nach-hackerangriff-giesse-schadsoftware-einen-namen-noch-schlimmeres-verhindert-zr-13281448.html, zuletzt abgerufen: 10.02.2020)

211 „Hackerangriff auf Uniklinik Düsseldorf: War der Ausfall der IT-Systeme vermeidbar?“, Interview mit R. Trost im Medical Tribune, 06.10.2020 (https://www.medical-tribune.de/meinung-und-dialog/artikel/hackerangriff-auf-uniklinik-duesseldorf-war-der-ausfall-der-it-systeme-vermeidbar/, zuletzt abgerufen 02.02.2021)

212 „IT-Ausfall an der Uniklinik Düsseldorf“, Pressemitteilung vom 17.09.2020 (https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/it-ausfall-an-der-uniklinik-duesseldorf, zuletzt abgerufen 02.02.2021)

213 K. Collier: „Major hospital system hit with cyberattack, potentially largest in U.S. history“, NBC News, 28.09.2020 (https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254, zuletzt abgerufen März 2021).

214 „Hackerangriff auf Gesundheitssystem in Irland“, Deutsche Welle, 14.05.2021 (online https://www.dw.com/de/hackerangriff-auf-gesundheitssystem-in-irland/a-57528161, zuletzt abgerufen Mai 2021))

215 J. Power: „HSE examines extent to which patient records were compromised in cyberattack“, The Irish Times, 16. Mai 2021 (online unter https://www.irishtimes.com/news/health/hse-examines-extent-to-which-patient-records-were-compromised-in-cyberattack-1.4566421, zuletzt abgerufen Mai 2021)

216 Ebd.

217 Thomas Hungenberg: „Emotet, Trickbot, Ryuk – ein explosiver Malware-Cocktail“, https://m.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html, zuletzt abgerufen: 10.02.2020

218 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/infos/20190114_Update_BSI_Schadsoftware_Emotet.html, zuletzt abgerufen: 10.02.2020

219 Zwar meldete das Bundeskriminalamt in einer Pressemitteilung vom 27.01.2021 bezüglich Emotet einen wichtigen Ermittlungserfolg und die erfolgreiche Zerschlagung der verwendeten Infrastruktur im Rahmen einer international koordinierten Aktion (BKA: „*Infrastruktur der Emotet-Schadsoftware zerschlagen*“, Pressemitteilung vom 27. Januar 2021), andererseits wird erwartet, dass die Lücke schnell von Anderen gefüllt werden wird, vgl. z.B. J. Schmidt: „Ist der König wirklich tot?“, c‘t 2021, Heft 5, S. 45 .

220 Verbreiten von Schadsoftware mittels Links oder Anhängen in/an möglichst glaubwürdigen E-Mails.

Schritt erfolgt die Verschlüsselung des Datenträgers verbunden mit der Aufforderung zur Zahlung eines Lösegeldes, typischerweise in „Bitcoin“.

So geschehen z.B. im Jahr 2021 in der beschaulichen Gemeinde Østre Toten in Südnorwegen. Dort gelangten Hacker ins interne Netzwerk, verschlüsselten alle Daten und löschten alle Sicherheitskopien[222], betroffen waren auch Patientendaten. Es folgten Lösegeldforderungen, im März tauchten personenbezogene Daten aus dem Angriff schließlich im Darknet auf[223].

Die Verschlüsselung kann offensichtlich mehrere Gründe haben. Zum Einen kann es wirklich darum gehen, Geld zu erpressen, entweder um sich persönlich zu bereichern, oder um eine „Schwarzgeldkasse“ zu füllen, aus der weitere Hackingoperationen finanziert werden. So schreibt der amerikanische Sonderermittler Robert Mueller in seinem Untersuchungsbericht über russische Einflussnahme auf die US amerikanischen Präsidentschaftswahlen[224]: „*Eine Abteilung [des russischen Geheimdienstes GRU], beispielsweise, entwickelte spezielle Schadprogramme („malware“), während eine andere Abteilung umfangreiche Spearfishing-Kampagnen durchführte. [geschwärzt] eine Bitcoin-Gewinnungsoperation, um Bitcoins zu erzeugen, die zum Kauf von Computer Infrastruktur verwendet wurden, die für Hacking-Aktivitäten verwendet wurde*.“

Daneben kann die auf die Ausspäh-Phase folgende Verschlüsselung gleichzeitig auch ein eleganter Weg sein, die Spuren von irregulären Datenzugriffen zu verwischen, indem beispielsweise Log-Dateien, wie die für Zugriffe auf die virtuelle Patientenakte vorgesehene Protokoll-Datei, nicht mehr zugänglich sind.

Insbesondere im Fall von Rechenzentren ist ja, anders als bei Privatpersonen, davon auszugehen, dass praktisch nie ein Lösegeld gezahlt wird, sondern ausreichend Ressourcen und Fachkenntnis vorhanden sind, um das System zu löschen und wieder neu aufzusetzen, z.B. anhand von älteren Sicherungskopien. Und selbst bei Zahlung eines Lösegeldes gibt es keine Notwendigkeit für den Täter, den Schlüssel zur Aufhebung der Entschlüsselung wirklich zu liefern.

Zu diesen Beispielen gezielter Einbrüche und Attacken mit unbekannter Dunkelziffer kommen noch die Fälle organisatorischen und „menschlichen Versagens“, die bequem irreguläre Datenzugriffe auch auf medizinische Datensammlungen ermöglichen. Auch hier sollen beispielhaft einige Fälle genannt werden.

Irreguläre Datenzugriffe „aus Versehen“

So berichtete der norwegische Staatssender im Mai 2017, knapp ein Jahr vor dem oben genannten, gezielten Angriff auf den Gesundheitsverbund Helse Sør-Øst, über einen Fall organisatorischen Versagens im Rahmen einer Kooperation mit dem amerikanischen IT-

221 Die Website der Tagesschau meldete am 27.02.2020 zur Angriffswelle mit der Software Emotet:*„[…] Die Datenschutzbeauftragen von Bund und Ländern zählten im vergangenen Jahr bundesweit eine dreistellige Zahl von erfolgreichen Angriffen mithilfe der Schadsoftware Emotet, heißt es auf Anfrage. Dabei seien Behördendaten, Personal- oder Krankendaten oder andere sensible Informationen abgeflossen. […] Sicherheitsexperte Nohl glaubt, dass die Täter im Ausland sitzen. "Von dem, was wir über Emotet wissen, scheint es eine mittelgroße Gruppe in Russland ansässiger Hacker, aber auch Geschäftsleute zu sein", sagt er.*“ (https://www.tagesschau.de/investigativ/kontraste/hackerangriffe-oeffentliche-einrichtungen-101.html , zuletzt abgerufen 27.02.2020)

222 H. Solbakken: „Sensitiv pasientinformasjon kan være på avveie etter dataangrep“, 10.01.2021, NRK (https://www.nrk.no/innlandet/ostre-toten-kommune-angrepet-av-hackere-_-pasientinformasjon-og-helsedata-kan-vaere-pa-avveie-1.15321398, zuletzt abgerufen April 2021)

223 V. Haagensen, A. Løberg: „Kommunen kan få kjempegebyr etter at de ble hacka“, 08.04.2021, NRK (https://www.nrk.no/innlandet/ostre-toten-kan-bade-bli-erstatningsansvarlig-og-fa-gebyr-etter-at-persondata-kom-pa-avveie-1.15446840, zuletzt abgerufen April 2021)

224 Robert S. Mueller: „Report On The Investigation Into Russian Interference In The 2016 Presidential Election“, Washington, März 2019; S. 43f.

Dienstleister DXC, dessen Ausmaß nur dank interner Hinweisgeber öffentlich geworden ist, während die (später zurückgetretenen) Verantwortlichen den Vorfall lbzw. sein Ausmaß leugneten. Unter dem Titel „ Helse Sør-Øst räumt ein, dass ausländische IT-Mitarbeiter Zugriff auf auf sensible Patientendaten hatten“ berichten die Autoren[225]:
„*Informationen, die NRK vorliegen, zeigen, dass in den vergangenen Wochen etliche IT-Mitarbeiter in Asien und Osteuropa Zugang und erweiterte Rechte im Datensystem von Helse Sør-Øst hatten. Sie hatten die Möglichkeit, medizinische Daten von 2,8 Millionen Norwegern herunterzuladen. […] Eine große Zahl IT-Mitarbeiter aus Asien und Ost-Europa hatte seit Mitte März die Möglichkeit, die Patientenakten von 2,8 Millionen Norwegerinnen und Norwegern zu kopieren, ohne Spuren zu hinterlassen. NRK vorliegende Informationen zeigen, dass sie auf diese Weise die Möglichkeit hatten, sich intimste Informationen über halb Norwegen anzueignen, wie Geburten und Abtreibungen, psychische Probleme, Krebserkrankungen, Medikamenteneinnahme, Geschlechtskrankheiten und Ähnliches. […] Wie die Quellen NRK mitteilten, konnten die ausländischen IT-Mitarbeiter dabei auch weiteren Externen Zugriff erteilen, ohne dass es möglich gewesen wäre, dies nachzuvollziehen. [...]*“.

In einem weiteren NRK-Artikel, der im Oktober 2017 veröffentlicht wurde, berichten die Autoren unter dem Titel „IT-Mitarbeiter in Israel hatten Zugriff auf Patientendaten bei Helse Sør-Øst“ darüber, dass sich zudem herausstellte, dass Subunternehmer eines eigenen Tochterunternehmens in Israel Fernzugriff auf Datensysteme in Krankenhäusern des Gesundheitsverbunds hatten, und dass diese Entdeckung nicht öffentlich gemacht worden sei[226].

In Deutschland wiederum berichtete u.a. die Tagesschau über die Sicherheitsrisiken von Arztpraxen, die sich aufgrund des E-Health-Gesetzes zwangsweise mit dem Internet verbinden mussten. Unter der Überschrift „Sensible Patientendaten in Gefahr“ heißt es dort[227]:
„*Zahlreiche Arztpraxen sind nach Recherchen von NDR und "Süddeutscher Zeitung" (SZ) nur ungenügend vor Hacker-Angriffen geschützt. Das geht aus einem vertraulichen Papier der Gesellschaft "Gematik" hervor, das Panorama 3 und der SZ vorliegt. Die Gematik gehört mehrheitlich dem Bund. […] Hacker können sich daher leicht Zugang zu den sensiblen Gesundheitsdaten von Millionen Patienten verschaffen. Dass das Problem nicht nur theoretischer Natur ist, berichten Ärzte, die auf ihren Praxis-Computern bereits Schadsoftware zum Abgreifen von Daten gefunden haben. […] Es [das Gesundheitsministerium] erklärt auf Anfrage, dass die "IT-Netze in den Praxen nicht Teil der Telematikinfrastruktur" seien. Die sichere Installation sei Aufgabe der Praxen zusammen mit den von ihnen beauftragten Dienstleistern. Die vom Bundesgesundheitsminister beauftragte Gesellschaft Gematik ergänzt, sie habe keine Vertragsbeziehung zu den Dienstleistern und könne "daher nicht direkt auf die Dienstleister Einfluss nehmen". […] “* Dies bedeutet, dass der Gesetzgeber sich nicht vollumfänglich für die erst infolge der Gesetzgebung entstehenden Sicherheitslücken verantwortlich sieht.

Als Beispiel für ganz normale Fehler hier zwei Beispiele aus ganz verschiedenen Kontexten: Im Jahr 2019 wurde öffentlich, dass aufgezeichnete Anrufe bei einer medizinischen Hotline in Schweden versehentlich per Internet frei zugänglich waren - insgesamt 170 000 Stunden oder

225 Anne Cecilie Remen und Line Tomter: „Helse Sør-Øst: Innrømmer at utenlandske IT-arbeidere fikk tilgang til sensitive pasientdata“ (NRK, 03.05.2017, online: https://www.nrk.no/norge/helse-sor-ost_-innrommer-at-utenlandske-it-arbeidere-har-hatt-tilgang-til-pasientjournaler-1.13478443, zuletzt abgerufen 13.02.2020)

226 Anne Cecilie Remen und Line Tomter: „IT-arbeidere i Israel har hatt tilgang til pasientdata i Helse Sør-Øst“ (NRK, 24.10.2017, online unter: https://www.nrk.no/norge/it-arbeidere-i-israel-har-hatt-tilgang-til-pasientinfo-i-helse-sor-ost-1.13745814 , zuletzt abgerufen 13.02.2020)

227 Jasmin Klofta, Katrin Kampling und Anne Ruprecht: Sensible Patientendaten in Gefahr“ (ARD/NDR, 12.11.2019, online: https://www.tagesschau.de/investigativ/panorama/patientendaten-105.html , zuletzt abgerufen 13.02.2020)

2,7 Millionen Bürgeranrufe zu mediznischen Fragen als Audiodateien, die bis in das Jahr 2013 zurückreichten[228]. Im Januar 2020 wurde publik, dass Firmendaten und Millionen Kundendaten des Autovermieters Buchbinder aufgrund eines falsch konfigurierten, für Sicherheitskopien verwendeten Servers völlig ungeschützt per Internet zugänglich waren[229]; so etwas sollte nicht passieren, kann es aber. Aufgefallen war dies einer IT-Sicherheitsfirma, die den Zugang mithilfe eines automatisierten Scan-Programms entdeckt hatte.

Um die bisher genannten Beispiele in die Gesamtlage einzuordnen, ist der sog. „Breach Level Index“ der Firma Gemalto hilfreich, der die bekannten Fälle irreguläre Datenzugriffe (data breaches) aufschlüsselt[230]. Für das erste Halbjahr 2018 beispielsweise ist der Gesundheitssektor mit Abstand der am häufigsten betroffene Sektor (27 % der betrachteten irregulären Zugriffe, gefolgt vom Finanzsektor mit 14 %).

Darauf, dass sich die Situation auch später nicht gebessert hat, weist die vom „US Department of Health – Office for Civil Rights“ veröffentlichte Übersicht über irreguläre Datenaneignungen medizinischer Daten in den USA hin[231]. Allein für die ersten drei Monate des Jahres 2020, den Zeitraum vom 01.01.2020 bis 01.03.2020, werden dort 56 Vorfälle unter der Bezeichnung „Hacking/IT incident“ aufgeführt, die die Daten von 1.145.355 Personen betrafen. Darunter wird für die Daten von 281.448 Personen von der Behörde als Speicherort der angeeigneten Daten „Network Server“ angegeben, für die restlichen im Wesentlichen „Email“. Für denselben Zeitraum werden zwei Vorfälle mit insgesamt 7.302 Betroffenen aufgeführt, für die als Speicherort „Electronic Medical Record“ angegeben ist (allein im Zeitraum 16.12.2019 – 31.12.2019 gab es in dieser „Kategorie“ vier Vorfälle, die 22.216 Personen betrafen, darunter 12.000 Patienten einer psychologischen/psychiatrischen Einrichtung).

Zusammenfassend lässt sich festhalten, dass sowohl gezielte Angriffe auf medizinische Datensammlungen in professionellen, mit dem Internet verbundenen Netzwerken Realität und erfolgreich sind, als auch von der Möglichkeit ihre irregulären, möglicherweise verschleierten Aneignung ausgegangen werden muss.

Dabei ist insbesondere davon auszugehen, dass beispielsweise Programme zum automatisierten Aufspüren irregulärer Zugriffswege („scannen“) nicht nur der genannten Flensburger IT-Sicherheitsfirma zur Verfügung stehen, sondern insbesondere auch professionellen internationalen Akteuren mit kriminellem oder nachrichtendienstlichem Hintergrund.

gematik GmbH: kein Korrektiv von Fehlentwicklungen

Tatsächlich ist es im Licht dieser Beobachtungen und der des folgenden Teils sehr fraglich, dass die „Gesellschaft für Telematik“, die vom Gesetzgeber mit der sicheren Implementierung der Telematikinfrastruktur auch im Zusammenhang mit einer virtuellen Patientenakte beauftragt ist, diese Aufgabe objektiv überhaupt erfüllen kann, oder ob es sich hier nicht vielmehr um eine unmögliche Aufgabe handelt.

Da der Bund vertreten durch das Bundesministerium für Gesundheit mit 51 % der Geschäftsanteile Haupteigner der „Gesellschaft für Telematik“ ist, ist zudem der Staat gleichzeitig Auftraggeber und Auftragnehmer. Dadurch steht zu befürchten, dass die Unabhängigkeit der gematik GmbH dahingehend beeinträchtigt ist, dass sie nicht als Korrektiv

228 „Schweden: 2,7 Millionen Patienten-Anrufe ungeschützt im Netz“, Februar 2019, heise online
229 Jens Tönnesmann: „Unterwegs mit Wagen 417711“, (ZEIT, 22.01.2020)
230 https://safenet.gemalto.com/resources/data-protection/breach-level-index-2018-h1/ , zuletzt abgerufen 13.02.2020
231 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (zuletzt abgerufen: 06.03.2020)

einer unmöglichen Beauftragung fungieren und eine solche weder öffentlich machen noch verweigern kann.

Dabei sollen weder die Professionalität noch der gute Wille der Mitarbeiterinnen und Mitarbeiter der gematik GmbH in Zweifel gezogen werden. Ganz bestimmt ist beispielsweise das Design und die Betreuung eines Systems zum sicheren, d.h. Ende-zu-Ende verschlüsselten Email-Versand z.B. zwischen Krankenhäusern und Arztpraxen[232] im Prinzip absolut sinnvoll und auch sicher gut durchdacht und nach bestem Wissen und Gewissen durchgeführt.

Die Mitarbeiterinnen und Mitarbeiter der gematik GmbH geben sich innerhalb des ihnen vorgegebenen Rahmens ganz ohne Zweifel große Mühe, sorgfältig zu arbeiten und Risiken im Kleinen möglichst gut minimieren. Aber den vorgegebenen Rahmen können sie nicht verlassen und nie die Grundfrage stellen, ob das System an sich sinnvoll ist. Sie können gewissermaßen versuchen, den Weg zu ebnen und Stolperfallen zu vermeiden - aber die Marschrichtung gibt wie immer der Hauptanteilseigner vor, auch wenn die Richtung in die Katastrophe führt.

Und der Hauptanteilseigner ist der Bund[233], vertreten durch den Bundesgesundheitsminister mit seiner Agenda eine zentralen Speicherung von Patientendaten. Vor diesem Hintergrund kann die gematik GmbH nicht mehr leisten als Schadensbegrenzung.

Konsequenterweise werden im Whitepaper „Datenschutz und Informationssicherheit“ der gematik GmbH auch nur „banale“ Risiken wie eine verlorenen oder gestohlenen Versichertenkarte bzw. Heilberufeausweises betrachtet. Nicht aber das gesamtgesellschaftlich deutlich relevantere Risiko eines gezielten und umfassenden, hochprofessionellen Angriffs.

Was das für Angreifer sind, und was in ihren Köpfen vorgeht, werden wir uns im folgenden Teil näher anschauen.

232 Gematik GmbH: Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur (September 2020)
233 Ebd.

Teil 2 – Na und? Wen interessieren schon meine Daten?

Vielleicht denken Sie sich: „Ja, ok, kann schon passieren, dass jemand Anderes theoretisch an meine Daten kommen kann – na und? Ich habe nichts zu verbergen, und außerdem interessiert doch eh keinen, was ich gestern um 9 Uhr 36 gemacht oder mit wem ich mich wann worüber unterhalten habe. Es ist doch wie am FKK-Strand: Wenn alle nackt dastehen, braucht sich keiner zu schämen. Totale Ehrlichkeit - ist doch super. Wo ist das Problem?“

Nun, dagegen könnte man einwenden, dass nicht jeder und jede, die ihre Privatsphäre nicht mit Anderen teilen möchte, etwas zu verbergen hat. Vielleicht möchte sie einfach ihre Privatsphäre nicht mit Anderen teilen. Punkt.

Die eigentliche Antwort ist aber eine andere: Es geht nicht um Voyeurismus oder um Scham, nicht darum, dass jemand aus Neugier oder abseitiger Veranlagung Ihnen mithilfe Ihrer Daten ständig „hinterherspioniert“.

Um das eigentliche Problem besser zu verstehen, treten wir eine kurze Zeitreise an. Eine Zeitreise zum Internet des frühen 20. Jahrhunderts: dem Radio.

War die Nutzung von Funkwellen zunächst eine interessante technische Spielerei und faszinierende „Spielwiese“ für Nerds und Ingenieure, entwickelte sich ab Mitte der 1920er Jahre ein allgemeiner Rundfunk, mit verschiedenen Unterhaltungssendern und vor allem mit Funkempfängern - Radios - in zahlreichen Haushalten.

Das Radio war teuer, aber es war ein Versprechen von Freiheit. Man konnte ja nicht nur seinen lokalen oder nationalen Sender hören, sondern auch Sender aus andern Ländern, Radio Wien, Paris, London, Prag. Man konnte auf einmal „live“ dabei sein, wenn der Reichspräsident, der englische König oder Albert Einstein eine Rundfunkansprache hielt. Das Radio stieß auf einmal in jeder Kleinstadt das Tor zur Welt auf, durch das man direkt und ungefiltert miterleben konnte, was in anderen Teilen des Landes und der Welt geschah. Sofort und ohne erst auf den Bericht oder Kommentar in der Zeitung warten zu müssen. Wahnsinn – echte Basisdemokratie, was für ein Potential...

...erkannten die Nationalsozialisten unter ihrem Propagandaminister Joseph Goebbels. Als eine der ersten Amtshandlungen kurbelten sie ab 1933 die Produktion von Billigradios an, den sogenannten „Volksempfängern“. Damit sollte sichergestellt werden, dass auch wirklich jede und jeder erreicht werden konnte. Die Erfindung des Radios war für die gesteuerte Propaganda ein Geschenk des Himmels.

Ab sofort konnten Goebbels und vor allem Hitler Millionen von Menschen direkt erreichen. Ihre Halbwahrheiten, Lügen und selbst ihre bizarrsten Wahnvorstellungen konnten direkt und unkommentiert in die „gute Stube“ jedes Hauses, in jede Familie transportiert werden. Ohne lästige Vermittler wie Zeitungen oder Journalisten. Ohne Instanzen, die Mittel und Zeit hätten, kritisch nachzufragen, die Lügen der Nazis als Lügen zu entlarven und ihre Mitbürger vor dem Weg in die Katastrophe zu warnen.

Die Nazis hatten jedoch ein Problem. Zwar konnte Hitler jetzt zu Millionen Deutschen direkt sprechen und ihnen erzählen was er wollte. Aber wie konnte man verhindern, dass die Leute sich auch aus anderen Quellen informierten? Und Hitler konnte zwar die Menschen quasi persönlich erreichen – aber er sagte ja allen dasselbe. Wie konnte man sicherstellen, dass die Botschaft trotzdem bei allen wirkte?

Den ersten Teil des Problems - lästige Fakten und unabhängige Information - lösten die Nazis bekanntlich dadurch, dass unabhängige Medien zunächst so laut wie frei erfunden als „Lügenpresse“ verunglimpft wurden, um erst ihre Vertrauensstellung zu sabotieren und sie dann ohne große Gegenwehr „gleichschalten“ zu können. Wo dies nicht möglich war, zum Beispiel bei internationalen Radiosendern, wurden alle zu Außenseitern erklärt und mit drakonischen Strafen belegt, die sie hörten. Parallel dazu lief der Aufbau eines Systems von „Blockwarten“ und Spitzeln, das wie die Fäden einen Schimmelpilzes die gesamte Gesellschaft durchzog, um eine unauffällige aber permanente Überwachung und Beobachtung zu erreichen. Wobei auch die ausgefeilteste Überwachung natürlich noch ärgerliche Begrenzungen hatte, da selbst der eifrigste Sptzel oder brutalste GeStaPo-Beamte den Leuten nicht wirklich hinter die Stirn schauen und kein wirklich umfassendes Profil der Leute erstellen konnte.

Den zweiten Teils des Problems – dieselbe Botschaft für Millionen verschiedener Menschen – versuchten die Nazis dadurch zu lösen, dass sie die Vorstellungen und Werte der Menschen möglichst einheitlich formten durch eine permanente „weltanschauliche Erziehung“.

Tatsächlich war diese Unterdrückung der Individualität lange Zeit das Erkennungszeichen totalitärer Systeme, vom Nationalsozialismus bis zum Kommunismus[234]: Da die manipulativen Botschaften der Partei zwar zu allen transportiert aber nicht individuell angepasst werden konnten, musste man notgedrungen die Individuen anpassen und vereinheitlichen. Am besten zu einem Zeitpunkt, zu dem die Menschen noch möglichst ohne Erfahrung aber gutgläubig sind, d.h. mit diversen Jugendorganisationen beginnend im frühesten Kindesalter.

Aber es ist völlig klar: Das war extrem aufwändig und umständlich, eigentlich eher eine Notlösung. Dass sie trotzdem leidlich funktionierte und halbwegs erfolgreich war, bezeugt ein sechsjähriger Weltkrieg mit rund 70 Millionen Toten und ungezählten Verletzen und Verstümmelten an Leib und Seele.

Und trotzdem war das Vorgehen natürlich ineffektiv, und es blieb lange ein ungelöstes Problem: Wie konnte man Propaganda und Manipulation individuell anpassen? Wie sollte man herausfinden, wie die Leute wirklich „ticken“? Wie kann man eine subtile, individuell oder wenigstens nach Persönlichkeitstyp maßgeschneiderte Manipulation realisieren, wie gleichzeitig viele verschiedene Menschen unauffällig mit verschiedenen, individuell angepassten Botschaften erreichen?

Wonach Nazis und Kommunisten lange so intensiv wie vergeblich suchten, worüber sie sich verzweifelt den Kopf zerbrachen – fast hundert Jahre später können Unternehmen und Netzwerke wie Google, Facebook und VKontakte mit Fug und Recht von sich behaupten: „Es ist uns gelungen.“

Und die Nazis des 21. Jahrhunderts wie die großen und kleinen Diktatoren und Autokraten danken es ihnen.

234 Tatsächlich sind vielleicht weder Zwang zur Einheitlichkeit noch die Anwendung von Gewalt die sichersten Erkennungszeichen totalitärer Systeme. Abgesehen von Psychopathen, die in totalitären Regimen sicher etwas besser gedeihen, war beides wohl oft eher lästiges Mittel zum Zweck. Das eigentliche Erkennungsmerkmal totalitärer Ideologien scheinen mir eher die Abschaffung der Privatsphäre und der Versuch der „Kontrolle des Willens und Wollens“ zu sein. D.h. sie stellen ihre jeweilige Ideologie unangreifbar über alles, ignorieren lästige Fakten und meinen, dass alle nur fest genug an die Ziele der Ideologie glauben müssten und sprechen den Menschen das Recht auf einen freien Willen und auf freie Entfaltung der Persönlichkeit ab.

Aber dazu später. Hier wollen wir zunächst einmal kritisch zwei Frage aufwerfen. Offensichtlich benötigt man für die individuell angepasste Gestaltung von Botschaften ja erst einmal vernünftige Persönlichkeitsprofile der Leute. Nun wäre es vielleicht theoretisch denkbar, dass sich staatliche Akteure dafür in Datenbanken mit persönlichen Daten einhacken. Aber mal ehrlich: Das ist doch extrem aufwändig, bei all den Sicherheitsmaßnahmen...

Staatliche Akteure, Einfluss-nahme auf Prozesse der Demokratie

Haben staatliche Akteure wie Geheim- und Nachrichtendienste tatsächlich die Ressourcen und Möglichkeiten, derart ausgefeilte Hackerangriffe durchzuführen? Können die das? Und selbst wenn, gibt es irgendeinen ernsthaften Hinweis, dass seitens staatlicher oder nicht-staatlicher Akteure die Möglichkeit und der Wille bestehen, demokratisch Prozesse wie beispielsweise Wahlen in manipulativer Weise zu beeinflussen?

Ja und ja, beides ist der Fall.

So beschreibt das Bundesamt für Verfassungsschutz in seiner 2018 veröffentlichten Publikation „Nachrichtendienstlich gesteuerte Cyberangriffe“ zusammenfassend und anhand von Beispielen Aktivitäten russischer, chinesischer (sowie iranischer) Akteure[235]:

„*Die Nachrichtendienste der Russischen Föderation nutzen in großem Umfang Cyberangriffe zur Informationsbeschaffung, Desinformation und Propaganda. Russische nachrichtendienstliche Cyberangriffe gegen deutsche Ziele sind meist Teil mehrjähriger, international ausgerichteter Cyberspionage-Operationen. Sie finden im Rahmen einer umfassenden taktischen und strategischen Informationsgewinnung statt.*

Diese Angriffskampagnen zeichnen sich aus durch

• eine hohe technische Qualifikation,

• starke finanzielle Ressourcen und

• außergewöhnliche Operativ- und Auswerterfähigkeiten.

[…]

Russische Nachrichtendienste verüben in diesen Fällen[236] Cyberangriffe unter dem Deckmantel vermeintlicher Hacktivistengruppen. Solche Operationen stellen mitunter eine Ergänzung der Spionage um Sabotage und deren Flankierung mit gezielten Desinformationskampagnen und Propaganda dar.

[...]

Bei der Analyse staatlich gesteuerter Cyberangriffe aus Russland zeigt sich deutlich die hohe informationstechnische Qualität der Angriffsoperationen, z. B. durch Ausnutzung noch unbekannter Sicherheitslücken. Sichtbar wird auch die Finanzstärke der Täter. Zudem lassen Art und globaler Umfang der Operationen immense Operativ- und Auswertekapazitäten erkennen. Offensichtlich ist Russland in der Lage, auf außenpolitische Kräfteverschiebungen und auf „störend“ empfundene Ereignisse kurzfristig zu reagieren. Dabei wird auch vor Sabotageakten nicht zurückgeschreckt.

Die festgestellten Angriffe erfolgen meist sehr zielgerichtet und passgenau. Die Erfolgswahrscheinlichkeit und damit das Schadpotenzial russischer Angriffe er scheint

235 „Nachrichtendienstlich gesteuerte Cyberangriffe“, Bundesamt für Verfassungsschutz, Köln, Mai 2018.
236 Gemeint sind hier sog. „False Flag“-Operationen.

aufgrund des erkennbar hohen Ressourcenansatzes, der Hochwertigkeit der Ziele, der herausgehobenen technischen Fähigkeiten und des guten Social Engineerings hoch.

[...]

Chinesische Cyberangriffskampagnen […] Die Möglichkeit zur Durchführung längerfristiger und strategisch angelegter Spionageangriffe im Cyberbereich gehört zum Fähigkeitenportfolio chinesischer Nachrichtendienste. Die dortigen Kapazitäten umfassen nicht nur die Möglichkeit, komplexe, international angelegte Angriffe zielgerichtet durchzuführen, sondern diese auch parallel mit einer Vielzahl von einzelnen Opfern zu betreiben.

[…]

Die Bandbreite chinesischer Cybergruppierungen reicht von kriminellen Strukturen über sogenannte patriotische Hacker bis hin zu Unternehmern, Regierungs- und Militärakteuren. Die Interessen und Ziele der einzelnen Gruppierungen überschneiden sich, so dass eine konkrete Zuschreibung teilweise schwierig ist.

Die Kampagnen werden meist über mehrere Jahre fortgeführt. Folgende technische Charakteristika sind dabei typisch:

• Schwer zu detektierendes Vorgehen bei der Zustellung der Malware, der Netzwerkinfiltration, -erkundung und -ausbreitung sowie der Datenausleitung.

• Die Fähigkeit, innerhalb weniger Stunden vom eingeschränkten Zugriff auf ein Netzwerksegment einen vollumfänglichen Zugriff auf das gesamte (Unternehmens-) Netzwerk zu erlangen.

• Etablierung möglichst vielfältiger Zugangsmöglichkeiten zum infiltrierten Netzwerk, um die Verbindung zum System auch bei Gegenmaßnahmen des Opfers lange aufrecht zu erhalten.

• Kombination von gezielten Spear-Phishing-E-Mails und Massenversand von E-Mails, um eine Verschleierung der echten Ziele zu erreichen.

• Sofortige Ausnutzung von bekannt gewordenen und bisher nicht angegriffenen Schwachstellen mittels Zero-Day-Exploits. So wurde im Juli 2015 bei WikiLeaks eine bislang unbekannte Sicherheitslücke veröffentlicht. Bereits wenige Tage danach wurde diese Schwachstelle von mutmaßlich chinesischen Stellen dazu ausgenutzt, um deutsche Wirtschaftsunternehmen anzugreifen.

• Verwischen von „digitalen Spuren“, um eine forensische Analyse von Vorfällen zu erschweren oder unmöglich zu machen.

• Vorgehen nach dem sogenannten „Staubsaugerprinzip“. Dabei werden alle verfügbaren Daten ohne vorweggenommene Selektion extrahiert.

[…]

Derzeit richten sich die Cyberangriffe der Gruppe gezielt gegen IT Service Provider, vor allem Cloud-Dienstleister, um von dort aus in die oft besser geschützten Systeme der Kunden zu gelangen. Das Vorgehen wird als „Operation Cloud Hopper“ bezeichnet.

[…]

Der Rückgang der mutmaßlich chinesischen APT[237]-Angriffe auf westliche Ziele in den letzten Jahren war international sichtbar. Die Aufdeckung der „Operation Cloud Hopper“ in der

237 APT: Advanced Persistent Threat

jüngsten Vergangenheit zeigt jedoch, dass chinesische APT-Gruppen noch immer aktiv Cyberspionage betreiben. Dabei ist ein immer anspruchsvolleres Vorgehen erkennbar, was die Detektion derartiger Cyberangriffe erschwert.

Waren die Cyberangriffe mutmaßlich chinesischen Ursprungs bis zum Jahr 2016 in Deutschland rückläufig, konnte allerdings zuletzt eine Zunahme sichtbarer Angriffsoperationen verzeichnet werden.

[…]

Das Gefährdungspotenzial iranischer Cyberangriffe hat sich in den letzten Jahren signifikant erhöht."

Die vom Bundesamt für Verfassungsschutz angeführten Beispiele umfassen dabei u.a. den Angriff auf die interne Kommunikation des Bundestags 2015, das US Democratic National Committee („Demokraten") im Vorfeld der US Präsidentschaftswahlen, die OSZE, die Welt-Doping-Agentur WADA, politische Parteien und Industrieunternehmen.

Die im Bericht genannte „Operation Cloud Hopper" bzw. ihr Ausmaß fand dabei einen besonders intensiven Widerhall in der öffentlichen Berichterstattung. So schreibt die Zeitschrift „Forbes" Anfang 2020 unter dem Titel „5 zentrale Lektionen aus dem Cloud Hopper Mega-Hack"[238]:

„*Im Dezember 2019 hat die US Regierung Haftbefehle gegen zwei chinesische Hacker ausgestellt, die angeblich an einer mehrjährigen Kampagne beteiligt waren, die das Ziel verfolgte, in die Systeme von Firmen einzudringen, die Daten und Anwendungen ihrer Kunden mittels Clouds verwalten. [...] Die „Cloud Hopper", die vor ihrer Entdeckung mehrere Jahre lang aktiv waren, haben Berichten zufolge mindestens ein Dutzend Dienstleister angegriffen, u.a. IBM und DXC Technology in den USA und CGI in Kanada. Fanden sie Schwachstellen, so nutzten sie diese, um sich über die Netzwerke verschiedener Kunden hinwegzubewegen und dabei geistiges Eigentum, Sicherheitsfreigaben und andere Daten zu stehlen.*"

Bei der Firma DXC handelt es sich um den oben erwähnten Dienstleister des gehackten norwegischen Gesundheitsverbundes Helse Sør-Øst. IBM wiederum ist der Dienstleister der Techniker Krankenkasse und anderer Krankenversicherungen für den Betrieb und die Verwaltung einer virtuellen Patientenakte.

Die Nachrichtenagentur Reuters berichtete zuvor[239]: „*Große Firmen, von IBM über Hewlett Packard Enerprise bis Fujitsu wurden zum Opfer einer Invasion durch chinesische Cyberspione. […] Angriffswellen auf die Opfer nahmen ihren Ausgang von diesen sechs [Fujitsu, Tata Consultancy Services, NTT Data, Dimension Data, Computer Sciences Corporation, DXC Technology] plus HPE und IBM: ihre Kunden. […] NTT Data, Dimension Data, Tata Consultancy Services, Fujitsu und IBM lehnten einen Kommentar ab. IBM hatte zuvor angegeben [said previously], dass sie keine Hinweise darauf hätte, dass sensible Firmendaten durch die Attacken kompromittiert worden seien.*".

Weitere Hinweise auf und Beispiele für die Möglichkeiten und Ressourcen von Geheimdiensten sind durch die Veröffentlichungen des früheren CIA- und NSA-Mitarbeiters

238 Martin Giles; „5 Key Security Lessons From The Cloud Hopper Mega Hack", Forbes, 03.01.2020 (online: https://www.forbes.com/sites/martingiles/2020/01/03/cloud-computing-security-cloud-hopper/ , zuletzt abgerufen 13.02.2020)

239 Jack Stubbs, Joseph Menn und Christopher Bing: „Inside the West's failed fight against China's ‚Cloud Hopper' hackers" (Reuters, 26. Juni 2019)

Edward Snowden bekannt geworden[240]: „*Mit PRISM konnte die NSA routinemäßig Daten von Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL und Apple sammeln, darunter E-Mails, Fotos, Video- und Audio-Chats, Webbrowsing-Inhalte, Anfragen an Suchmaschinen und alle anderen Daten, die in ihren Clouds gespeichert waren […]. Upstream Collection [...] war noch invasiver. Es ermöglichte die routinemäßige Datensammlung unmittelbar aus der Internetinfrastruktur des privaten Sektors aus den Switches und Routern, die den weltweiten Internetverkehr über Satelliten im Orbit und die am Meeresboden verlegten Breitband-Glasfaserkabel abwickeln. Diese Datensammlung wurde von der Special Source Operations Unit der NSA (SSO) betrieben, die geheime Gerätschaften zum Anzapfen von Kabeln baute und sie auf der ganzen Welt in den unternehmenseigenen Einrichtungen der entgegenkommenden Internet-Service-Provider unterbrachte. Zusammen sorgten PRISM […] und Upstream Collection […] dafür, dass weltweit Informationen, ob sie gespeichert oder übermittelt wurden, überwacht werden konnten. […] Genau genommen durchläuft Deine [Website-]Anfrage einige schwarze Server, die übereinandergestapelt sind und zusammen ungefähr die Größe eines Bücherregals mit vier Regalbrettern haben. Sie sind in allen [mit den USA] verbündeten Ländern in besonderen Räumen der Gebäude großer privatwirtschaftlicher Telekommunikationsunternehmen installiert […]. Sie enthalten zwei entscheidende Werkzeuge. Das erste, TURMOIL genannt, […] fertigt eine Kopie der durchlaufenden Daten an. Das zweite namens TURBINE […] manipuliert aktiv den Nutzer. Wenn TURMOIL [anhand von Selektoren] den Internetverkehr als verdächtig einstuft, gibt es ihn an TURBINE weiter, das die Anfrage auf Server der NSA umleitet. Dort entscheiden Algorithmen, welche Exploits – Schadprogramme – die Behörde gegen Nutzer einsetzt. […] Diese ausgewählten Exploits werden dann wieder an TURBINE geschickt […]. Die schleust sie zurück in den Kanal des Internetverkehrs und liefert sie dem Nutzer zusammen mit der gewünschten Website. Das Endergebnis: Du bekommst den gesamten gewünschten Inhalt zusammen mit der unerwünschten Überwachung, und alles geschieht in weniger als 686 Millisekunden. Du weißt nichts davon. Wenn sich die Exploits dann auf Deinem Computer befinden, hat die NSA nicht nur Zugang zu Deinen Metadaten, sondern auch zu Deinen Daten. [...]*“

Für die Russische Föderation ist ein ähnliches Überwachungssysteme bekannt: „SORM“[241]. Seine Anfänge gehen in die Zeit der Sowjetunion zurück, in den vergangenen Jahren wurde es intensiv ausgebaut[242]. Es ist u.a. in der Lage, individuelle Nutzerprofile zu erstellen und „Soziale Netzwerke“ auszulesen, und es beinhaltet die Installation staatlicher „Black Boxes“ unbekannter Funktionalität bei Internet-Anbietern in der Russischen Föderation[243]. Auch für das stark regulierte „chinesische Internet“ darf man ähnliche Überwachungssysteme annehmen.

Generell ist davon auszugehen, dass diese oder ähnliche Möglichkeiten bei verschiedenen Geheimdiensten logischerweise auch heute bestehen, und dass sie letztlich auch z.B. Zugriffe auf virtuelle „elektronische Patientenakten“ über das Internet mittels PCs oder mobilen Endgeräten betreffen werden.

Eine weitere Möglichkeit für irreguläre Zugriffe auf digitale Datensammlungen sind ausgefeilte, mehrstufige Angriffe, die reguläre Updates und Wartungszugriffe als Vehikel für die Implementierung von Schadsoftware verwenden, über die dann wiederum auf Server und

240 Edward Snowden: „Permanent Record“, Verlag S. Fischer, Frankfurt am Main (2019), S. 284ff.
241 Mitunter als „PRISM on steroids“ bezeichnet.
242 V. Wingerter: „Staatliche Regulierung des Internets in Russland“, Tagungsband des 17. Deutschen IT-Sicherheitskongresses des BSI, Tagungsband, S. 229ff. (2021)
243 Ebd.

Daten zugegriffen und Datensätze kopiert werden können. Ein eindrucksvolles Beispiel ist hier ein breit angelegter Hackerangriff Ende 2020, der „SolarWinds-Vorfall“. Dabei wurden über reguläre Updates zehntausende von Servern gehackt, er betraf in den USA zahlreiche Ministerien und Regierungseinrichtungen[244] [245] [246] bis hin zu Abteilungen des „Department of Energy“, die für die militärische Atomwaffenforschung zuständig sind[247]. Auch hier wird man den Betroffenen sicher nicht unterstellen können, dass sie hinsichtlich ihrer Sicherheitsvorkehrungen einfach zu nachlässig gewesen seien. Im Gegenteil dürfen wir annehmen, dass die Sicherheitsvorkehrungen „auf dem aktuellen Stand der Technik“ waren.

Dieser verheerende Angriff, der russischen Hackern zugeschrieben wird, wurde wenig später noch überboten durch den „Exchange-Hack“, der im März 2021 bekannt wurde[248] [249]. Bei diesem Hacker-Angriff, der einer chinesischen Hackergruppe zugeschrieben wird und der auch mehrere Bundesbehörden betrifft[250], wurde eine Sicherheitslücke des „Microsoft Exchange Servers“ ausgenutzt, einer Serversoftware, die z.B. hinter weit verbreiteten Email-Programmen wie „MS Outlook“ steht. Als bekanntgegeben wurde, dass Microsoft die Sicherheitslücke in absehbarer Zeit schließen werde, wurden von den Hackern weltweit *alle* ans Internet angeschlossenen Microsoft Exchange Server gescannt und automatisiert „Backdoors“ installiert, die durch das Sicherheitsupdate nicht entfernt werden und den späteren Zugriff auf die Server erlauben[251]. Dabei dürfte es um hunderte Millionen Betroffene gehen[252]. Sie benutzen MS Outlook? Dann wurden Sie wahrscheinlich gehackt. Vielleicht haben Ihre Freunde und Kollegen unter Ihrem Namen bereits automatisiert gefälschte Mails mit Schadsoftware und vertrauensvoll auf Links zu infektiösen Websites erhalten.

Der IT-Sicherheitsexperte Jürgen Schmidt stellt fest: „*Hier jetzt sehen wir auf einmal staatliche Hacker, die Hunderttausende von Systemen ‚ownen‘, und die im Wesentlichen uns vor Augen führen, dass unser System, wie wir Sicherheit machen, nämlich, dass wir Sicherheitslücken finden und die dann so schnell wie möglich patchen [schließen], im Prinzip eigentlich gar nicht funktioniert. Und ich frage mich: Was kommt da eigentlich als Nächstes?*“[253]

Andere, eher „klassische“ Möglichkeiten für irreguläre Zugriffswege auf digitale Datensammlungen mit geheimdienstlichen Mitteln sind beispielsweise die Gründung von Tarnfirmen als Dienstleister oder das Einschleusen, Manipulieren, Bestechen oder Erpressen von Mitarbeitern, idealerweise mit Administratorrechten.

---

244 „Hackerangriff erschüttert USA“, Deutsche Welle, 18.12.2020 (www.dw.com/de/hackernagriff-erschüttert-usa/a-55990457 , zuletzt abgerufen 15.01.2021)

245 „US-Regierung bestätigt Hackerangriffe“, Tagesschau, 14.12.2020 (www.tagesschau.de/ausland/amerika/cyberangriff-usa-ministerien-101.html , zuletzt abgerufen 15.01.2021)

246 „US-Behörde warnt vor ‚ernster Gefahr‘“, Tagesschau, 18.12.2020 (www.tagesschau.de/ausland/usa-cyberangriff-101.html , zuletzt abgerufen 15.01.2021)

247 A. Meiritz: „Umfassende Angriffe auf US-Sicherheitsapparat: Hacker haben wohl auch Atomwaffenbehörde attackiert“, Handelsblatt (17.12.2020)

248 M. Muth: „Opfer im Cyberkrieg“, Süddeutsche Zeitung (12.03.2021)

249 J. Schmidt: „Exchange Lücken: BSI ruft ‚IT-Bedrohungslage rot‘ aus“, 09.03.2021, heise online (https://www.heise.de/news/Exchange-Luecken-BSI-ruft-IT-Bedrohungslage-rot-aus-5075457.html, zuletzt abgerufen März 2021).

250 Ebd.

251 #heiseshow: ‚IT Bedrohungslage rot‘ - Was es mit dem Exchange Hack auf sich hat“, https://www.youtube.com/watch?v=Q7RJxaiQk18, zuletzt abgerufen März 2021)

252 Im Jahr 2015 wurde die Zahl der Outlook-Nutzer mit 400 Millionen angegeben (F. Kalenda; „Aktualisierte Microsoft-Statisikseite erwähnt 1,2 Milliarden Office-Nutzer“, ZDNet, 30.09.2015, https://www.zdnet.de/88247826/aktualisierte-microsoft-statistikseite-erwaehnt-12-miliarden-offoce-nutzer/ , zuletzt abgerufen März 2021)

253 Ebd.

Hinsichtlich geheimdienstlicher Aktivitäten allgemein schätzt das Bundesamt für Verfassungsschutz neben technischen Angriffspunkten die Bedeutung menschlicher Quellen bzw. Einfallstore[254]: *„Bei der Spionage gegen Deutschland bilden die „klassischen" Spionagemittel, wie z. B. der Einsatz menschlicher Quellen, nach wie vor eine wichtige Handlungsoption.*"

Wie funktioniert die Anwerbung „menschlicher Quellen"? Das zeigt sehr schön ein Beispiel aus dem Lagebild 2021 der litauischen Sicherheitsdienste[255]: Ein litauischer IT-Administrator reist zur feucht-fröhlichen Geburtstagsfeier eines Freundes in das benachbarte Belarus und lernt dort ein Mädchen kennen, das ihm besondere Aufmerksamkeit widmet. Nachdem reichlich Alkohol geflossen ist, nimmt sie ihn mit in ihre Wohnung, und der Abend nimmt im Weiteren einen Verlauf, den er für den Familienvater besser nicht hätte nehmen sollen. Mit dem Ergebnis, das er sich am nächsten Tag in einem Auto mit zwei Geheimdienstmitarbeitern wiederfindet, die ihm kompromittierende Bilder der vergangenen Nacht präsentieren und drohen, sie seiner Frau zu schicken. Sie würden aber darauf und auch auf eine (fingierte) Strafanzeige verzichten, wenn mit ihnen zusammenarbeite und z.B. die Daten kopiere, auf die er Zugriff habe. Wobei neben der Peitsche ganz klassisch noch das Zuckerbrot folgt: Er schade ja niemandem und könne sich so sogar noch etwas dazuverdienen...

Der Punkt ist dabei nun nicht, dass der - mit dem russischen vermutlich eng verbundene - belarusische Geheimdienst KGB eine „Honigfalle" inszeniert, um die Zielperson anschließend mit kompromittierendem Material zu erpressen und zur Kooperation zu zwingen. Die Botschaft ist: IT-Administratoren sind heute das, was im Kalten Krieg des 20. Jahrhunderts Kernwaffen-Experten und „Atom-Physiker" waren. Also mit hohem Aufwand ausgespähte Zielpersonen geheimdienstlicher Tätigkeit. Zentrale Sammlungen personenbezogener Daten entsprechen eben dem hoch angereicherten Spaltmaterial, das jeder haben will, der an einer „Digitalen Atombombe" für den Cyberraum bastelt. Ist es wirklich sinnvoll, so eine Sammlung aufzubauen und sich als „digitales Plutonium" in den digitalen Keller der Krankenkassen bzw. ihrer Dienstleister zu legen? Hm...

Nachrichtendienste und kriminelle Dienstleister

Dabei muss hinzugefügt werden, dass insbesondere jenseits der „Gewinnung menschlicher Quellen" die geheimdienstlichen Methoden nicht auf staatliche Akteure beschränkt sind. Es ist ein offenes Geheimnis, dass es eine Art „Informationsbeschaffungs-Söldner" gibt, die man für Aufklärungsarbeit mit quasi-geheimdienstlichen Mitteln kommerziell „mieten" kann.

Tatsächlich können Interessierte wohl, wie das Bundeskriminalamt im Lagebild „Cyberkriminalität 2019" beschreibt, auf eine hochprofessionelle und arbeitsteilig organisierte „Schattenwirtschaft" (*underground economy*) zurückgreifen[256], die Datenkriminalität als Dienstleistung anbietet. Die Grenzen zwischen staatlichen Akteuren und gewinnorientiert agierender organisierter Kriminalität verschwimmen dabei[257].

Das zeigt auch verdeckt gefilmtes Material aus dem Jahr 2018, dass der britische Sender „Channel 4" veröffentlicht hat[258]. Dort geben der Leiter der Politikberatungsfirma „Cambridge

254 „Nachrichtendienstlich gesteuerte Cyberangriffe", Bundesamt für Verfassungsschutz, Köln, Mai 2018; S. 5

255 State Security Department of hte Republic of Lithuania/Defence Intelligence and Security Service: „National Threat Assessment 2021", Vilnius (2021); S. 41ff. + S. 46.

256 „Cybercrime – Bundeslagebild 2019", Bundeskriminalamt , Wiesbaden (2020), S. 29ff.

257 z.B. ebd., S. 44

258 „Cambridge Analytica uncovered", Channel 4, März 2018; https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose , zuletzt abgerufen 13.02.2020

Analytica“, Alexander Nix, und sein „Managing Director“ , Mark Turnbull, in einem vermeintlichen Verkaufsgespräch Einblicke in ihre Methoden und Geschäftstätigkeiten:

Mark Turnbull: „*Sie sprachen von Informationsbeschaffung […] Wir haben, wir haben Beziehungen und Kooperationen mit speziellen Organisationen, die diese, die diese Art von Arbeit erledigen.“*

Mark Turnbull: „*Es gibt da verschiedene Informationsbeschaffungs-Organisationen, die sehr diskret arbeiten, um entsprechende Informationen [kompromittierendes Material] zu finden. Ich kenne Leute, die früher für den MI5, MI6 gearbeitet haben. Sie arbeiten jetzt für diese privaten Organisationen.*“

Alexander Nix: „*Wir beschäftigen sie als Unterauftragnehmer. […] Wir greifen auf [...] Unternehmen zurück [...] die sehr effektiv Informationen beschaffen.*“

Darüber hinaus geben andere Aussagen von Herrn Nix deutliche Hinweise auf verdeckte Tätigkeiten durch privatwirtschaftliche Akteure, z.B. zur Gewinnung von kompromittierendem Material.

Zusammenfassend lässt sich feststellen, dass insbesondere professionelle staatliche Akteure wie Geheimdienste, aber auch privatwirtschaftliche Akteure wohl die Kenntnisse und Ressourcen haben, um an die medizinischen Daten in einer virtuellen „elektronischen Patientenakte“ zu gelangen.

Offen ist aber noch die Frage, ob es überhaupt Hinweise darauf gibt, dass diese Akteure demokratische Prozesse wie z.B. Wahlen beeinflussen bzw. manipulieren wollen, und sie damit beispielsweise auch ein Motiv hätten, sich sensible medizinische Daten anzueignen.

Datenanhäufung, Profilerstellung, Angriffe auf freiheitlich-demokratisch verfasste Gesellschaften

Tatsächlich gibt es die.

So fasst das Bundesamt für Verfassungsschutz zusammen[259]: „*Eine besonders weitreichende False-Flag-Operation bildete der Cyberangriff auf das Netzwerk des US-amerikanischen Democratic National Committee (DNC), der Verwaltungsorganisation der Demokratischen Partei der Vereinigten Staaten. Sie wurde von dem bis dahin unbekannten Pseudonym „Guccifer 2.0“ verübt, das von Sicherheitsbehörden und IT-Sicherheitsunternehmen als eine False-Flag-Operation von APT 28 angesehen wird. Unter dem Namen „Guccifer 2.0“ bekannte sich ein angeblicher Hacker im Juni 2016 zu einem Cyberangriff, bei dem es zu einem Datendiebstahl im Netzwerk des DNC kam.*

„Guccifer 2.0“ gab in seinem Blog an, einen Großteil der entwendeten Daten an WikiLeaks übermittelt zu haben. Am 22. Juli, drei Tage vor dem Nominierungsparteitag der US-Demokraten, wurden über 19.000 interne E-Mails des DNC auf WikiLeaks veröffentlicht, diese enthielten u. a. Angaben zu Personen, die an die Demokratische Partei gespendet hatten sowie interne Finanzberichte der Partei. Die Untersuchung des Vorfalls ergab Hinweise auf die russischen Angriffskampagnen APT 28 und APT 29 als Urheber. Die Aktivitäten von „Guccifer 2.0“ wurden dabei als mögliche russische Desinformationskampagne gewertet, die den Präsidentschaftswahlkampf zugunsten des republikanischen Spitzenkandidaten Trump beeinflussen sollte.

Auch der französische Präsidentschaftskandidat Macron hat Cyberangriffe auf sein Wahlkampfteam beklagt, die dortigen Untersuchungen zufolge von russischen Stellen ausgegangen sein sollen.“

259 „Nachrichtendienstlich gesteuerte Cyberangriffe“, Bundesamt für Verfassungsschutz, Köln, Mai 2018; S. 14f.

Eine naturgemäß noch detailliertere Analyse liefert der Untersuchungsbericht des US amerikanischen Sonderermittlers Robert S. Mueller[260] zur russischen Einflussnahme auf die dortigen Präsidentschaftswahlen im Jahr 2016, die der Bericht mit den Worten zusammenfasst: „*Die russische Regierung nahm […] systematisch auf die Präsidentschaftswahlen 2016 Einfluss*“[261].

Der Bericht unterscheidet im Wesentlichen zwei Arten der Einflussnahme auf Wahlen: einerseits das auch vom BfV beschriebene Erbeuten und Verbreiten von Daten, andererseits „aktive Maßnahmen“ über soziale Medien (*Russian „active measures“ social media campaign*): „*[…] kam die Untersuchung zu dem Ergebnis, dass Russland im Wesentlichen durch zwei Operationen auf die Präsidentschaftswahlen 2016 Einfluss nahm. Erstens führte eine russische Einrichtung eine Kampagne in den sozialen Medien zum Vorteil von Präsidentschaftskandidat Donald J. Trump und zum Nachteil von Präsidentschaftskandidatin Hillary Clinton durch. Zweitens drang ein russischer Nachrichtendienst in Rechner von Einrichtungen, Mitarbeitern und Freiwilligen des Clinton-Wahlkampfes ein und veröffentlichte dann gestohlene Dokumente.*“[262]

Der Bericht beschreibt auf Seite 38 einige Details des nachrichtendienstlichen Vorgehens der Russischen Föderation: „*Einheit 26165 implementierte in den DCCC und DNC Netzwerken zwei Arten speziell angepasster Schadprogramme, die als „X-Agent“ und „X-Tunnel“ bezeichnet werden, sowie Mimikatz, ein Werkzeug zum Abgreifen von Zugangsinformationen und rar.exe, ein Werkzeug, das im Rahmen dieser Einbrüche dazu verwendet wurde, Materialien für das Abschöpfen zu kompilieren und zu komprimieren. X-Agent war ein Multifunktions-Hacking-Werkzeug, dass es Einheit 26165 erlaubte, die gedrückten Tasten mitzuprotokollieren, den Bildschirm abzuphotographieren und andere Informationen über die infizierten Computer zu sammeln […]. X-Tunnel war ein Hacking-Werkzeug, das eine verschlüsselte Verbindung zwischen dem DCCC/DNC-Opfer-Rechner und Computern außerhalb der DCCC und DNC Netzwerke aufbaute, die vom [Geheimdienst] GRU kontrolliert wurden und umfangreiche Datenübertragungen durchführen konnte. GRU Offiziere verwendeten X-Tunnel dann, um gestohlene Daten von den betroffenen Computern auszuleiten.*“

Die oben genannte, systematische Wahlbeeinflussung über soziale Medien verfolgte dabei zunächst das Ziel, gesellschaftliche Konflikte zu schüren:

„*Die Internet Research Agency[263] (IRA) führte die frühesten Maßnahmen russischer Einflussnahme durch, die im Rahmen dieser Untersuchung festgestellt wurden – eine Kampagne in sozialen Medien, die darauf ausgerichtet war, politische und soziale Konflikte [discord] in den Vereinigten Staaten zu provozieren oder zu verstärken. […] In der Mitte des Jahres 2014 entsandte die IRA im Rahmen einer Mission zur Informationsbeschaffung Mitarbeiter in die Vereinigten Staaten mit dem Auftrag [geschwärzt]. Später benutzte die IRA Konten bei sozialen Medien sowie Interessengruppen um innerhalb des politischen Systems der USA Konflikte zu schüren durch eine von ihr so genannte „informationelle Kriegsführung“. Die Kampagne entwickelte sich von einem allgemeinen Programm, das in den Jahren 2014 und 2015 das Ziel verfolgte, das US Wahlsystem zu untergraben, zu einer zielgerichteten Operation, die Anfang 2016 Kandidat Trump unterstützte und Kandidatin Clinton*

260 Robert S. Mueller: „Report On The Investigation Into Russian Interference In The 2016 Presidential Election“, Washington, März 2019.
261 ebd., S. 1
262 ebd., S. 1f.
263 Lt. Bericht in St. Petersburg ansässig und durch einen Putin-nahen Oligarchen finanziert.

verunglimpfte. Die Operation der IRA beinhaltete den Kauf politischer Werbeanzeigen in sozialen Medien im Namen von US amerikanischen Personen und Einrichtungen, sowie die Inszenierung von politischen Demonstrationen [rallies] in den USA. […] Im April 2016 hackte der GRU[264] sich in die Rechnernetzwerke des Democratic Congressional Campaign Committee (DCCC) und des Democratic National Committee (DNC). Der GRU stahl hunderttausende Dokumente aus kompromittierten E-Mail-Konten und Netzwerken.“[265]

Was meint „informationelle Kriegführung“? Dem Lagebericht 2021 des estnischen Auslandsnachrichtendienstes zufolge, der aus geographisch naheliegenden Gründen die Entwicklungen in der Russischen Föderation mit besonderer Aufmerksamkeit verfolgt, umfasst die Doktrin der gezielten „informationellen Kriegführung“ des russischen Militärs neben der üblichen Abwehr von Cyberbedrohungen insbesondere zwei weitere Säulen[266]: psychologische Kriegführung (z.B. Falsch- und Desinformation) und Cyberangriffe (=Hackerangriffe). Er führt als aktuelle Beispiele u.a. das Hacken von Nachrichtenseiten in Litauen und Polen 2020 auf, die mit dem Platzieren gefälschter Meldungen im Vorfeld von Wahlen verbunden waren. Das Hacken von Nachrichtenseiten verfolgt dabei einen doppelten Zweck: Verbreiten von Falschinformationen aus scheinbar seriöser Quelle und Unterminieren der Glaubwürdigkeit klassischer Informationskanäle, die sich ansonsten dem eigenen Einfluss entziehen.

Der Bericht des Sonderermittler Mueller unterstreicht die hohe Reichweite der „informationellen Kriegführung“ über soziale Medien[267]: „*[…] Mitarbeiter der Internet Research Agency unterhielten Konten und Gruppen bei sozialen Medien, die darauf ausgerichtet waren, US Zielgruppen [audiences] anzusprechen. Diese Gruppen und Konten zu kontroversen politischen und sozialen Themen gaben fälschlicherweise vor, von Aktivisten aus den USA betrieben zu werden. […] Gegen Ende der US Präsidentschaftswahlen 2016 konnte die IRA so Millionen von Menschen in den USA erreichen. IRA-kontrollierte Twitterkonten hatten Zehntausende von Followern, darunter verschiedene Personen der amerikanischen Politik, die von der IRA produzierte Inhalte weiterverbreiteten. Facebook vermutete, das die IRA über ihre Facebook-Konten bis zu 126 Millionen Menschen erreichte. [...]*“

Darüber hinaus schildert der Bericht, wie die „Internet Research Agency“ politische Kundgebungen inszenierte, indem sie sie vorbereitete und dann als geeignet identifizierte Zielpersonen innerhalb der USA dazu brachte, als Veranstalter aufzutreten[268]: „*Die IRA organisierte und bewarb politische Kundgebungen in den USA, wobei sie sich als US Graswurzelaktivisten ausgab. Dabei verwendete die IRA im ersten Schritt eine ihrer existierenden Tarnidentitäten in sozialen Medien (z.B. Facebook-Gruppen und Twitter-Konten) um eine Veranstaltung anzukündigen und dafür zu werben. Dann sandte die IRA eine große Zahl Nachrichten, die sich direkt an „Follower“ ihres Kontos richteten, mit der Aufforderung, daran teilzunehmen. Unter denen, die antworteten und ein Interesse an einer Teilnahme erkennen ließen, suchte sich die IRA dann einen US Bürger, der als Koordinator der Veranstaltung diente. In den meisten Fällen gab der IRA Mitarbeiter, der das Konto betrieb, an, dass er aufgrund eines Terminkonfliktes, oder da er zur Zeit verreist sei, selbst nicht an der Veranstaltung teilnehmen könne. Die IRA bewarb die Veranstaltung dann weiter, indem sie die US Medien bezüglich der Veranstaltung kontaktierte und sie dazu brachte, mit dem*

264 GRU: Militärischer Nachrichtendienst Russlands
265 ebd. S. 4
266 Lagebild 2021 des estnischen Auslandsnachrichtendienstes Välisluureamet: „International Security and Estonia 2021“ (2021).
267 ebd. S. 14
268 ebd. S. 31

Koordinator Kontakt aufzunehmen. Nach der Veranstaltung veröffentlichte die IRA Film- und Fotoaufnahmen der Veranstaltung auf ihren Konten bei sozialen Medien. […] Die IRA gewann auch Moderatoren konservativer Gruppen auf sozialen Medien dafür, Material, das von der IRA erzeugt worden war, weiterzuverbreiten [promote] und rekrutierte Einzelpersonen für politische Aktionen […] als der von der IRA online erreichte Personenkreis größer wurde, verfolgte die IRA die Aktivitäten [tracked] von US Bürgern, mit denen sie Kontakt aufgenommen und erfolgreich dazu gebracht hatten, Aufträge [tasks] zu übernehmen (die von der Organisation von Kundgebungen bis zur Aufnahme von Bilden mit bestimmten politischen Botschaften reichten).“

Der Bericht weist zudem darauf hin, dass „*die US Operationen Teil einer größeren Menge miteinander verflochtener Operationen*“ seien, die als „*Projekt Lakhta*“ bezeichnet würden[269].

Nähere Informationen zu dieser Operation „Projekt Lakhta“ und ihrer möglicher Relevanz für Deutschland finden sich in einer Pressemitteilung des US amerikanischen Justizministerium vom 19. Oktober 2018[270]: „*Das strategische Ziel dieser mutmaßlichen Verschwörung [alleged conspiracy], die bis heute andauert, ist es, soziale Zwietracht im politischen System der USA zu säen und das Vertrauen in unsere demokratischen Institutionen zu untergraben. […] des „Projekts Lakhta“, einer umfassenden russischen Maßnahme [effort], finanziert durch den russischen Oligarchen Jewgenij Viktorowitsch Prigoshin und zwei von ihm kontrollierte Unternehmen, „Concord Management and Consulting LLC“ und „Concord Catering“. Das Projekt Lakhta umfasst mehrere Komponenten, von denen sich manche auf Zielgruppen [audiences] innerhalb der Russischen Föderation beziehen, während andere auf ausländische Zielgruppen ausgerichtet sind, u.a. in den USA, Mitgliedsstaaten der Europäischen Union und der Ukraine. […] Das vermutliche Gesamtbudget des Projekts Lakhta zwischen Januar 2016 und Juni 2018 betrug 35 Millionen US$, wenngleich nur ein Teil dieser Mittel sich auf die USA bezog. […] Sie eröffneten Tausende von Konten […] auf Plattformen sozialer Medien die scheinbar von US Bürgern genutzt wurden, und verwendeten sie zur Schaffung Konflikt schürender, an Zielgruppen in den USA gerichteter sozialer und politischer Inhalte. Diese Konten wurden auch dazu genutzt, für oder gegen die Wahl von Kandidaten bei den US Wahlen in den Jahren 2016 und 2018 aufzurufen. […] Die Verschwörung nutzte vermutlich soziale Medien und andere Internetplattformen, um einen weiten Themenbereich abzudecken, u.a. Einwanderung, […], Rassebeziehungen, LGBT-Themen […]. Teilnehmer der Verschwörung nutzten dabei spezifische Ereignisse in den Vereinigten Staaten als Aufhänger ihrer Themen, wie das Attentat auf Kirchenmitglieder in Charleston […]. Im Rahmen der Aktivitäten der Beteiligten wurde dabei nicht exklusiv ein einzelner ideologischer Standpunkt vertreten, sie vertraten unterschiedliche und manchmal gegensätzliche Positionen. Die Beteiligten waren u.a. dazu angehalten, die ‚Intensität der politischen Auseinandersetzung durch die Unterstützung radikaler Gruppierungen zu steigern‘ und ‚Konflikte zwischen Minderheiten und dem Rest der Bevölkerung zu verschärfen‘. Die Akteure entwickelten dabei Drehbücher und Leitfäden für die Verbreitung strategischer Botschaften, die eine Anleitung lieferten, wie bestimmte soziale Gruppen angesprochen werden können, z.B. durch das Timing der Botschaften, die Art des Nachrichtenkanals, sowie zum Verpacken [framing] Zwietracht säender Botschaften.*“

Daraus lässt sich ableiten, dass es in der Tat ein Beispiel für umfassende geheimdienstliche Aktivitäten gibt, die das Ziel verfolgen, demokratische Prozesse zu manipulieren und zu untergraben, dass diese Aktivitäten über die Präsidentschaftswahlen in den USA hinaus bis

269 Ebd. S. 16

270 https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system (zuletzt abgerufen 13.02.2020)

mindestens 2018 andauerten, und dass nicht nur die USA, sondern auch „*Mitgliedsstaaten der Europäischen Union*“ *[members of the European Union]* Ziel der Aktivitäten waren. Es ist zudem plausibel anzunehmen, dass derartige Aktivitäten bis heute weiterbestehen.

Ein wesentliches Muster der Aktivitäten scheinen dabei einerseits der irreguläre Zugriff auf Datensammlungen und deren Aneignung zu sein, sowie die möglichst gezielte und passgenaue Sendung kontroverser Botschaften an bestimmte Zielgruppen in der Absicht, soziale und politische Konflikte zu eskalieren. Besonders effektiv wäre hier aus Sicht der Akteure offensichtlich die Kombination von Aneignung personenbezogener Informationen, die eine möglichst optimale Profilbildung erlauben und deren Nutzung zur zielgerichteten Sendung manipulativer Botschaften.

Interessanterweise tragen die erwähnten investigativen Dokumentarfilme des britischen Senders Channel 4 über die politische Beratungsfirma „Cambridge Analytica“ weitere Facetten bei. So beschreibt Alexander Nix, in Personalunion Direktor von „SCL Elections“ und Leiter des eng mit der SCL Group verbundenen Tochterunternehmens (jetzt: Emerdata), in einem mit versteckter Kamera aufgenommenen Treffen den Beitrag seiner Firma zu den Präsidentschaftswahlen in den USA bzw. dem Wahlkampf 2016 von Donald Trump[271]: „*Die gesamte Recherche war von uns, alle Daten, alle Analysen, das ganze Targeting, wir waren für die digitale Kampagne verantwortlich, die Fernsehkampagne, und die ganze Strategie basierte auf unseren Daten [our data informed all the strategy].*“

Laut Channel 4 brüstet die Firma sich damit, die Wahlen für den Präsidentschaftskandidaten Trump gewonnen zu haben, indem sie „*Zugriff auf eine riesige Datensammlung hatten, Namen und E-Mail-Adressen von 230 Millionen Amerikanern. Für jeden konnten sie auf tausende Schichten personenbezogener Informationen zugreifen und die Botschaft so gestalten, dass Sie Dich einzeln [individually] davon überzeugt, dass Donald Trump Dein nächster Präsident sein sollte. Sie benutzen dieses ‚Mikrotargeting‘ um den maximalen Effekt zu erzielen [...]*“

In den verdeckten Filmaufnahmen berichten die Mitarbeiter von SCL/Cambridge Analytica zudem davon, wie insbesondere negative Nachrichten über scheinbar von den Wahlkampagnen unabhängige Vereine/Gruppen verbreitet werden. Sie selbst hätten im US Wahlkampf die „Crooked Hillary Clinton“-Schmutzkampagne kreiert[272] und mit zahlreichem „Kreativmaterial“ online verbreitet. Sie führen auch aus, wie sie dabei verdeckt und möglichst ohne Spuren zu hinterlassen agieren, z.B. durch die Gründung scheinbar unabhängiger Organisationen oder über Dritte (*proxy organisations*), die „*mit Material gefüttert werden*“ und es dann weiterverbreiten: „*Wir injizieren einfach die Informationen in den Blutkreislauf des Internets und schauen dann zu, wie sie wachsen und geben ihnen hier und da einen kleinen Schubs. Auf diese Weise infiltrieren die Sachen die Online Community und verbreiten sich – aber ohne Erkennungszeichen, ohne dass sie zugeordnet oder zurückverfolgt werden können.*“. Sie schildern auch, wie sie unter falscher Identität Missionen in Ländern durchführen (lassen) und sie ihre Tätigkeiten als Forschungsprojekt tarnen und sich gegebenenfalls als Studenten bzw. Universitätsmitarbeiter ausgeben. Und sie legen Wert darauf, in der Kommunikation mit den Kunden sich automatisch löschende Mails zu verwenden, um die Strafverfolgung zu erschweren.

Ein wesentlicher Punkt der Wahlmanipulation ist dabei die datenbasierte Profilerstellung von Wählerinnen und Wählern. So sagt der Datenverantwortliche von Cambridge Analytica, Alex

271 „The Trump campaign“, Channel 4, März 2018; https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose , zuletzt abgerufen 13.02.2020

272 Die Kampagne zielte dabei wohl vor allem darauf ab, potentielle Wähler von der Wahl abzuhalten.

Tayler, in den verdeckten Filmaufnahmen[273]: „*Wenn man Daten über Menschen sammelt und Profile von ihnen erstellt, dann versteht man besser, wie man die Bevölkerung in Gruppen einteilen kann, um Botschaften an sie zu richten zu Themen, die sie interessieren und mit einer Sprache und Bildern, die sie aller Wahrscheinlichkeit nach ansprechen.*“

Mark Turnbull, der Managing Director des „Politikberatungsunternehmens“ führt aus: „*Die zwei fundamentalen Triebkräfte des Menschen, wenn es darum geht, Informationen aufzunehmen, sind Hoffnungen und Ängste, und die sind oftmals unausgesprochen und sogar unbewusst. Sie wussten vielleicht gar nicht, dass ihnen etwas Angst macht, bis sie etwas sahen, das diese Reaktion einfach bei Ihnen auslöste. Und unsere Aufgabe ist es, herauszufinden, ist es, sozusagen den Eimer tiefer in den Brunnen hinabzulassen als jeder andere, um zu verstehen, welches diese wirklich tiefsitzenden Ängste und Sorgen sind. […] Es hat keinen Sinn, einen Wahlkampf auf der Basis von Fakten zu führen, es geht nur um Emotionen.*“

Wir haben hier also streng genommen nicht nur ein Beispiel für Akteure, die jeder für sich an möglichst sensiblen und intimen persönlichen Daten mit möglichst hohem „Manipulationspotential“, also zum Beispiel medizinischen Daten, interessiert sind, sondern gleich drei Beispiele: Neben einem ausländischen Geheimdienst eine inländische politische Gruppierung, die mit allen Mitteln die Macht erringen will und einen international agierenden Dienstleister für Profilerstellung und Manipulation demokratischer Prozesse, wobei die drei Akteure im US Wahlkampf offenbar in einer undurchsichtigen Wechselbeziehung standen.

Wäre das auch in Deutschland möglich? In der Tat könnte und sollte man kritisch fragen, ob es überhaupt Anhaltspunkte dafür gibt, dass etwas Ähnliches auch in Deutschland passieren könnte oder passiert sei.

Dies ist tatsächlich der Fall.

Bevor ich dies näher erläutere, der Vollständigkeit halber noch einige Punkte zum Hintergrund der Firma Cambridge Analytica bzw. der SCL Gruppe (jetzt: Emerdata) und zu den informationellen „Rahmenbedingungen“ einer neuen Sammlung personenbezogener Daten angeführt werden, d.h. zum Geschäftsmodell sozialer Netwerke und zu Datenhändlern.

Cambridge Analytica[274] war ein Tochterunternehmen der SCL Gruppe („strategic communications laboratory), die sowohl „Dienstleistungen“ im Zusammenhang mit Wahlen anbot (SCL Elections), als auch militärische Dienstleistungen im Bereich der pyschologischen Kriegsführung mit besonderer Expertise im Bereich „informationelle Dominanz“ (u.a. durch Verbreiten von Gerüchten, Desinformation und Falschnachrichten[275]). Gegründet wurde Cambridge Analytica 2014 unter anderem von dem Direktor von „SCL Elections“ Alexander Nix, dem amerikanischen Milliardär Robert Mercer und dem amerikanischen Rechtsextremen Stephen Bannon, der zunächst auch Vizepräsident von Cambridge Analytica war[276]. Nach eigener Aussage handelte es sich bei SCL/Cambridge Analytica um das „größte und wichtigste“ Unternehmen seiner Art[277], mit anderen Worten also nicht um das einzige. In

273 „Cambridge Analytica uncovered“, Channel 4, März 2018; https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose , zuletzt abgerufen 13.02.2020

274 Carole Cadwalladr: „‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower“, The Guardian, 18.03.2018 (online: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump, zuletzt abgerufen: 15.02.2020)

275 ebd.

276 ebd.

277 „Cambridge Analytica uncovered“, Channel 4, März 2018; https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose , zuletzt abgerufen 13.02.2020

einem in der Zeitung „The Guardian“ wiedergegebenem Zitat wird SCL von einem militärischen Spezialisten für informationelle Kriegführung mit den Worten charakterisiert: „*Oh, Sie sollten SCL kennenlernen. Sie betreiben informationelle Kriegführung [cyberwarfare] für Wahlen*.“[278]

Die Rolle kommerzieller Profilersteller

Das Geschäftsmodell von Firmen wie Facebook/Instagram/Twitter oder Google[279] wiederum ist eng verwandt. Es beruht wie oben erwähnt darauf, ihren zahlenden Kunden (nein, das sind nicht Sie, liebe Leserin und lieber Leser) die Erstellung und Ansprache möglichst passgenauer Zielgruppen unter ihren kostenlosen Nutzern zu ermöglichen (*das* sind Sie). Zu diesem Zweck haben die zahlenden Kunden die Möglichkeit, sich anhand der von den Firmen gesammelten personenbezogenen Daten Profile der Personengruppen zu erstellen, die erreicht und beeinflusst werden sollen. Die Firmen wie z.B. Anbieter virtueller „sozialer Netzwerke“ geben dabei natürlich nicht die Rohdaten ihrer Nutzer weiter. Die bilden ja quasi den Grundstock ihres Geschäftsmodells[280]. Statt dessen bieten sie ihren Kunden über Software wie Facebook‘s „audience manager tool“ die Möglichkeit an, sich z.B. anhand geographischer, demographischer, interessens- oder verhaltensbasierter Parameter maßgeschneiderte Wunschprofile ihrer Adressaten zusammenzustellen[281]. Wobei Facebook auch auf externe Datensätze von Datenhändler zurückgreift[282], die Rohdatensätze personenbezogener Daten kommerziell anbieten. Die Personen, die den entsprechenden Profilen entsprechen, werden dann zu den Adressaten personalisierter „Botschaften“.

Zur Illustration der eigenen Datensammlung solcher Internet-Dienstleister sei hier als Beispiel ein Auszug aus der Datenschutzerklärung von Google wiedergegeben[283]:
„[…] Wir erheben auch die Inhalte, die Sie bei der Nutzung unserer Dienste erstellen, hochladen oder von anderen erhalten. Dazu gehören beispielsweise E-Mails, die Sie verfassen und empfangen, Fotos und Videos, die Sie speichern, Dokumente und Tabellen, die Sie erstellen, und Kommentare, die Sie zu YouTube-Videos schreiben. […] Wir erheben Daten über die Apps, Browser und Geräte, die Sie beim Zugriff auf Google-Dienste verwenden. […] Zu den von uns erhobenen Daten zählen eindeutige Kennungen, der Typ und die Einstellungen des Browsers, der Typ und die Einstellungen des Geräts […]. Wenn Sie ein Android-Gerät mit Google Apps verwenden, kontaktiert Ihr Gerät regelmäßig die Google-Server, um Daten über Ihr Gerät und die Verbindung zu unseren Diensten bereitzustellen. […] Wir erheben in unseren Diensten Daten zu Ihren Aktivitäten. Diese Daten verwenden wir beispielsweise, um Ihnen ein YouTube-Video zu empfehlen, das Ihnen gefallen könnte. Unter anderem könnten folgende Aktivitätsdaten erhoben werden:

- *Begriffe, nach denen Sie suchen*

278 Carole Cadwalladr: „‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower“, The Guardian, 18.03.2018.

279 Der Sammelbegriff „Google“ meint hier nicht nur die gleichnamige Suchmaschine zur Erfassung und Verarbeitung von Suchanfragen sondern z.B. auch den Google-Webbrowser Chrome zur Anzeige von und Navigation zwischen Websites, die Softwareplattform Google Playstore, das Google-Betriebssystem Android, die Übersetzungsdienstleistung Google Translator, das Mailprogramm bzw. den Mailserver Google Mail (Gmail) und den („Cloud“-)Datenspeicher Google Drive, die funktional ebenfalls Zubringerdienste zur Sammlung und Auswertung personenbezogener Informationen sind.

280 Allerdings haben z.B. im Jahr 2014 zahlreiche Nutzer eines von Aleksandr Kogan entwickelten, vermeintlich der Forschung dienenden Online-“Persönlichkeitstests“ ihre bei Facebook gespeicherten persönlichen Daten und die der mit ihnen verbundenen Facebook-Nutzer als „Datenspende“ freiwillig preisgegeben. Aleksandr Kogan, Gründer des mit SCL/Cambridge Analytica kooperierenden Unternehmens „Global Science Research“, war zu der Zeit wissenschaftlicher Mitarbeiter der Universität Cambridge und außerordentlicher Professor der Universität St. Petersburg mit Finanzierung durch den russischen Staat. (https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump, zuletzt abgerufen 15.02.2020)

281 Siehe z.B. https://adespresso.com/guides/facebook-ads-beginner/ , zuletzt abgerufen 14.02.2020

282 Ebd., s.a.: Kalev Leetaru: „The data brokers so powerful even Facebook bought their data – but they got me wildly wrong“, Forbes, 05.04.2018.

283 Google Datenschutzerklärung und Nutzungsbedingungen, Stand 15.10.2019, https://policies.google.com/privacy?hl=de (zuletzt abgerufen 23.02.2020.

- *Videos, die Sie sich ansehen*
- *Inhalte und Werbeanzeigen, die Sie sich ansehen und mit denen Sie interagieren*
- *Sprach- und Audiodaten bei Ihrer Nutzung von Audiofunktionen*
- *Kaufaktivitäten*
- *Personen, mit denen Sie kommunizieren oder Inhalte austauschen*
- *Aktivitäten auf Websites und Apps von Drittanbietern, die unsere Dienste nutzen*
- *Der Chrome-Browserverlauf, den Sie mit Ihrem Google-Konto synchronisiert haben*

Wenn Sie unsere Dienste nutzen, um Anrufe zu tätigen und zu erhalten oder um Nachrichten zu senden und zu empfangen, erheben wir möglicherweise Telefonie-Informationen wie Ihre Telefonnummer, die Anrufernummer, die Nummer des Angerufenen, Weiterleitungsnummern, das Datum und die Uhrzeit von Anrufen und Nachrichten, die Dauer von Anrufen, Routing-Informationen und die Art der Anrufe. […] Wenn Sie unsere Dienste nutzen, erheben wir Daten zu Ihrem Standort. […] Ihr Standort kann mit unterschiedlicher Genauigkeit bestimmt werden. Dazu verwenden wir:

- *GPS*
- *IP-Adresse*
- *Sensordaten von Ihrem Gerät*
- *Informationen über Objekte in der Nähe Ihres Geräts, wie etwa WLAN-Zugriffspunkte, Funkmasten und Bluetooth-fähige Geräte“*

Kurz gesagt und für die Star Trek Fans unter Ihnen: Sie sind die Borg (des Internets)...[284]

Es geht weiter: Kosinski et al. konnten 2013 zeigen, dass die von einem Facebook-Nutzer vergebenen „Likes“ es erlauben, mit recht hoher Zuverlässigkeit auf dessen politische und sexuelle Orientierung zurückzuschließen[285], d.h. ihn entsprechend zu profilieren. In einer weiteren Veröffentlichung aus dem Jahr 2014 zeigten die Autoren, dass automatisierte Verfahren die wesentlichen Persönlichkeitszüge von Menschen anhand von Likes im Durchschnitt gleich gut oder besser erfassen als andere Menschen: bei Auswertung von 10 „Likes“ besser als Arbeitskollegen, bei Auswertung von 70 „Likes“ besser als Freunde oder Mitbewohner, bei Auswertung von 150 „Likes“ besser als Familienmitglieder, bei Auswertung von 300 „Likes“ besser als der Ehepartner/die Ehepartnerin[286]. Die mittlere Zahl von zur Verfügung stehenden Likes liegt dem Artikel zufolge bei 227 „Likes“.

Facebook selbst hat von 2012 bis 2016 eine Reihe von Patenten beantragt, die Daten und Maschinelles Lernen für Ihre automatisierte Klassifizierung kombinieren. Die Patente tragen den Titel: „Die Bestimmung von Persönlichkeitsmerkmalen von Nutzern anhand der Kommunikation und Charakeristiken in sozialen Netzwerken“[287]: „*Ein soziales Netzwerk gewinnt linguistische Daten aus der schriftlichen Kommunikation eines Nutzers. […] Die linguistischen und nicht-linguistischen auf den Nutzer bezogenen Daten werden in einem antrainierten Modell verwendet, um ein oder mehrere Persönlichkeitsmerkmale des Nutzers zu bestimmen [to predict]. Die abgeleiteten Persönlichkeitsmerkmale werden in Verbindung mit dem Profil des Nutzers gespeichert und können für zielgerichtete Ansprache [targeting], Reihung, die Auswahl von Produktversionen oder verschiedene andere Zwecke benutzt werden.“*

284 Vgl. auch die Beobachtungen zum Deutschen Ethikrat bzw. seiner Vorsitzenden in Teil 1.

285 M. Kosinski, D. Stilwell, T. Graepel: „Private traits and attributes are predictable from digital records of human behavior“, Proceedings of the National Academy of Sciences USA (PNAS), 110, 5802-5805 (2013).

286 W. Youyou, M. Kosinski und D. Stilwell: „Computer-based personality judgments are more accurate than those made by humans“, Proceedings of the National Academy of Sciences USA (PNAS), 112, 1036-1040 (2014).

287 „Determining user personality characteristics from social networking system communications and characteristics“, US Pat. Nr. 8825764, 9386080, 9740752.

Eng mit Facebook verbunden ist ja der Messenger-Dienst „Whatsapp“, der von ca. 58 Millionen Bundesbürgerinnen und Bundesbürgern genutzt wird[288], das entspricht ca. 69,8 % der Gesamtbevölkerung:

„*WhatsApp erhält bzw. sammelt Informationen, wenn wir unsere Dienste betreiben und bereitstellen. Dies geschieht unter anderem, wenn du unsere Dienste installierst, nutzt oder auf sie zugreifst.[…] Automatisch gesammelte Informationen*

- *[…] Dies umfasst auch Informationen über deine Aktivität (beispielsweise wie du unsere Dienste nutzt, wie du mit anderen bei der Nutzung unserer Dienste interagierst und Ähnliches), Log-Dateien sowie Diagnose-, Absturz-, Webseiten- und Performance-Logs und -berichte.*
- *[…] Wenn du für unsere Dienste bezahlst, erhalten wir möglicherweise Informationen und Bestätigungen, wie z.B. Zahlungsbelege, auch von App Stores oder anderen Dritten, die deine Zahlung bearbeiten.*
- *[…] Wenn du unsere Dienste installierst, nutzt oder auf sie zugreifst, sammeln wir gerätespezifische Informationen. Dazu gehören auch Informationen wie das Hardware-Modell, die Informationen zum Betriebssystem, Browser-Informationen, die IP-Adresse, Angaben zum Mobilfunknetz, einschließlich der Telefonnummer, sowie Gerätekennungen. Wir sammeln Standortinformationen des Geräts, wenn du unsere Standort-Funktionen verwendest, also z. B. wenn du deinen Standort mit deinen Kontakten teilst, Orte in der Nähe anschaust, Standorte, die andere dir gesendet haben, anschaust oder Ähnliches [...].*
- *[...]Wir verwenden Cookies, um unsere Dienste zu betreiben und bereitzustellen. […] Darüber hinaus können wir Cookies einsetzen, um deine Einstellungen[…] zu speichern und um unsere Dienste auf sonstige Art und Weise individuell für dich zu gestalten. [...]*
- *[…]Wir sammeln Informationen über die Änderungen deines Online-Status und deiner Statusmeldung auf unseren Diensten[...].*

Informationen Dritter

- *[…] Wir erhalten Informationen von anderen Personen, die möglicherweise auch Informationen über dich enthalten. [...]*
- *[…] Wir arbeiten mit Drittanbietern zusammen, die uns dabei helfen, unsere Dienste zu betreiben, anzubieten, zu verbessern, zu verstehen, zu individualisieren, zu unterstützen und zu vermarkten. […] Diese Anbieter können uns unter bestimmten Umständen Informationen über dich zur Verfügung stellen [...].*

Wir gehören seit 2014 zur Facebook-Unternehmensgruppe. Als Teil der Facebook-Unternehmensgruppe erhält WhatsApp Informationen von den Unternehmen dieser Unternehmensgruppe und teilt Informationen mit ihnen.[…] Facebook und die anderen Unternehmen in der Facebook-Unternehmensgruppe können Informationen von uns auch verwenden, um deine Erlebnisse in ihren Diensten, wie Vorschläge zu unterbreiten (beispielsweise Freunde oder Verbindungen oder interessante Inhalte) und um relevante Angebote und Werbeanzeigen zu zeigen. […] Du akzeptierst unsere Datenpraktiken, einschließlich des Sammelns, der Verwendung, der Verarbeitung und des Teilens deiner

288 https://allfacebook.de/toll/whatsapp-nutzerzahlen

Informationen gemäß Darlegung in unserer Datenschutzrichtlinie, sowie die Übertragung und Verarbeitung deiner Informationen in die/den USA und andere/n Länder/n weltweit, in denen wir Einrichtungen, Dienstleister oder Partner haben bzw. einsetzen, und zwar unabhängig davon, wo du unsere Dienste nutzt.“[289]

Neben diesen Datenverwertern mit eigener Datenerhebung gibt es noch reine Datenhändler (data broker), die entsprechend personenbezogene (Roh-)Daten anbieten, die dann kommerziell erworben und zur Profilerstellung von Bürgerinnen und Bürgern verwendet werden können. Interessant dabei ist, dass sie offenbar die Möglichkeit bieten, sie z.B. mit den von Facebook erhobenen Daten sinnvoll zu verbinden. Das bedeutet, sie müssen Identifikatoren enthalten, die diese Zusammenführung personenbezogen erlauben. Durch den Zugriff auf Inhalte der virtuellen „elektronischen Patientenakte“, z.B. über stationäre oder mobile Endgeräte wie PC oder Smartphone, stehen über die oben genannten Metadaten (IP-Adresse, Gerätekennung, etc., aber auch Cookies oder installierte Benutzerkonten) die Identifikatoren ebenfalls zur Verfügung. Ein Weg, eine Pseudonymisierung oder Anonymisierung umgehen und die Daten mit denen aus anderen Quellen personenbezogen zu verknüpfen.

Ein konkretes Beispiel für die Möglichkeit, sich irregulär Zugang zu Daten zu verschaffen, schildert zudem der frühere Datenspezialist der SCL Firmengruppe bzw. der Firma „Cambridge Analytica“, Christopher Wylie, in seinem 2019 erschienenen Buch[290]: Scheinbar harmlose Zusatzprogramme für Webbrowser, wie Rechner oder Kalender, wurden von SCL gezielt dazu verwendet, sich auf Endgeräten gespeicherte sogenannte „Session-Cookies“ anzueignen, d.h. kleine Dateien, die einer Website signalisieren, dass der Nutzer sich dort kürzlich eingeloggt hatte. Mit Hilfe der angeeigneten Dateien konnten Mitarbeiter von SCL dann auf die (Facebook-)Benutzerkonten zugreifen und Inhalte ausspähen und später zur Profilierung und psychologischen Manipulation verwenden, wobei dies automatisiert geschah. Ähnliches wäre sicher auch mit dem Passwort-Manager von Web-Browsern denkbar, der den Nutzern typischerweise anbietet, die Zugangsdaten inklusive Passwort für zukünftige Besuche der jeweiligen Website abzuspeichern.
Dies alles gilt nicht nur für Facebook-, Google- oder Microsoft-Benutzerkonten sondern könnte genauso auch auf medizinische „Apps“ zutreffen, die auf eine virtuelle Patientenakte zugreifen.

Zudem können Dateien, die von Bürgerinnen und Bürgern in Apps verarbeitet und vielleicht sogar aus der virtuellen Patientenakte regulär exportiert werden, je nach technischer Ausgestaltung der Apps unter Umständen automatisch auf die Server von Datenverwertern übertragen („Cloud-Speicher“, „Google Drive“ bei Smartphones mit Android-Betriebssystem, Microsoft Cloud, Angebot von „Google Health“ etc.) und dann dort verarbeitet werden.

Dabei ist mit Blick auf Datenverwerter wie Facebook oder Google „personenbezogen“ nicht so zu verstehen, dass „klassische“ Identifikatoren wie Name, Adresse oder genaues Geburtsdatum zwingend bekannt sein müssten. Pseudonymisierte Daten erfüllen den Zweck völlig: Es ist ausreichend, den einzelnen Nutzer „irgendwie“ als Datenquelle und Zielobjekt kohärent identifizieren zu können, sei es anhand der Kennung oder einer Kennzeichnung persönlich benutzter Geräte wie mobiler Endgeräte/Smartphones, sei es geräteübergreifend z.B. durch das Einloggen in Nutzerkonten.

So hat beispielsweise praktisch jeder Besitzer eines Smartphones mit Android Betriebssystem fast schon zwangsweise auch ein Google-Konto, da dies Voraussetzung für das Herunterladen von Anwendungen aus dem „Google Playstore“ ist. Weitere Beispiele sind

289 Aus: WhatsApp Datenschutzrichtlinie, Stand 19. 12. 2019 (https://www.whatsapp.com/legal?eea=0#privacy-policy, zuletzt abgerufen 02.03.2020)

290 Christopher Wylie: „Mindf*ck – Inside Cambridge Analytica‘s Plot to Break the World“, Profile Books (2019), S. 113f.

Facebook-Konten, Konten auf Instagram oder Twitter, Microsoft-Konten, in Zukunft vielleicht auch Nutzerkonten bei Krankenkassen.

Firmen wie beispielsweise Facebook oder Google weiten die eigene Datensammlung über den Kreis ihrer unmittelbaren Nutzer zudem weit aus, indem sie Betreibern von Webseiten kostenlose „Analyse-Werkzeuge“ als Dienste anbieten, die den Betreibern Aufschlüsse über das Nutzerverhalten der Besucher ihrer Seite liefern (Facebook analytics, Google analytics, Facebook Pixel, web beacons[291]…). Die für die Analyse gesammelten Daten werden dabei typischerweise an Facebook oder Google gesandt und dort ausgewertet und vergrößern damit gleichzeitig die Datensammlung der genannten Firmen. Damit wird jeder Website-Betreiber, der entsprechende Analysetools auf seiner Seite verwendet, zu einem informellen Datenzuträger der Firmen, deren Geschäftsmodell auf der personenbezogenen Profilerstellung und deren kommerzieller Verwertung beruht. Ein Geschäft mit der Handelsware „Manipulierbarkeit“.

Eine interessante Nebenbeobachtung ist dabei, dass es mit „VKontakte“/„VK“ inzwischen auch ein einflussreiches russisches virtuelles „soziales Netzwerk“ gibt, das sich etwaiger Regulierung oder Sanktionierung nach Akten „informationeller Kriegsführung“ weitgehend entzieht. Im Licht der oben wiedergegebenen Berichte über das „Projekt Lakhta“ ist davon auszugehen, dass auch hier das auf persönlicher Datenpreisgabe und -verknüpfung beruhende Wesen virtueller „sozialer Netzwerke“ und die Möglichkeit der gezielten Ansprache/ Manipulation angepasst an bestimmte Profile als attraktives Operationsmedium geheimdienstlicher Tätigkeiten genutzt werden. Der inneren Logik nach auch zur Sammlung personenbezogener Daten mit dem Ziel, die Integrität demokratischer Prozesse zu untergraben und diese mittels datengeleiteter Kampagnen zu manipulieren.

Tatsächlich ist mit Blick auf das oben erwähnte Überwachungssystem „SORM“ davon auszugehen, dass der russische Staat Zugriff auf die bei VK gespeicherten und verarbeiteten Daten hat und regelmäßig Nutzerprofile erstellt. Tatsächlich sind die Anbieter in der Russischen Föderation zur mehrmonatigen Vorratsdatenspeicherung verpflichtet, sowie dazu, für verschlüsselte Daten „Hintertüren“ für den Staat einzurichten oder den staatlichen Behörden die Schlüssel zugänglich zu machen. Unter anderem durch das „Gesetz über ein Autonomes Internet“ von 2019 wurde die Zugriffsmöglichkeiten des russischen Staates weiter ausgebaut[292]. Dasselbe Gesetz führt übrigens eine eigene „Adressliste“ für Internetadressen (DNS-Liste) ein und verpflichtet die Internet-Anbieter, den internationalen Internetverkehr über staatlich kontrollierte Knotenpunkte (IXPs) laufen zu lassen. Dadurch erhält die russische Staatsführung, über sogenannte „Kill-Switches“ prinzipiell die Möglichkeit, den russischen Teil des Internets in ein nach außen abgeschottetes Intranet („RuNet“) zu verwandeln[293]. Im Zweifelsfall auch, um der Forensik oder Vergeltung nach Cyberangriffen zu entgehen.

Aber es muss noch einmal betont werden, dass auch ohne staatlichen Eingriff die Manipulierbarkeit und Manipulation der Nutzerinnen und Nutzer von Diensten wie Facebook, VK oder Google auf der Grundlage umfassender Datensammlungen nicht Folge einer missbräuchlichen Nutzung der Dienste durch Dritte oder Zufall ist, sondern ihr Charakteristikum und ihre Geschäftsgrundlage. Ihr Geschäftszweck ist die Erstellung personenbezogener Profile und deren Angebot an zahlende Kunden. Die Fassade von kostenlosen Dienstleistungen (Suchmaschine, virtuelles „soziales Netzwerk“, Parallelinternet, Messengerdienst etc.) sind Mittel zu diesem Zweck. Mittel, um die Nutzer zu einer möglichst umfassenden, freiwilligen Datenpreisgabe zu bringen und so in möglichst großem Umfang personenbezogene Daten zu erheben, zu sammeln und zu verarbeiten.

---

291 Unsichtbare Graphiken, oft nur 1x1 Pixel groß, die beim Aufruf einer Website automatisch nachgeladen werden und dadurch Informationen (Metadaten) über den Nutzer preisgeben.

292 V. Wingerter: „Staatliche Regulierung des Internets in Russland“, Tagungsband des 17. Deutschen IT-Sicherheitskongresses des BSI, Tagungsband, S. 229ff. (2021)

293 Ebd.

Schon durch die Rückwirkung durch gezielte, einem bestimmtem Profil angepasste Botschaften bedeuten Profilbildung und Kategorisierung ja nicht einen rein passiven, beschreibenden Vorgang sondern bilden eine Art „Regelschleife“. Die Rückwirkung kann aber noch weiter gehen und gezielt eingesetzt werden. Der wirtschaftliche Erfolg des Geschäftsmodells dieser Firmen hängt ja davon ab, dass die erstellten Profile möglichst zutreffend sind, d.h. dass die an ihre Zielobjekte gerichteten Botschaften der zahlenden Kunden möglichst wirksam sind.

Der inneren Logik entsprechend bedeutet dies, dass grundsätzlich nicht allein eine möglichst genaue, rein passive Kategorisierung und Profilerstellung des Zielobjekts die Erfolgsquote erhöht, sondern auch eine aktive Verstärkung oder sogar Formung und Anpassung von dessen Interessen und Gefühlen an ein (tatsächliches oder vermeintliches) Profil des Nutzers. Dies kann z.B. durch die Auswahl der angezeigten Inhalte und Informationen „angepasst an die Interessen des Nutzers“ erfolgen. Dass den Datenverwertern dieses Potential zur „Manipulation der Manipulierbarkeit“ zumindest bewusst ist, unterstreicht ein Experiment von Facebook an seinen Nutzern, über das die britische Zeitung „The Guardian“ am 29.06.2014 unter dem Titel „Facebook enthüllt Experiment zur Steuerung von Emotionen mithilfe angezeigter Nachrichten“ berichtete[294]. Der Berichterstattung zufolge hat Facebook in einem gemeinsam mit zwei amerikanischen Universitäten durchgeführten Experiment den sogenannten „News Feed“ von knapp 700.000 Nutzern gezielt manipuliert und dann anhand der Inhalte ihrer Online-Beiträge untersucht und gezeigt, wie sich der emotionale Zustand der Nutzerinnen und Nutzer als Folge einer vermehrten Anzeige fröhlicher bzw. einer vermehrten Anzeige trauriger Nachrichten änderte. Ein Ausrutscher? Sagen wir mal: Facebook hat daraus gelernt. Zum Beispiel wie man das Ganze so verfeinert, dass man ganz gezielt Jugendliche identifiziert, wenn sie am verletztlichsten und damit am leichtesten beeinflussbar sind, wie 2017 aufgedeckt wurde[295]...

Bedrohung von Freiheit und Demokratie: Deutschland, USA

Nun fragen Sie sich vielleicht: Schön und gut, aber gibt es jetzt Anhaltspunkte dafür, dass etwas wie die oben erwähnte „informationelle Kriegführung“ gegen die Demokratie auch in Deutschland geschehen ist, oder dass irgend jemand auch nur Interesse daran haben könnte?

Das ist der Fall.

Einen ersten Hinweis gibt ein Bericht des Komitees für Auswärtige Angelegenheiten des Europäischen Parlaments, das 2016 mit Blick auf die gesamte Europäische Union und ihre Nachbarländer berichtet[296]:
„[…] stellt fest, dass die russische Regierung in aggressiver Weise eine breite Palette von Werkzeugen verwendet, wie Think Tanks und spezielle Stiftungen (z. B. Russkiy Mir), spezielle Behörden (Rossotrudnichestvo), mehrsprachige Fernsehsender (z.B. RT[297]), Pseudo-Nachrichtenagenturen und -multimediadienste (z. B. Sputnik), […], soziale Medien und Internet-Trolle, um demokratische Werte zu attackieren [to challenge], Europa zu teilen, inländische Unterstützung zu gewinnen, […]; betont, dass Russland bedeutende finanzielle Ressourcen in seine Werkzeuge zur Verbreitung von Propaganda und Desinformation investiert, die entweder vom Staat direkt oder von Kreml-kontrollierten Organisationen und Einrichtungen verwendet werden; unterstreicht […], dass der Kreml politische Parteien und Organisationen innerhalb der EU finanziell unterstützt mit dem Ziel, den politischen Zusammenhalt zu untergraben.[...]“.

294 Robert Booth: „Facebook reveals news feed experiment to control emotions“, The Guardian, 29.06.2014.
295 I. Dachwitz: „Verhaltensbasierte Werbung: Facebook identifiziert emotional verletzliche Jugendliche“, 2.5.2017, netzpolitik.org (https://netzpolitik.org/2017/verhaltensbasierte-werbung-facebook-australien-analysiert-emotionen-und-aengste-von-jugendlichen, zuletzt abgeufen März 2021)
296 A. E. Fotyga: „Report on EU strategic communication to counteract propaganda against it by third parties“, A8-0290/2016 (14.10.2016)
297 RT: Russia Today

Auf Deutschland bezogen ist zu konstatieren, dass es mit Blick auf die Bundestagswahl 2017, sowie auch die Landtagswahl in Baden-Württemberg 2016, offensichtliche Parallelen zu der im Bericht des Sonderermittlers Robert S. Mueller beschriebenen Methoden der Einflussnahme auf den Wahlprozess in den USA durch die russische „Internet Research Agency“ gibt, sowie zu den von der Firma SCL beschriebenen Maßnahmen: Eine Flut von Falschmeldungen mit polarisierenden und gesellschaftlichen Zwist säenden und ihn verstärkenden Inhalten über soziale Netzwerke; der gezielte Versuch, über sog. „Trolle“ und automatisierte Beiträge in sozialen Medien bzw. deren automatisierte Verbreitung gesellschaftliche Debatten zu verschieben; die Diffamierung von Personen des öffentlichen Lebens, insbesondere von Mitgliedern der Bundesregierung; den Versuch, das Vertrauen in die Berichterstattung von Qualitätsmedien zu untergraben („Lügenpresse“) und sie durch unkritische, manipulative und gesteuerte „Nachrichten“quellen zu ersetzen; massive und technisch professionelle Wahlkampfunterstützung durch vermeintlich unabhängige Dritte[298].

Um das Ausmaß gezielter Desinformation zu verstehen, und auch die gesellschaftlichen Folgen, wenn man sich durch sie in Entrüstung oder Hysterie treiben lässt[299]: Lassen Sie uns einen kurzen Blick auf die Landtagswahlen in Baden-Württemberg 2016 werfen, bzw. auf die Zeit davor.
Vielleicht erinnern Sie sich an den „Fall Lisa“[300] (der keiner war)? Ein 13-jähriges Mädchen aus Berlin, Tochter deutsch-russischer Eltern, war vom 11. auf den 12. Januar für 30 Stunden verschwunden. Nachdem sie zunächst behauptet hatte, Opfer einer Entführung durch „Südländer“ geworden zu sein, ergaben die polizeilichen Ermittlungen, dass sie die Nacht bei einem Freund verbracht hatte.
Nicht so in der russischen staatlichen Presse, die unbeirrt von Fakten das gesamte Crescendo der Desinformation durchlief mit dem offensichtlichen Ziel, die Stimmung gegen Migranten aufzuheizen: Zunächst taucht in russischen Medien die Behauptung auf, das Mädchen sei von Migranten vergewaltigt worden, diese Behauptung wird von Propagandasendern wie RT Deutsch verbreitet, sowie über Soziale Netzwerke und rechtsextreme Netzwerke; über Facebook werden Demonstrationen organisiert, an denen sich Neo-Nazis aber auch Mitbürgerinnen und Mitbürger mit russischen Wurzeln beteiligen, u.a. vor dem Kanzleramt; von den Demonstrationen wiederum berichten russische Auslandssender, was wiederum zu einer allgemeineren medialen Berichterstattung führt und schließlich in öffentlichen Äußerungen des russischen Aussenministers Lawrow gipfelt, der raunt, dass die deutsche Polizei und Justiz den Fall wohl aus Gründen politischer Korrektheit vertuschen wollten[301].
Wenig später wurde in Baden-Württemberg gewählt...

Ein Blick nach Sachsen. Auch die Kundgebungen der sog. „Patriotischen Europäer gegen die Islamisierung des Abendlandes“ (PEGIDA) mit ihrem Koordinator Lutz Bachmann werfen Fragen zu möglichen Parallelen zu den USA auf, auch wenn sie hier spekulativ bleiben.
Während das öffentliche politische Engagement Herrn Bachmanns, der zum Zeitpunkt der ersten Kundgebungen in sozialen Netzwerken aktiv war, sich eigentlich nicht schlüssig aus seiner Vita[302] erklärt, passen seine von Brüchen gekennzeichnete Biographie, sowie sein durch familiäre Konflikte, Konflikte mit dem Gesetz und Kriminalität geprägter Werdegang nach seiner Schulzeit an einer Spezialschule der DDR geradezu perfekt in das „Beuteschema“ geheimdienstlicher Personalgewinnung und besitzt eine hinreichend große Schnittmenge mit

298 Gemeint sind hier insbesondere der „Verein zur Förderung der Rechtsstaatlichkeit und der bürgerlichen Freiheiten“ mit seinem Vorläufer „Vereinigung zur Erhaltung der Rechtsstaatlichkeit und der bürgerlichen Freiheiten“, sowie die mit ihm verbundene Schweizer Marketing-Firma „Goal AG“, vgl. z.B. https://de.wikipedia.org/wiki/Verein_zur_Erhaltung_der_Rechtsstaatlichkeit_und_b%C3%BCrgerlichen_Freiheiten (zuletzt abgerufen 19.02.2020).

299 Im Umkehrschluss ein gutes Gegenmittel gegen Desinformation: Gelassenheit und Optimismus.

300 https://de.wikipedia.org/wiki/Fall_Lisa (zuletzt abgerufen März 2021)

301 S. Meister: „The ‚Lisa case‘: Germany as a target of Russian disinformation“, 25.07.2016, NATO Review (https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html, zuletzt abgerufen März 2021)

302 https://de.wikipedia.org/wiki/Lutz_Bachmann (zuletzt abgerufen 19.02.2020)

dem des Unternehmens SCL/Cambridge Analytica[303]. Der Umstand, dass die Kundgebungen in Deutschland ihren Ursprung ausgerechnet in der Stadt nahmen, in der der KGB-Offizier Wladimir Putin von 1985 bis 1990 seinen Dienst, d.h. „politische Aufklärung“[304] oder „Personalgewinnung, Ausbildung in Funkkommunikation und Überwachung von Besuchergruppen“[305], versah, der dabei mit dem Ministerium für Staatssicherheit vernetzt war[306] und 1990 versuchte, einen Spionagering aus ehemaligen Mitarbeitern des Ministeriums für Staatssicherheit aufzubauen[307], sind zumindest bemerkenswert. Herr Bachmann war kurioserweise zur gleichen Zeit Schüler der Sport-Eliteschule „Artur Becker“ in Dresden[308].

In die Zeit von Wladimir Putin als Direktor des russischen Inlandsgeheimdienstes FSB fiel einige Jahre später dann übrigens die Einführung des russischen Überwachungssystems „SORM-2“, mit dem der Geheimdienst Zugriff auf den Internetverkehr bekam[309].

Putin/Lawrow und Deutschland: Im Bezug auf das Verhalten der russischen Führung unter Wladimir Putin gegenüber Deutschland bemerkte schon der Verfassungsschutzbericht 2015: „*Mit ihren breit angelegten [...] Beeinflussungsbemühungen sind die russischen Nachrichtendienste seit vielen Jahren mit hoher Intensität sowohl in Deutschland als auch in der Russischen Föderation gegen deutsche Interessen aktiv.*“[310]

Im Vorfeld der Bundestagswahlen wird 2017 in einer Anhörung vor dem US Senat festgestellt: „*Für ein Russland, das offensichtlich entschlossen ist, Europa und die transatlantische Allianz zu destabilisieren, ist Deutschland die Siegestrophäe: Schwäche Deutschland und du schwächst die Europäische Union und das Europäische Projekt.*“[311] Insbesondere die Partei „Alternative für Deutschland“ wirke dabei als Multiplikator russischer Staatspropaganda, die über Kanäle wie „RT Deutsch“, „Sputnik Deutsch“ und „NewsFront Deutsch“ eingespeist werde, wobei noch nicht absehbar sei, welche genaue Form die Beeinflussungsversuche auf die anstehende Bundestagswahl annehmen würden[312].

Das berichtet erst der rückblickende Forschungsbericht „Make Germany Great again – Einflüsse des Kreml, rechtsextremer und internationaler Akteure auf die deutschen Wahlen 2017“ des „Institute for Strategic Dialogue“ (ISD) und des „Institute of Global Affairs“ der „London School of Economics“ (LSE)[313]:
„*Dieser Bericht stellt die Ergebnisse eines Projekts vor, das Versuche des Kreml sowie andere ausländische Versuche, Einfluss auf die Wahlen in Deutschland 2017 zu nehmen, untersuchte. Das Projekt deckte die Taktiken und Narrative auf, die Kreml-finanzierte Medien, Kreml-freundliche Netzwerke auf sozialen Medien und ein internationales rechtsextremes*

303 Christine Heuer: „Innenansichten eines Manipulateurs“, Deutschlandfunk, 04.11.2019 (https://www.deutschlandfunk.de/cambridge-analytica-innenansichten-eines-manipulateurs.2907.de.html?dram:article_id=462580, zuletzt abgerufen: 19.02.2020)
304 Viktor Timtschenko: „Putin und das neue Russland“, Hugendubel Verlag, Kreuzlingen/München (2003), S. 27f.
305 https://de.wikipedia.org/wiki/Wladimir_Wladimirowitsch_Putin#cite_note-25 (zuletzt abgerufen 19.02.2020)
306 ebd.
307 ebd.
308 https://de.wikipedia.org/wiki/Lutz_Bachmann
309 V. Wingerter: „Staatliche Regulierung des Internets in Russland“, Tagungsband des 17. Deutschen IT-Sicherheitskongresses des BSI, Tagungsband, S. 230 (2021)
310 Bundesministerium des Innern: „Verfassungsschutzbericht 2015“ S. 256
311 C. Stelzenmüller: „The impact of Russian interference on Germany‘s 2017 elections“, 28.06. 2017 (https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/, zuletzt abgerufen März 2021)
312 Ebd.
313 “MAKE GERMANY GREAT AGAIN” Kremlin, Alt-Right and International Influences in the 2017 German Elections“, Institute for Strategic Dialogue (ISD), 2017. Ein Untersuchungsbericht deutscher Institutionen oder Behörden ist mir nicht bekannt.

Netzwerk verwendeten, um den politischen Diskurs während des Wahlkampfs zu verzerren.“[314]

Die Autoren untersuchen dabei die Rolle von drei sich zum Teil überschneidenden Gruppen in der Bevölkerung: rechts-nationalistischen Kreisen, linksorientierten Gruppen sowie russisch-stämmiger deutscher Staatsbürger. Die Untersuchung beruht nach eigenen Angaben auf einem Methodenmix aus Analyse sozialer Netzwerke und investigativem Journalismus. Ein zentrales Ergebnis ist dabei die Aufdeckung „*deutlicher und koordinierter Bemühungen, drei Schlüsselgruppen zu beeinflussen: die nationalistische Rechte, die Linke und die Russlanddeutsche Gemeinschaft*“[315], vor dem Hintergrund einer russlandfreundlichen Grundhaltung und bestehender Institutionen wie des Forschungsinstituts „Dialogue of Civilizations“ in Berlin, dass von einem früheren KGB-Mitarbeiter und Kollegen Herrn Putins, Wladimir Jakunin, geleitet werde[316]. Im Zentrum sehen die Autoren dabei die Partei „Alternative für Deutschland“, die die intensivsten Verbindungen zu Russland unterhalte[317] und hier systematisch Unterstützung erhalte, die der im Untersuchungsbericht des amerikanischen Sonderermittlers Mueller stark ähneln:

„*Es gibt keine direkten Hinweise darauf, dass die AfD finanzielle Unterstützung seitens des Kreml erhalten hat. Jedoch haben viele einzelne Politiker der AfD enge Verbindungen [deep ties] nach Russland und ihre Agenden überschneiden sich oft mit der nationalistischen Agenda Russlands. Die vorliegende Untersuchung hat gezeigt, dass diese Interaktionen häufig sind und eine systematische Unterstützung darstellen [pattern of support]. […] Die AfD bildete eine Allianz zwischen ihrer Jugendorganisation und Jugendorganisation der Partei „Einiges Russland“. Von Anfang an hat die AfD das russische Verhalten bezüglich der Krim unterstützt. Kurz nachdem er Ko-Vorsitzender der Partei wurde, erklärte Alexander Gaulandt, dass die Krim „ursprüngliche russisches Territorium“ sei, das nicht zur Ukraine zurückkehren könne. […] Marcus Pretzell, Abgeordneter für die AfD im Europäischen Parlament […] nahm 2016 an einer Konferenz auf der annektierten Krim teil. Seine Reisekosten wurden vom Veranstalter, dem Internationalen Wirtschaftsforum Jalta getragen, das vom Präsidialamt der Russischen Föderation unterstützt wird. Der russische Oligarch Konstantin Malofeyev, der sich seit 2014 auf einer Sanktionsliste der EU befindet und beschuldigt wird, illegale militärische Gruppen in der Ukraine zu finanzieren, unterhält enge Kontakte mit der AfD. Er unterstützt insbesondere Alexander Gaulandt […]. […] Im August 2017 veranstaltete die AfD in Magdeburg eine Russland-Konferenz. […] Sowohl Redner als auch Gäste bezeichneten Deutschland als ein besetztes Land und Angela Merkel als amerikanische Marionette, die die echten Deutschen durch muslimische Eindringlinge ersetzen wolle. Unter den Teilnehmern waren Aktivisten, die eine Zeitschrift namens „Die Russlanddeutschen Konservativen“ verteilen, eine Neo-Nazi-Broschüre voller Hakenkreuze […], in der aber auch die AfD und ihre Führung vorkam [featured].*“[318]

Hierbei ist anzumerken, dass bereits unmittelbar nach dem Einmarsch russischer Truppen und der Besetzung der Krim 2014 in Athen eine „Krimkonferenz“ durch die auf psychologische Kriegführung spezialisierte Einheit „54777“ des russischen Geheimdienstes GRU organisiert wurde, um die öffentliche Meinung zu beeinflussen[319]. Dort wie auch später wurde gezielt der Kontakt zu kleinen westlichen Parteien und Politikern gesucht, in diesem Fall zu dem späteren griechischen Verteidigungsminister. Dies ist offenbar Teil einer langfristig angelegten Strategie. Auch der Versuch der gezielten Ansprache von Russlanddeutschen ist in diesen Kontext einzuordnen. Über Tarnorganisationen wie z.B. „InfoRos“ oder das „Institut der Russischen Diaspora“ wird gezielt versucht, russischstämmige Mitbürger mit Falsch- und Desinformationen in russischer Sprache zu anzuvisieren[320].

314 Ebd., S. 2
315 Ebd. S. 5
316 Ebd., S. 8
317 Ebd. S. 10
318 Ebd.
319 Aus dem Lagebild 2021 des estnischen Auslandsnachrichtendienstes Välisluureamet: „International Security and Estonia 2021“ (2021).
320 Ebd., S. 61f.

Darüber hinaus weisen die Autoren der oben genannten Studie auf enge Verbindungen rechtsnationalistischer und rechtsextremer deutschsprachiger Medien mit dem „Kreml“ hin. Als Beispiele werden genannt u.a. die Zeitschrift „Zuerst!“, deren Herausgeber mit AfD-Mitgliedern in die Donbass-Region gereist sei und als Beobachter bei dem „Referendum“ auf der Krim gedient habe; die Zeitschrift „Compact“, dessen Gründer eng mit dem russischen „Institut für Demokratie und Kooperation“ zusammenarbeite und Führungspersonen von AfD und PEGIDA im Rahmen sogenannter „Souveränitätskonferenzen“ zusammengebracht habe; die Zeitschrift „Junge Freiheit“, deren Artikel von einem internationalen rechtsextremen Netzwerk [„*the international far right*“] verbreitet worden seien; „Tichys Einblick“, ein Blog dessen gegen die etablierten Parteien und gegen Migranten gerichteten Beiträge durch russischsprachige „Trollkonten“[321] und Putin unterstützende Konten in sozialen Medien verbreitet worden seien; „Epoch Times Germany“, eine Website, die demokratiefeindliche Falschnachrichten und Verschwörungstheorien verbreite und indirekt für die Partei „Alternative für Deutschland“ werbe. Dabei weisen die Autoren darauf hin, dass insbesondere rechtsgerichtete und rechtsextreme Kreis in Deutschland sich im Wesentlichen über soziale Netzwerke „informiert“ hätten. Dort habe es auf der Online-Plattform „Twitter“ bestimmte Konten gegeben, die diesen „Informations“austausch geleitet hätten. Dies seien neben namentlich zuzuordnenden Konten wie denen von Erika Steinbach und Beatrix von Storch vor allem anonyme Nutzer gewesen, welche insbesondere in der Woche vor der Wahl bestimmten Stichworten [hashtags] wie „#fakenews“ und „#MerkelMussWeg“ künstlich ein signifikant höheres Gewicht verliehen hätten [helped push hashtags]. Einer Untersuchung des „Oxford Internet Institute“ zufolge seien auf die AfD mehr Twitter-Aktivitäten entfallen als auf jede andere Partei, in den ersten zehn Septembertagen seien 30% aller deutschsprachigen Twitterbotschaften solche mit spezifischen AfD-Stichworten gewesen[322].

Die Studie weist zudem darauf hin, dass in russischen Sendern wie „Russia Today Deutsch“ und „Sputnik“ systematisch negativ über die Bundesregierung, die Bundeskanzlerin und die deutsche Polizei berichtet worden sei, während die sog. „Alternative für Deutschland“ systematisch als normale Volkspartei dargestellt worden sei. Sie hätten gleichzeitig systematisch eine Plattform für Botschaften der Partei „Alternative für Deutschland“ geboten, wie der Falschinformation, dass „*Vergewaltigungen infolge der Politik von Frau Merkel zunehmen würden*“[323]. Dabei habe sich Material über Sputnik in rechtsextreme Foren durch „*automatisierte Pro-AfD- und Pro-Kreml-Konten*“[324] in sozialen Medien verbreitet. Als Beispiele werden Falschmeldungen über angeblichen Wahlbetrug bei den Landtagswahlen in Nordrhein-Westfalen 2017 sowie das Thema Flüchtlinge/Einwanderung genannt. Genannt wird auch ein Wechselspiel zwischen „Russia Today Deutsch“ und der Website „Russlanddeutsche für AfD“ bei der Verbreitung und Verstärkung verzerrter Berichterstattung und von Falschnachrichten[325]. Einen Einblick in dieses strategische Wechselspiel gibt auch eine Meldung aus dem Jahr 2019, der zufolge ein Mitglied der Partei „Alternative für Deutschland“ in einem Kreml-internen Strategiepapier aus dem Jahr 2017 explizit als aussichtsreicher Kandidat genannt wird der in der Einschätzung „*ein unter absoluter Kontrolle [der russischen Führung] stehender Abgeordneter im Bundestag“* sein werde, aus anderer Quelle werde eine „*materielle oder mediale Unterstützung*“ für seinen Wahlkampf thematisiert[326]. Der Betreffende sitzt seit 2017 als Abgeordneter im Deutschen Bundestag.

321 „Troll“: verdeckt agierender Internetnutzer, der in manipulativer Absicht versucht, Debatten zu verzerren oder zu dominieren

322 “MAKE GERMANY GREAT AGAIN” Kremlin, Alt-Right and International Influences in the 2017 German Elections“, Institute for Strategic Dialogue (ISD), 2017, S. 11

323 Ebd., S.12

324 Ebd.

325 Ebd., S. 13

326 M. Wehner: „Kreml setzte offenbar auf AfD-Politiker Frohnmaier“, 05.04.2019, Frankfurter Allgemeine Zeitung (https://www.faz.net/aktuell/politik/inland/kreml-setzte-offenbar-auf-afd-politiker-markus-frohnmaier-16126378.html)

Die Autoren der Studie „ Make Germany Great again – Einflüsse des Kreml, rechtsextremer und internationaler Akteure auf die deutschen Wahlen 2017“ geben ausserdem die Aussagen eines „russischen Hackers“ wieder, demzufolge dieser und dreißig weitere Personen in Russland während des Wahlkampfs automatisierte Konten benutzt hätten, um Botschaften zur Unterstützung der Partei „Alternative für Deutschland“ zu verbreiten, zu einem Preis von 2000 Euro für 15000 Nachrichten [*tweets and retweets*], verbunden mit einer Schätzung der erforderlichen Nachrichtenhäufigkeit, um Stichwörten zugunsten der Partei „Alternative für Deutschland“ künstlich ein größeres Gewicht zu verleihen[327].
Die Autoren der Studie weisen darauf hin, dass gleichzeitig ein internationales rechtsextremes Netzwerk in koordinierter Art und Weise aktiv war: „*Amerikanische ‚alt-right‘ Foren und solche europäische Rechtsextremer bereiteten sich monatelang auf die Wahlen in Deutschland vor. Diese Vorbereitung umfasste das Teilen erfolgreicher Methoden [best practices] anhand vorangegangener Kampagnen zur Wahlbeeinflussung. Konten, die in den USA angesiedelt zu sein schienen, gaben rechtsextremen Aktivisten in Deutschland taktische Hinweise zu Themen wie psychologischer Kriegsführung mit graphischen Botschaften [memetic warfare], der Eröffnung falscher Konten bei sozialen Medien [fake accounts], falsch zugeordneten Konten [parody accounts] und Verschleierungstatiken [obfuscation]. Das Stichwort #MGGA (Make Germany Great Again, eine Abwandlung des Slogans, den Trump während des Präsdentschaftswahlkampfs verwendete) tauchte zwischen 1.7. und 6.9. in 2961 Beiträgen […] auf. Nachrichten mit dem Stichwort #MGGA verlinkten oftmals zu Alternativnachrichten-Seiten wie Daily Stormer und Breitbart. […] Der Daily Stormer, eine offen neo-nationalsozialistische Website forderte ihre Leser auf, den Kontakt mit PEGIDA, Identitären und der AfD zu suchen. Ein rechtsextremer „Discord“-Kanal wurde spezifisch mit der Absicht eröffnet, die Wahlen in Deutschland zu stören, er hat unter seinen Mitgliedern aber Personen aus aller Welt. Der Server des Kanals wurde von dem deutschen rechtsextremen Aktivisten Nikolai Alexander aufgesetzt […]. Das explizit genannte Ziel seines Kanals war es, den größtmöglichen Einfluss [the strongest possible showing] der AfD im Bundestag sicherzustellen‘. Mit Näherrücken der Wahlen wurden internationale rechstextreme Quellen wie Breitbart sowie Kreml-finanzierte Quellen wie Russia Today die Hauptquellen von Inhalten in sozialen Medien innerhalb der extremen Rechten in Deutschland*“.[328]
Die Autoren weisen zudem auf eine abgeschlossene Facebook-Gruppe „Bündnis Deutschland-Russland“ hin, die sowohl Personen aus Russland als auch Mitarbeiter der Partei „alternative für Deutschland“ vereine und Nachrichten verbreite, die sich gegen die etablierten Parteien in Deutschland richteten[329].

Gibt es weitere Hinweise auf Versuche, die Integrität demokratischer Prozesse und insbesondere von Wahlen in Deutschland zu untergraben und sie zu manipulieren, eventuell unter Nutzung personenbezogener Daten?

Das ist der Fall.

So beschreibt der abschließende Untersuchungsbericht des britischen Parlaments zu „Desinformation und ‚Falschnachrichten‘“[330] nicht nur analoge Einflussnahmen russischer Stellen über soziale Netzwerke sowie des amerikanischen Rechtsextremen Stephen Bannon und des o.g. „Politikberatungsunternehmens“ SCL/Cambridge Analytica auf demokratische

327 S“MAKE GERMANY GREAT AGAIN” Kremlin, Alt-Right and International Influences in the 2017 German Elections“, Institute for Strategic Dialogue (ISD), 2017.

328 Ebd., S. 14; der Einfluss Kreml-naher Medien auf Gruppen im linken Parteienspektrum wird in der Studie als deutlich geringer eingeschätzt, während „Russlanddeutsche“ über russischsprachige Sender aber auch soziale Netzwerke wie Odnoklassniki und Facebook (Russkaja Germanija) gezielt und mit dem Ziel einer Unterstützung der sog. „Alternative für Deutschland“ angesprochen worden seien. Die AfD wiederum habe als einzige Partei umfangreiches Wahlkampfmaterial in russischer Sprache zur Verfügung gehabt.

329 Ebd., S. 18

330 „Disinformation and ‚fake news‘: Final Report“, House of Commons, Digital, Culture, Media and Sport Committee, 18.02.2019

Prozesse im Vereinigten Königreich (wie das Referendum zum Austritt Großbritanniens aus der Europäischen Union), sondern erwähnt unter der Überschrift „*Einflussnahmen von SCL auf Wahlen in anderen Ländern“* auch Deutschland:
„Datenanalyse-Firmen haben rund um die Welt eine Schlüsselrolle bei Wahlen gespielt. Unternehmen, die sich mit strategischer Kommunikation beschäftigen, führen oft international Wahlkämpfe durch, deren Finanzierung intransparent ist und die juristische zweifelhafte Methoden verwenden. Wie wir in unserem Zwischenbericht schrieben, gibt das komplexe Beziehungsnetz zwischen den zur SCL (Strategic Communications Laboratory) Gruppe gehörenden Firmen Anlass zur Sorge, und ‚diese Sorgen wurden durch Alexander Nix und die eigenen Verbindungen von SCL zu Organisationen aus dem militärischen, nachrichtendienstlichen und Sicherheitsbereich vergrößert‘. Wir haben die folgenden Wahlkämpfe und Referendumskampagnen hervorgehoben, in die SCL Elections und mit ihr verbundene Firmen involviert waren: Australien, Brasilien, Tschechische Republik, Frankreich, Gambia, Deutschland, […].“[331]

Diee Zeugenaussage von Brittany Kaiser, die als „Direktorin für Programmentwicklung“ im Vertriebsbereich bei Cambridge Analytica arbeitete, llefert weitere Hinweise[332]:
„[…]
Vorsitzender: Es kam die Frage auf, ob es Tätigkeiten im Bezug auf Deutschland gab.

Brittany Kaiser: Oh. Ich war an Vorbereitungen eines Angebots [pitch] im politischen Bereich mit Bezug auf Deutschland beteiligt, aus dem nie etwas wurde, sowie für verschiedene kommerzielle Projekte, bei denen wir für einige den Zuschlag erhielten.

Vorsitzender: An wen richtete sich das Angebot?

Brittany Kaiser: An die CDU.

Vorsitzender: An die CDU?

Brittany Kaiser: Ja.

[…]

Vorsitzender: Zu meinem Verständnis: Sie erwähnten, dass Chris Wylie für SCL Kanada arbeitete.

Brittany Kaiser: Das war der Name für...ich kenne ihn nicht persönlich und auch nicht das Büro von AIQ. Es wurde als „SCL Kanada“ betrachtet. Unser Unternehmen hatte meist ein Geschäftsmodell, bei dem wir uns ein anderes Unternehmen als Partner suchten, und dieses Unternehmen repräsentierte uns als „SCL Deutschland“ oder „SCL USA“. Das war das Modell.

[...]

Brittany Kaiser: Ich war nie in der Position, irgendwelchem Kampagnenmaterial zuzustimmen oder es abzulehnen. Ich war nicht im operativen Kampagnenbereich tätig.[any piece of creative] zuzustimmen

Ian C. Lucas: […] Gab es Beispiele für andere Dinge, bei denen Sie sich unwohl fühlten?

331 Ebd., S. 78
332 Digital, Culture, Media and Sport Committee, oral evidence: Fake News, HC 363, 17.04.2018; S.5 und S. 34f.

Brittany Kaiser: Mir wurde die Einführung bei Kunden angeboten, bei denen ich es ablehnte, sie zu treffen, wie die Alternative für Deutschland und das Wahlkampfteam von Marine Le Pen. Ich habe mich sogar geweigert, mit ihnen auch nur zu telephonieren.

Ian C. Lucas: Aber nicht bei der UKIP?

Brittany Kaiser: Nein, bei UKIP nicht.

Vorsitzender: Darf ich fragen, wer Sie um ein Treffen mit der AfD und Marine Le Pen gebeten hat?

Brittany Kaiser: Möglicherweise dieselbe Person, die uns den Kontakt zur UK Independence Party vermittelt hat; aber ich bin mir nicht sicher, da ich ihnen nicht direkt vorgestellt wurde. Es wurde vorgeschlagen, dass der Kontakt vermittelt werden könnte.

Vorsitzender: Sie sprechen von Steve Bannon, d.h. Ihnen wurde vorgeschlagen, dass Steve Bannon Sie sowohl bei Marine Le Pen als auch bei der Alternative für Detuschland einführen könnte?

Brittany Kaiser: Es war...ich glaube, wir wurden per E-Mail einem der für Werbung zuständigen Mitarbeiter [one of the communications officers] der Alternative für Deutschland vorgestellt Ich müsste nachschauen, wer diesen Kontakt vermittelt hat. […]

Vorsitzender: OK, aber warum glauben Sie, dass Steve Bannon in diesen Vorgang involviert war?

Brittany Kaiser: Weil ich nicht denke, dass Julian Verbindungen zu einer dieser Parteien hatte.

Vorsitzender: Die eine Person neben Steve Bannon, die Verbindungen zu diesen Parteien hat, ist Nigel Farage. Denken Sie dass er…?

Brittany Kaiser: Das ist möglich.

Vorsitzender: Aber das wurde Ihnen nicht mitgeteilt?

Brittany Kaiser: Das wurde mir nicht mitgeteilt, aber ich kann in meinen E-Mails nachsehen, ob eine bestimmte Personen genannt ist, ja.

Vorsitzender: Das wäre sehr hilfreich.“

Bei dem in der Zeugenaussage genannten „communications officer“ handelt es sich möglicherweise um einen der Mitarbeiter der texanischen Firma „Harris Media“, die im Rahmen des Bundestagswahlkampfes 2016/2017 für die Partei „Alternative für Deutschland“ tätig waren, insbesondere auch für ihre digitalen Auftritte in Sozialen Netzwerken[333] [334]. Bei Harris Media handelt es sich um ein extrem rechts gerichtetes, US amerikanisches Medienunternehmen, das, um für sich zu werben, auf seiner Website beispielsweise offen über „erfolgreich“ inszenierte digitale Schmutzkampagnen in Sozialen Medien bei Wahlen in den USA berichtet, sowie über die Manipulation von Internet-Suchergebnissen bzw. der bei Suchanfragen gezeigten Anzeigen in Zusammenarbeit mit Google[335]. Die Firma hat laut

333 Jane Macintosh: „Germany's AfD takes on Trump campaign-linked Harris Media for social media“, Deutsche Welle, 30.08.2017 (https://www.dw.com/en/germanys-afd-takes-on-trump-campaign-linked-harris-media-for-social-media/a-40306137 , zuletzt abgerufen 06.03.2020).

334 Jill Petzinger: „Germany’s far-right party hired an ad agency that worked on the Trump campaign“, Quartz, 01.09.2017 (https://qz.com/1067764/germanys-far-right-afd-party-hires-harris-media-an-ad-agency-that-worked-for-the-trump-campaign/ , zuletzt abgerufen 06.03.2020).

335 https://www.harrismediallc.com/client (zuletzt abgerufen 06.03.2020).

amerikanischer Berichterstattung im Jahr 2016 ein praktisch volksverhetzendes Video produziert, das einen vermeintlichen „Islamischen Staat Deutschland“ voller Menschenhandel, Zwangsheirat und Sprengstofffallen vorstellt[336]. In demselben Jahr hat Harris Media, wie das Unternehmen stolz berichtet, den Wahlkampf des US amerikanischen Senators Ted Cruz unterstützt (einige Jahre später, im Vorfeld des Sturms auf das Kapitol, einer der eifrigsten Unterstützer Donald Trumps bei der Verbreitung von Falschinformationen zur Präsidentschaftswahl 2020). In Cruz‘ Wahlkampf war ein weiteres Unternehmen involviert: Das bereits oben erwähnte Unternehmen „Aggregate IQ“ (AIQ). Bei AIQ handelte es sich um ein Subunternehmen von Stephen Bannons „Cambridge Analytica“/SCL, das für dessen zielgenauen Manipulation von Bürgerinnen und Bürgern mittels speziell angepasster Online-Botschaften, z.B. in virtuellen „sozialen Netzwerken“, die Plattform „Ripon“ entwickelte. Diese Plattform erlaubt es ihren Nutzern, aus einer Unmenge gesammelter und zusammengeführter Daten „*riesige Mengen [universes] von Wählerinnen und Wählern anhand hunderter psychometrischer und verhaltensbasierter Faktoren in (Zielgruppen-)Segmente zu unterteilen.“*[337] Auf die Mitarbeiter von Harris Media bei der Partei „Alternative für Deutschland“ geht möglicherweise auch eine Facebook-Anzeige der Partei zurück, die vor einem Hintergrund blutiger Reifenspuren die Bundeskanzlerin als Verantwortliche für eine Reihe von Attentaten in Europa benennt, darunter den Anschlag vom Breitscheid-Platz in Berlin[338].

In der Ausgabe vom 01./02. Februar 2020 der Süddeutschen Zeitung werden diese Begebenheiten in einem Bericht über/mit Brittany Kaiser nochmals thematisiert[339]:
„*[…] Steve Bannon wollte die Firma der AfD vorstellen, erzählt sie. ‚Meine Kollegen und ich waren nicht gerade begeistert. Bannon hatte uns schon mit den Brexiteers verkuppelt. Der einzige Weg, wie wir Alexander (Nix) von solchen Bannon-Kontakten abbringen konnten, war, wenn wir ihn davon überzeugten, dass man woanders mehr Geld verdienen konnte.[…] Deswegen haben wir ihm ein Treffen mit der CDU verschafft.‘ Doch die Antwort aus Berlin war eindeutig. ‚Die haben gesagt, das ist ja alles sehr beeindruckend, aber lasst uns in Ruhe. Nein. Wir können die Daten so nicht einsetzen. Weil Deutschland die strengsten Datenschutzgesetze der Welt hat.*“

Hieraus lässt sich entnehmen, dass Stephen (Steve) Bannon eine treibende Kraft war und in Konsistenz mit dem oben genannten Bericht versuchte, auf die Wahlen zum Deutschen Bundestag Einfluss zu nehmen; und dass er die Absicht verfolgte, seine Ziele mithilfe der Firma SCL/Cambridge Analytica zu verfolgen, also mit manipulativen Mitteln auf der Basis von aus personenbezogenen Daten gewonnenen Profilen. Ob eine Zusammenarbeit zwischen SCL/Cambridge Analytica bzw. einem Partnerunternehmen und der Partei „Alternative für Deutschland“ trotz der von Frau Kaiser behaupteten persönlichen Weigerung auf anderem Weg dennoch geschehen ist[340], oder ob die beobachteten Parallelen zwischen den Ereignissen in den USA und in Deutschland eher auf die Weitergabe einer „Blaupause“ zurückzuführen sind, lässt sich den zitierten Aussagen nicht sicher entnehmen und bedarf

Methoden informationeller und psychologischer Kriegsführung geg. Demokratien

336 Leif Reigstad: „How an Austin Ad Agency Helped the Alt-Right Rise Again in Germany“, 28.09.2017, Texas Monthly (https://www.texasmonthly.com/the-daily-post/how-an-austin-ad-agency-helped-the-alt-right-rise-again-in-germany/ , zuletzt abgerufen 06.03.2020).

337 Christopher Wylie: „Mindf*ck – Inside Cambridge Analytica‘s Plot to Break the World“, Profile Books, London (2019), S. 166. Um es deutlich zu sagen: Bei der „gezielten Anpassung von Botschaften“ geht es nicht um eine „ansprechende Vermittlung politischer Informationen oder parteipolitischer Inhalte“, sondern um die nackte und bewusste Manipulation des freien Willens von Bürgerinnen und Bürgern mit allen verfügbaren Mitteln, um diese durch psychische Gewalt zu einem vom Manipulateur gewünschten, oft angstgeleiteten Verhalten zu bringen, auch wenn dieses ihren eigenen Interessen völlig widerspricht und schadet, um auf diese Weise die Numerik demokratischer Ergebnisse im Sinne des Manipulateurs „hinzubiegen“.

338 Leif Reigstad, loc. cit.

339 Adrian Kreye: „Greta der Daten“, Süddeutsche Zeitung, 01./02. Februar 2020.

340 Ausgehend von der Beschreibung Alexander Nix‘ in Wylies Buch wäre eigentlich nicht zu erwarten, dass er die Weigerung einer Mitarbeiterin akzeptieren oder ihre moralischen Bedenken ihn stören würden.

weiterer Nachforschungen. In jedem Fall aber spielten personenbezogene Daten bzw. deren - von der CDU offenbar abgelehnte - Verwertung offensichtliche eine zentrale Rolle.

Was ist unter der schon mehrfach genannten „psychologischen Kriegführung“, wie sie auch der russische Geheimdienst GRU betreibt, zu verstehen, einer Kriegführung, die gegen Bürgerinnen und Bürger gerichtet wurde, um die Integrität freiheitlich-demokratischer Grundordnungen zu zerstören? Dabei geht es letztlich immer darum, die Willensbildung und Handlungen des Zielobjekts im eigenen Sinn zu manipulieren und möglichst zu steuern. Dafür ist die zentrale Voraussetzung die Erstellung möglichst vollständiger psychologischer und Persönlichkeitsprofile der Zielobjekte, die wiederum möglichst umfassende personenbezogene Datensammlungen voraussetzen.

Eine der Schlüsselfiguren von SCL/Cambridge Analytica, der Datenspezialist und Soziologe Christopher Wylie, beschreibt einige Grundideen der psychologischen Kriegführung in seinem 2019 erschienen Buch[341]: *„[…] es ist erforderlich, seine Ressourcen zunächst auf einige wenige Zielpersonen zu konzentrieren. Das optimiert man dadurch, dass man gute Profile erstellt und die Art von Personen identifiziert, die sowohl empfänglich für neue Gedanken sind als auch gut genug vernetzt, um unsere Gegenerzählung [counternarrative] in ihr soziales Umfeld zu injizieren. Die effektivste Art, eine Sichtweise zu vernichten [perspecticide] ist eine, die das Selbstbild verändert. Dabei versucht der Manipulator, das Selbstbild der Zielperson durch ein von ihm gewähltes zu ersetzen. Das beginnt üblicherweise mit dem Versuch, die Narrative des Gegners zu unterdrücken und schließlich selbst die Informationsumgebung des Zielobjekts zu dominieren. Oftmals beinhaltet das die schrittweise Zerstörung von psychologischen Resilienzfaktoren über einen Zeitraum von mehreren Monaten. Es werden Strategien entwickelt, um im Zielobjekt eine verzerrte Wahrnehmung der Realität zu erreichen, die zu Verwirrung und Einschränkung der Selbstwirksamkeit führt. Die Zielpersonen werden dazu ermuntert, sich die Folgen unwichtiger oder eingebildeter Ereignisse in den düstersten Farben auszumalen, und Gegenerzählungen zielen darauf, diesen die Sinnhaftigkeit zu nehmen, um den Eindruck verwirrender und sinnloser Ereignisse zu bewirken. Gegenerzählungen zielen auch darauf ab, Misstrauen zu säen und zu verstärken, um die Kommunikation mit Anderen, die die Entwicklung des Zielobjekts beeinträchtigen könnten, zu schwächen. […] Das Endziel ist es jedoch, negative Gefühle und Denkprozesse auszulösen, die zu impulsivem, erratischem oder zwanghaftem Verhalten führen. […] Die am leichtesten beeinflussbaren Zielpersonen sind typischerweise diejenigen, die neurotische oder narzistische Züge aufweisen, da sie psychologisch tendentiell weniger widerstandsfähig gegen den Druck von Narrativen sind. […] Dies sind die einfachsten Ansatzpunkte [low-hanging fruit], um die Zersetzung einer größeren Organisation in die Wege zu leiten. Diese Erkenntnis bildete später eine der Grundlagen für die Arbeit von Cambridge Analytica […] Um es klar zu sagen: Hier geht es nicht um irgendeine therapeutische Maßnahme sondern um einen psychologischen Angriff […].* “[342]
Dazu ist zu sagen, dass Christopher Wylie die Firma relativ früh, nach eigener Darstellung, als der Einfluss von Stephen Bannon zunahm, verließ und sich von ihr distanzierte, er letztlich als Hinweisgeber fungierte und sich danach im englischsprachigen Raum - weitgehend erfolglos – für eine juristische Aufarbeitung engagierte.

Der US-Amerikaner Stephen Bannon spielt ideologisch und organisatorisch eine Hauptrolle bei der Entwicklung immer ausgefeilterer Methoden datengesteuerter Angriffe auf die freie Willensbildung und die Grundlagen der freiheitlich-demokratischen Grundordnung. Um deren Bedeutung und Ausmaß einschätzen zu können, ist es notwendig, ihn bzw. seine Motivation zu beschreiben.
Stephen Bannon übernahm ab 2012 eine Führungsrolle in dem Internetportal „Breitbart News“. Diese Website, die als Nachrichtenportal auftritt, zeichnet sich dadurch aus, dass sie einen ideologischen Auftrag ihres Gründers verfolgt. Ihre „Mission“ sieht sie darin, die Kultur

341 Christopher Wylie: „Mindf*ck – Inside Cambridge Analytica‘s Plot to Break the World“, Profile Books, London (2019).
342 Ebd. S. 48f.

insbesondere der USA so „umzuprogrammieren“, dass sie missliebigen politischen Strömungen keine Grundlage mehr biete, auf der sie gedeihen können[343]. Sie meint, sich dabei in einem fundamentalen ideologischen Kampf zu befinden, der alle Mittel rechtfertigt.

Wylie führt quasi aus erster Hand zu Stephen Bannon aus, zu dessen historischen Vorbildern Napoleon Bonaparte, Adolf Hitler und Josef Stalin zählen: „*[… Bannon] bemerkte, dass zornige, einsame weiße Männer sich in extremer Weise mobilisieren ließen, wenn sie sich in ihrer Lebensweise bedroht fühlten[344]. Bannon realisierte die Macht, die in der Kultivierung des Frauenhasses sexuell deprivierter Männer lag. Ihre nihilistische Wut und ihr Gerede von „Aufständen der Betas“[345] brodelten in den Tiefen des Internets. Sich eine Armee von unfreiwillig sexuell deprivierten Männern heranzuzüchten, würde aber nicht für die Bewegung, von der er fantasierte, ausreichen.*“[346] Solche Personen ließen sich vermutlich auch anhand der Dokumentation in personenbezogenen medizinischen Daten identifizieren.

Die Lösung fand Stephen Bannon in der Firma „SCL Group“ und ihrer Expertise in informationeller und psychologischer Kriegführung. Gemeinsam mit Alexander Nix konnte Stephen Bannon den rechtskonservativen US amerikanischen Milliardär Robert Mercer davon überzeugen, diese Idee zu finanzieren. Dies führte zur Gründung von Cambridge Analytica als Tochterfirma der SCL Gruppe.

Wylie schreibt: „*Bannon hatte die Kontrolle über die Firma übernommen, und er war ein ehrgeiziger und überraschend ausgefeilter Kulturkämpfer. […] Jedes Bewußtsein setzt sich aus vielen Facetten zusammen. Und Bannons neuer Job war es, herauszufinden, wie man die Leute entsprechend ins Visier nehmen konnte. […] Verbitterte Konservative hatten das Gefühl, keine ‚echten Männer‘ mehr sein zu können, weil die Frauen sich auf einmal nicht mehr mit Männern verabredeten, die sich so verhielten, wie sich Männer über Jahrtausende verhalten hatten. Sie waren gezwungen, ihr wahres Selbst aus Rücksicht auf die Gesellschaft zu verstecken – und waren darüber stinksauer. In ihrer Wahrnehmung hatte der Feminismus die ‚echten Männer‘ eingesperrt. Das war demütigend, und Bannon wusste, dass es keine mächtigere Kraft gibt als einen gedemütigten Mann. Das war ein Gemütszustand, den er unbedingt erkunden (und ausnutzen) wollte. […] Viele dieser leicht entflammbaren jungen Männer waren bereit, die Gesellschaft bis auf die Grundmauern niederzubrennen. Bannon unternahm es, Ihnen mit Breitbart ein Sprachrohr zu geben, aber sein Ehrgeiz ging weiter. Er sah diese jungen Männer als frühe Rekruten seines zukünftigen Aufstands*“[347]

Um diesen und andere Gemütszustände, psychologische Schwächen und Persönlichkeitsmerkmale zur systematischen Manipulation von Bürgerinnen und Bürgern und damit demokratischer Prozesse möglichst effektiv zu nutzen, ging Stephen Bannon‘s Firma systematisch vor und entwickelte und verfeinerte ihre Werkzeuge in einem fortwährenden Entwicklungsprozess: „*Als Cambridge Analytica im Sommer 2014 aus der Taufe gehoben wurde, war es Bannons Ziel, die Politik durch Veränderung der Kultur zu ändern; Daten von Facebook, Algorithmen und Narrative waren seine Waffen. Zunächst verwendeten wir Fokusgruppen[348] und qualitative Beobachtungen um an die Wahrnehmungen einer bestimmten Bevölkerungsgruppe heranzukommen und zu erfahren, was ihnen wichtig war […]. Dann entwickelten wir Hypothesen darüber, wie sich ihre Meinungen verändern lassen*

343 Ebd. S. 62.

344 Der Autor bezieht sich hier auf die teils drastischen Reaktionen der „Gamerszene“ auf die Kritik von Frauen an einem aus ihrer Sicht in der Szene grassierenden Frauenhass („Gamergate“).

345 (Selbst-)Bezeichnung für angeblich als unattraktiv empfundene Männer, die im Unterschied zu den „Alphas“ vermeintlich keine Chancen bei Frauen hätten, wobei an deren Ablehnung u.a. der Feminismus Schuld sei. Vgl. a. Die Ansichten des Attentäters von Hanau.

346 Ebd. S. 62

347 Ebd. S. 116f. & S. 118

348 In einer Fokusgruppe lässt der Beobachter die Teilnehmenden ausgehend von einem bestimmten Thema möglichst frei diskutieren, um so möglichst unverfälscht ihre Einstellungen und Überzeugungen kennenzulernen.

könnten. Cambridge Analytica testete diese Hypothesen dann an mit Querschnitten der Zielgruppe – in Online-Foren oder Versuchen – um herauszufinden, ob die Hypothesen den vom Team anhand der vorliegenden Daten erwarteten Effekt hatte. Wir zogen auch Facebook-Profile heran und suchten nach Mustern, um einen Algorithmus basierend auf neuronalen Netzen zu entwickeln, der uns bei den Vorhersagen unterstützen sollte. Ein kleiner Teil der Bevölkerung weist Züge von übersteigerter Selbstwahrnehmung (Narzismus), rücksichtslosem Egoismus (Machiavellianismus) und extremer Gefühllosigkeit (Psychopathie) auf. […] Anhand der Daten, die Cambridge Analytica gesammelt hatte, konnte das Team Personen identifizieren, die neurotisch waren und Züge aus diesem ‚finsteren Dreigestirn' aufwiesen, sowie diejenigen, die anfälliger für impulsive Wutausbrüche und verschwörungstheoretisches Gedankengut waren als der Durchschnittsbürger. Cambridge Analytica sprach sie speziell an, indem sie über Facebook Gruppen, Anzeigen oder Artikel Narrative in Umlauf brachte, von denen das Unternehmen wusste, dass sie die sehr kleinen Segmente der Bevölkerung, die diese Züge aufwiesen, aufstacheln würden. Cambridge Analytica wollte die Leute provozieren, damit sie aktiv werden [to get them to engage]. […] Im Sommer 2014 begann Cambridge Analytica bei Facebook und auf anderen Plattformen falsche Seiten zu erstellen, die aussahen wie echte Foren, Gruppen oder Nachrichtenkanäle. Das war eine völlig übliche Taktik, die SCL, das Mutterunternehmen von Cambridge Analytica, in allen seinen Operationen in anderen Teilen der Welt schon verwendet hatte. […] Das Unternehmen machte das auf lokaler Ebene, indem es rechte Seiten mit allgemein gehaltenen Namen aufsetzte […]. Entsprechend dem Facebook-Algorithmus erschienen diese Seiten in den Nachrichtenleisten der Leute, die zuvor bereits ähnliche Inhalte mit einem „Like" versehen hatten. Sobald Nutzer den Gruppen von Cambridge Analytica beitraten, wurden Videos und Artikel gepostet, die die Nutzer weiter provozieren und anstacheln sollten. In den Unterhaltungen auf der Gruppenseite ging es hoch her, wobei sich die Leute gemeinsam darüber ausließen, wie furchtbar oder ungerecht irgendetwas sei. Cambridge Analytica gelang es, soziale Barrieren zu überwinden und Beziehungen zwischen den Mitgliedern der Gruppe zu etablieren und zu entwickeln. Und dabei wurden die Botschaften die ganze Zeit getestet und verbessert, um die Aktivierung [engagement] zu maximieren. Damit verfügte Cambridge Analytica über Nutzer die 1. sich selbst mit einer extremen Gruppe identifizierten, 2. ein aufmerksames Publikum darstellten und 3. mithilfe von Daten manipuliert werden konnten. In der Berichterstattung wurde oft der Eindruck erweckt, dass Cambridge Analytica viele Menschen gezielt angesprochen habe. Tatsächlich wurden gar nicht so viele gezielt angesprochen […] weil die meisten Wahlen Nullsummenspiele sind: wenn Du eine Stimme mehr bekommst als der Andere, hast Du die Wahl gewonnen. Cambridge Analytica brauchte nur einen schmalen Ausschnitt der Bevölkerung zu infizieren und dann zuzusehen, wie sich das Narrativ verbreitete."[349]

Aus dieser Schilderung möchte ich zwei Umstände hervorheben, die hier besonders relevant sind: Zum Einen wird deutlich, dass es immer darum ging, die Schwachstellen der Zielpersonen zu finden und bestimmte Neigungen und Merkmale aus den Daten(kombinationen) zu rekonstruieren – mit einem Satz personenbezogener medizinischer Daten ist man praktisch sofort am Ziel, insbesondere wenn er Daten zu psychiatrischen Diagnosen und Medikationen enthält. Ein zweiter Umstand ist der, dass es aufgrund des Mehrheitswahlrechts in den USA (und dem Vereinigten Königreich) ausreichte, eine vergleichsweise kleine Gruppe so zu manipulieren, dass sie das gewünschte Abstimmungsverhalten zeigen (oder auch sie von einer Teilnahme an der Wahl abzuhalten). In Deutschland wäre es im Umkehrschluss aufgrund des (teilweisen) Verhältnis-Wahlrechts von besonders großem Interesse, möglichst viele Leute manipulieren zu können, d.h. eine möglichst noch umfassendere und sensiblere Datensammlung zu haben. Bevorzugtes Ziel wäre also zum Beispiel eine zentrale Sammlung personenbezogener medizinischer Daten.

Der weitere Verlauf der Operationen beinhaltete dann den Schritt von der digitalen in die reale Welt: „*Sobald eine [digitale] Gruppe eine hinreichend große Mitgliederzahl erreichte, organisierte Cambridge Analytica ein physisches Event. Cambridge Analytica Teams suchten*

349 Ebd. S. 119ff.

kleine Räumlichkeiten aus […] damit die Gruppe das Gefühl hatte, größer zu sein. Wenn man z.B. tausend Leute in einer [digitalen] Gruppe hat, was für Facebook-Verhältnisse eher Mittelmaß ist, sind es immer noch einige Dutzend, wenn auch nur ein kleiner Bruchteil wirklich kommt. In einem kleinen Café sind vierzig Leute eine riesige Menge. Die Leute kamen und fanden Gleichdenkende voller Zorn und Paranoia vor. Das gab ihnen natürlich das Gefühl, Teil einer riesigen Bewegung zu sein und ermöglichte es ihnen, sich gegenseitig in ihren Verfolgungs- und Verschwörungsängste zu bestärken. Manchmal agierte jemand von Cambridge Analytica als ‚Verbündeter' - eine im militärischen Bereich übliche Taktik um Ängste in einer Zielgruppe heraufzubeschwören. Aber meistens entwickelten sich die Situationen von ganz alleine. Die Eingeladenen waren aufgrund ihrer Merkmale ausgesucht worden, daher wusste Cambridge Analytica im Allgemeinen wie sie aufeinander reagieren würden. […] die Leute empörten sich immer mehr über das, was sie als ‚Wir gegen Die da' betrachteten. Was als digitale Phantasie begonnen hatte, während sie spät nachts alleine in ihrem Schlafzimmer auf irgendwelche Links klickten, wurde ihre neue Realität. Das Narrativ stand direkt vor ihnen und sprach mit ihnen, in Fleisch und Blut."[350]

Vor dem Hintergrund dieser Insider-Beschreibung drängen sich offensichtliche Parallelen auf, zum Beispiel mit Blick auf die „Pegida"-Veranstaltungen und ihre „Ableger", auch mit Blick auf die Beschreibungen der Aktivitäten der staatsnahen St. Petersburger „Internet Research Agency" im Bericht des US amerikanischen Sonderermittlers Robert S. Mueller.

Die Parallelen zur Entstehung der Pegida-Veranstaltungen bedürften einer genaueren Untersuchung, ob es eine reine Konzidenz ohne kausalen Zusammenhang ist, oder ob bereits 2014 Deutschland gezielt durch Stephen Bannon oder russische Stellen attackiert wurde, oder ob vielleicht Herr Bachmann, der einige Zeit in Südafrika gelebt hatte, per Zufall in eine englischsprache Facebook-Gruppe „gerutscht" ist.

Die Parallelen zu den Aktivitäten von russischer Seite insgesamt sind mit an Sicherheit grenzender Wahrscheinlichkeit kein Zufall. So beschreibt der SCL-Insider Christopher Wylie in seinem Buch die verschiedenen Verflechtungen von Cambridge Analytica mit russischen Stellen. Diese Verflechtungen betreffen die Dienste russischer Hacker[351]; den Wissenschaftler der Universität Cambridge, Aleksandr Kogan, der für Cambridge Analytica die Software („App") entwickelte, die im Rahmen einer mit einem geringen Entgelt verbundenen „wissenschaftlichen" Erhebung die Facebook-Profile der Teilnehmenden und ihrer Facebook-"Freunde" zur weiteren Verwertung kopierte, der psychologischer Studienleiter für Cambdridge Analytica war, und der gleichzeitig inhaltlich ähnlich gelagerten Tätigkeiten insbesondere zum „finsteren Dreigestirn" in St. Petersburg und Moskau nachging[352]; Fragen zu Einstellungen gegenüber Putin und der Krim, die im Lauf des Jahres 2014 ohne für Wylie erkennbaren Grund in den Feldstudien von Cambridge Analytica auftauchten; das aus Sicht von Wylie nicht recht erklärliche Interesse der russischen Firma Lukoil an den Werkzeugen und Daten von Cambridge Analytica[353], denen sich Alexander Nix, der formale Leiter von Cambridge Analytica und SCL Elections, andiente[354] und über die er später erfahren habe, dass sie mit dem russischen Geheimdienst FSB im Bereich Informationsbeschaffung zusammenarbeite[355].

Die Werkzeuge zur Manipulation freiheitlich-demokratischer Gesellschaften mittels datenbasierter Erstellung von Persönlichkeitsprofilen sind also spätestens seit 2014 in der Welt und wurden von verschiedenen Seiten bereits zu Angriffen auf demokratische Gesellschaften und ihre Grundlagen eingesetzt. Man muss davon ausgehen, dass diese

350 Ebd. S. 122

351 Hacker wurden laut Wylie zum Beispiel genutzt, um in Nigeria im Rahmen einer dortigen Wahlbeeinflussung an die medizinischen Daten eines Kandidaten zu gelangen.

352 Ebd. S. 138

353 Ebd. S. 133ff.

354 Ebd.

355 Ebd. S. 150.

Werkzeuge seitdem weiter entwickelt und verfeinert wurden bzw. bis zur nächsten großen Wahl noch werden, und zwar unter Hinzuziehung aller irgendwie verfügbaren Sammlungen personenbezogener Daten.

Einen Einblick in das Ausmaß der Datensammlung und -zusammenführung bereits im Jahr 2014, und das selbst ohne staatliche Ressourcen gibt eine Episode, die Wylie in seinem Buch schildert: „*Jucikas hielt einen kurzen Vortrag, bevor er sich an Bannon wandte. ‚Sagen Sie einen Namen.' Bannon guckte amüsiert und nannte einen Namen. ‚Okay, nennen Sie mir jetzt einen Bundesstaat.' - ‚Keine Ahnung', sagte er, ‚Nebraska.' Jucikas gab eine Suchanfrage ein, und eine Liste von Links erschien. Er klickte auf eine der vielen Personen dieses Namens in Nebraska – und da war alles über sie, direkt auf dem Bildschirm. Ihr Photo, wo sie arbeitet, ihr Haus. Ihre Kinder, auf welche Schule sie gehen, welches Auto sie fährt. Im Jahr 2012 hatte sie für Mitt Romney gestimmt, sie mag Kate Perry, sie fährt einen Audi, sie ist eher einfach… und so weiter, und so weiter. Wir wussten alles über sie – und für viele Eintragungen wurden die Informationen in Echtzeit aktualisiert, d.h. wenn sie etwas auf Facebook postete, konnten wir dabei zusehen. Und wir hatten nicht nur ihre Facebook-Daten, die führten wir zusammen mit allen Daten, die wir von kommerziellen oder staatlichen Stellen gekauft hatten. […] Wir hatten Daten über ihre Darlehensanträge, wir wussten wieviel Geld sie verdient, ob sie eine Waffe besaß. Wir hatten Informationen aus ihrem Bonusmeilenprogramms, daher wussten wir, wieviel sie flog. Wir konnten sehen, ob sie verheiratet war (war sie nicht). Wir hatten eine Vorstellung von ihrem Gesundheitszustand. Und wir hatten ein Satellitenbild ihres Hauses, ganz einfach per Google Earth. Wir hatten ihr Leben ins unserem Computer geklont. Und sie hatte keine Ahnung.*"[356] Die geschilderte Episode geht noch weiter und mündet schließlich darin, dass zunächst Alexander Nix und dann reihum alle Anwesenden zufällig ausgewählte, nichtsahnende Personen anrufen und ihnen anhand der über sie gesammelten Daten Fragen stellen.

Die Schlüsselfigur Stephen Bannon wird von Wylie folgendermaßen charakterisiert: „*[Bannon] wollte, dass Cambridge Analytica noch weiter ging – und finsterer wurde.. Er wollte die Formbarkeit der amerikanischen Psyche testen. Er drängte uns, Fragen in unsere Forschung aufzunehmen, die letztlich rassistisch voreingenommen waren, um zu sehen, wie weit er Leute bringen konnte zu gehen. Bannon glaubte daran, dass die Bürgerrechtsbewegung das ‚freie Denken' in Amerika eingeschränkt hatte. Er war entschlossen, die Leute zu befreien, indem er die vermeintlichen ‚unbequemen Wahrheiten' über Rassen enthüllte. […] In vielerlei Hinsicht stellte ‚Gamergate' einen konzeptionellen Rahmen für Bannons rechtsextreme Bewegung dar, da er wusste, dass es eine Unterströmung von Millionen leicht erregbarer, zorniger junger Männer gab. Üble Nachrede und Pöbelei [trolling and cyberbullying] im digitalen Raum wurden Schlüsselwerkzeuge der extremen Rechten. Aber Bannon ging weiter und sorgte dafür, dass Cambridge Analytica viele der Taktiken hochskalierte und einsetzte, die auch bei häuslichen Übergriffen zum Einsatz kommen, um die Widerstandsfähigkeit von Opfern zu erodieren. Bannon verwandelte Cambridge Analytica in ein Werkzeug für automatisierte Pöbeleien und hochskalierte psychologische Übergriffe. […] Bannon ging es darum, die hässlichsten Vorurteile der amerikanischen Psyche zu bestätigen und diejenigen, die sie besaßen, davon zu überzeugen, dass sie die Opfer seien, dass man sie schon viel zu lange gezwungen hätte, ihre wahren Gefühle zu unterdrücken. […] Bannon wollte, dass sie [die vermeintlich benachteiligten Teile der jungen Generation] ihre Rolle in seiner revolutionären Prophezeiung erkennen – dass sie eine historische ‚Wende' anführen und die ‚Künstler' seien, die nach ihrer ‚großen Auflösung' das Bild einer neuen, sinnerfüllten Gesellschaft malen würden. […] Für Bannon war diese Bewegung dazu bestimmt, sein großes Werk zu sein. […] Aber Bannon brauchte eine Armee, um das Chaos zu entfesseln. Aus seiner Sicht war es ein Aufstand, und um totale Loyalität und totalen Einsatz zu bewirken, war er bereit, jedwedes Narrativ zu verwenden, das wirkte. […] Während meines letzten Gesprächs mit Bannon sagte er zu mir, dass man, um die Gesellschaft fundamental zu verändern, ‚alles zerstören' müsse. Und genau das wollte er tun […]. Er wollte die Menschen von einem kontrollierenden Verwaltungsstaat befreien, der ihnen Entscheidungen abnahm*

356 Ebd. S. 109f.

und ihnen damit die Sinnhaftigkeit ihres Lebens nahm. Er wollte alles ins Chaos stürzen um die Diktatur der Sicherheit einer staatlichen Verwaltung zu beenden.“[357]

Verbindung von Akteuren informationeller Kriegsführung und rechtsextremer Netzwerke zu Parteien im Deutschen Bundestag

Wenngleich die von Christopher Wylie wiedergegebenen Schilderungen sich auf die USA beziehen, zeigt das „Engagement“ von Stephen Bannon im Umfeld von Wahlen in Europa, dass sich seine Pläne zur Beseitigung der verfassungsmäßigen Ordnung, der freiheitlichen Demokratie nicht nur auf die USA bezieht. Speziell für Deutschland demonstriert dies beispielsweise der Hinweis von Brittany Kaiser auf die angestrebte Zusammenarbeit zunächst mit der CDU, dann mit der Partei „Alternative für Deutschland“.
Anfang März 2018 wurde zudem von einem Treffen von Alice Weidel von der Partei „Alternative für Deutschland“ mit Stephen Bannon in einem Züricher Hotel für ein Beratungsgespräch zu „politischer Strategie und alternativen Medien“ berichtet[358] [359]. Im April 2019 im Vorfeld der Europawahl, lud die Partei „Alternative für Deutschland“ Stephen Bannon zu einer „Medienkonferenz“ in Berlin im Vorfeld der Europawahl ein, um zu diskutieren, wie man „in Zukunft Informationen besser und effizienter verpacken“ könne, es habe eine Einladung in Räumlichkeiten des Bundestags gegeben[360]. Es ist daher davon auszugehen, dass das gegen die verfassungsmäßige Ordnung Deutschlands und damit gegen unser Recht auf freie Entfaltung der Persönlichkeit gerichtete Interesse Stephen Bannons und seines Netzwerkes unverändert vorhanden ist.

Zusammenfassend lässt sich rekonstruieren, dass eine Einflussnahme auf die Wahlen zum Deutschen Bundestag 2017 stattgefunden hat, und dass sich ähnlich wie bei den Präsidentschaftswahlen in den USA ein undurchsichtiges Geflecht entwickelt hat. Ein Geflecht, in das russische staatliche oder staatsnahe Akteure, eine inländische politische Gruppierung, die mit allen Mitteln die Macht erringen will („Alternative für Deutschland“) und dabei von einem internationalen rechtsextremen Netzwerk unterstützt wird, besagtes Netzwerk und international agierende Dienstleister für Profilerstellung und Manipulation demokratischer Prozesse miteinander verstrickt waren und wechselwirkten.
Eine zentrale Rolle gespielt haben dabei neben breiter gestreuten Desinformation und Manipulation über Massenmedien auch auf Basis personenbezogener Daten erstellte Profile und die mit ihnen einhergehenden Möglichkeiten zur zielgenauen Ansprache über soziale Medien.

Ob es sich dabei um einen Teil des im Mueller-Bericht erwähnten „Projekts Lakhta“ handelt und wie dieses mit den Bestrebungen des rechtsextremen Netzwerks um Stephen Bannon interagiert, bedarf einer näheren Untersuchung. Allerdings ist nicht zu erkennen, dass sich die Bedrohungslage heute entspannter darstellt, im Gegenteil. Die Anti-Desinformationsdatenbank des Europäischen Auswärtigen Dienstes füllt sich praktisch täglich mit Einträgen zur Verbreitung von Falschinformationen und Desinformationsversuchen insbesondere russischer Stellen[361]. Besonders perfide ist dabei die Flut an Falschinformationen zur Covid19-Pandemie, die deren Bekämpfung erschwert und damit letztlich Menschenleben fordert. Eine Flut, die zuverlässig ihren Weg in rechtsextreme Netzwerke und das Umfeld von Parteien wie der „Alternative für Deutschland“ findet.

Um sich ein Bild vom Ausmaß der strategisch angelegten Desinformationskampagnen zu machen: Laut Europäischem Auswärtigen Dienst wurden zwischen Ende 2015 und Anfang

357 Ebd. S. 132
358 Elizabeth Schumacher: „Steve Bannon meets AfD's Alice Weidel during European far-right roadshow“, Deutsche Welle, 07.08.2018 (online unter: https://www.dw.com/en/steve-bannon-meets-afds-alice-weidel-during-european-far-right-roadshow/a-42873730 , zuletzt abgerufen: 06.03.2020).
359 Jill Petzinger: „A leader of Germany’s far-right party is getting advice from Steve Bannon“, Quartz, 07.03.2020 (online unter: https://qz.com/1223621/germanys-far-right-afd-partys-alice-weidel-is-getting-advice-from-steve-bannon/, zuletzt abgerufen: 06.03.2020).
360 „Germany's AfD invites ex-Trump aide Bannon to media conference“, 23.04.2019, Reuters (online unter: https://www.reuters.com/article/us-germany-afd, zuletzt abgerufen: 06.03.2020).
361 https://euvsdisinfo.eu

2021 mehr als 700 Fälle russischer Desinformation registriert, die sich ganz gezielt gegen Deutschland richteten[362]. Mit anderen Worten: Durchschnittlich jeden zweiten bis dritten Tag sind Deutschland und seine Bürgerinnen und Bürger seitens der derzeitigen russischen Führung das Ziel psychologischer Kriegsführung und Desinformation. Seit Jahren.

Dass die bisherigen Versuche der Einflussnahme auf Prozesse der politischen Willensbildung trotz allen gesellschaftlichen Schadens insgesamt weniger erfolgreich waren als in den USA, mag zum Einen auf Unterschiede im Wahlsystem zurückzuführen sein, zum Anderen auf eine im Vergleich bisher doch noch weniger umfassende Sammlung personenbezogener Daten für die deutsche Bevölkerung: Datenschutz schützt Demokratie. Datensparsamkeit und bisheriger Verzicht auf Datenakkumulation haben uns bis jetzt „gerettet".

Wie können wir die Lage zusammenfassen, in der die aktuelle Gesetzgebung ihre Wirkung entfaltet?

Die Lage in Deutschland

Zunächst ist zu erwähnen, dass die vergangenen Jahre sicherheitspolitisch einhergingen mit einer militärischen Aufrüstung der Russischen Armee Richtung Westen, wie der Neugründung eines Panzerregiments (2019) und einer Motorschützen-Division in der Enklave Kaliningrad/Königsberg (2020) als sechster neuer Divisionen in westlicher Richtung[363] und der Verlegung von drei Battalionen in den europäischen Teil Russlands, die mit mobilen Abschussvorrichtungen (Iskander-M) für die neuen Hyperschall-Boden-Boden-Raketen des Typs 9M729 ausgerüstet sind[364]. Diese Kurz-/Mittelstreckenraketen können neben Streu- und Splittermunition auch nukleare Sprengköpfe tragen und führten 2019 zur Aussetzung des INF-Abrüstungsvertrags[365]. Raketen dieses Typs sind laut estnischem Nachrichtendienst auch in Kaliningrad/Königsberg stationiert worden[366] und bedrohen damit auch Deutschland direkt.

Neben diesen militärischen Drohgebärden sind Deutschland wie auch andere Mitglieder der Europäischen Union und der westlichen Staatengemeinschaft aber faktisch fortgesetzt einem nicht-erklärten, tatsächlichen Angriff mit hybriden Mitteln[367] [368] seitens der Führung der Russischen Föderation und ihr nahestehender Institutionen ausgesetzt. Ein Angriff, zu dem neben Verbreitung von Falschinformationen und Desinformation u.a. auch gezielte Hackerangriffe und Datendiebstähle gehören[369], aber auch nicht zuletzt der entlarvende Versuch, den Außenbeauftragen der Europäischen Union auf offener Bühne bloßzustellen[370].

Tatsächlich hilft insbesondere dieses politische Ereignis die langfristige Strategie der aktuellen russischen Führung und deren Spuren zu erkennen. Eine Strategie und Taktik, die - wie ehedem die hämische Mobbing- und Propagandasendung „Der schwarze Kanal" in der DDR - der KGB-Logik der „Zersetzung" des „Gegners" folgt.

362 Europäischer Auswärtiger Dienst: „Vilifying Germany; wooing Germany", 09.03.2021 (https://euvsdisinfo.eu/villifying-germany-wooing-germany/, zuletzt abgerufen März 2021)
363 Lagebild 2021 des estnischen Auslandsnachrichtendienstes Välisluureamet: „International Security and Estonia 2021" (2021), S. 45f.
364 Ebd. S. 46ff.
365 https://de.wikipedia.org/wiki/9K720
366 Lagebild 2021 des estnischen Auslandsnachrichtendienstes Välisluureamet: „International Security and Estonia 2021" (2021), Grafik auf S. 49
367 Naja Bentzen: „Foreign influence operations in the EU", European Parliament Research Service, PE 625.123 (Juli 2018)
368 „EU to take action against fake news and foreign electoral interference", Pressemitteilung des Europäischen Parlaments, 10.10.2019 (https://www.europarl.europa.eu/news/en/headlines/priorities/disinformation/20191007IPR63550/eu-to-take-action-against-fake-news-and-foreign-electoral-interference, zuletzt abgerufen 20.02.2020)
369 Naja Bentzen: „Foreign influence operations in the EU", European Parliament Research Service, PE 625.123 (Juli 2018)
370 C. Tripp: „EU-Diplomatie - Mit leeren und lädierten Händen", Deutsche Welle, 06.02.2021 (https://www.dw.com/de/meinung-eu-diplomatie-mit-leeren-und-lädierten-händen/a-56479213, zuletzt abgerufen Februar 2021)

Der „Gegner“ ist dabei die Europäische Union als weltweit einmaliges Erfolgsmodell des freiwilligen, politischen Zusammenschlusses freiheitlich-demokratischer Staaten als Lehre aus zwei furchtbaren Kriegen. Ein freiwilliger Zusammenschluss, der auf Prinzipen wie Achtung der Menschenrechte, Rechtsstaatlichkeit und individueller Freiheit basiert. Aus Sicht autokratischer Führungen wie in Russland und auch China eine gefährliche Herausforderung[371]. Denn die erfolgreiche Europäische Union konterkariert die Selbstinszenierung der autokratischen Personen und Strukturen als alternativlose väterliche Garanten von Sicherheit und Stabilität in einer vermeintlich feindlich gesinnten Welt. Sie legt schonungslos deren eigenes Versagen bloß und dient zudem als Sehnsuchtsort und Motivation aller nach Freiheit und demokratischer Selbstbestimmung strebenden Bürgerinnen und Bürger.

Konsequenterweise versuchen unterdrückerische Autokraten mit allen Mitteln, die Europäische Union zu verleumden, ihr Bild zu verzerren und ihr in tschekistischer Tradition mit „aktiven Maßnahmen“ und durch die Rekrutierung ideologisch ähnlich gesinnter und nützlicher Gruppen und Parteien im Innern zu schaden[372]. Ganz nach dem Motto jeden Diktators seit Julius Cäsar: „divide et impera - teile und herrsche“.

Diese Strategie, ihre Aktualität und ihre Spuren lassen sich wie mit Lackmus-Papier gut sichtbar machen anhand des Narrativs: „Ich bin zwar gegen die Europäische Union aber natürlich für Europa“.

Dabei handelt es sich um ein Märchen, das bewusst Geographie und Politik miteinander vermischt wie Äpfel und Birnen und dann versucht, sie als Radieschen zu verkaufen. Denn zum Ärger der autokratischen Märchenerzähler *ist* die Europäische Union natürlich Europa im Sinn der Europäischen Idee[373] - nur halt nicht im Sinn ihrer nationalistischen Großmachtphantasien, die sich an geographischen, historischen oder kulturellen Grenzen orientieren...um so mehr versuchen die Märchenerzähler, ihr Märchen mit allen Mitteln zu verbreiten.

Dieses Narrativ zeigte sich unter anderem in der bereits erwähnten Inszenierung anläßlich des Besuchs des EU-Außenbeauftragten und noch expliziter wenig später beim Besuch des finnischen Außenministers in Moskau. Einige Tage zuvor hatte der ewige russische Außenminister Lawrow in einem bizarren Auftritt der Europäischen Union mit dem Abbruch der Beziehungen gedroht, verbunden mit dem sibyllinischen Hinweis: „*Wenn Du den Frieden willst, bereite Dich auf den Krieg vor*.“[374] Außenminister Lawrow, Repräsentant eines Landes, das als Sowjetunion jahrzehntelang halb Europa besetzt gehalten und die Lebensperspektiven und -chancen von Millionen Europäerinnen und Europäern zerstört hatte, wiederholte während der Pressekonferenz in Anwesenheit des finnischen Außenministers die Drohung eines Beziehungsabbruchs, um dann sein Narrativ zu platzieren[375]: „*Die Europäische Union ist nicht dasselbe wie Europa*.“ und fügt hinzu: „*Wir haben viele Freunde, viele ähnlich gesinnte Personen in Europa. Wir werden weiterhin die Beziehungen zu ihnen zum gegenseitigen Nutzen ausbauen*.“ Na prima.

---

371 Vgl. z.B. Lagebild 2021 des estnischen Auslandsnachrichtendienstes Välisluureamet: „International Security and Estonie 2021“ (2021).

372 Wobei es nicht ohne Ironie ist, dass es sich in den 70er und 80er Jahren um linksextreme Gruppierungen bis hin zur RAF handelte und heute um Gruppierungen und Parteien aus dem rechtsextremen Spektrum, die wiederum meinen, sie würden gegen die „linke Ideologie“ der 70er und 80er Jahre antreten...

373 Also der Idee eines in Frieden und Freiheit vereinten Europa, d.h. einer politischen und Wirtschafts- und Wertegemeinschaft, die gemeinsam nach der Verwirklichung von Freiheit, Gleichheit, Demokratie, Rechtsstaatlichkeit und Achtung der Menschenwürde und -rechte für Alle strebt.

374 Deutsche Welle: „Außenminister Lawrow droht mit Abbruch der EU-Beziehungen“, 12.02.2021 (https://www.dw.com/de/au%C3%9Fenminister-lawrow-droht-mit-abbruch-der-eu-beziehungen/a-56545571 , zuletzt abgerufen Februar 2021)

375 A. Rettman: „EU relations are a ‚carcass‘, Russia says“, euobserver, 16.02.2021 (https://euobserver.com/foreign/150943, zuletzt abgerufen Februar 2021)

Begeben wir uns weiter auf Spurensuche: Dasselbe Narrativ wird seit dem Brexit-Referendum in Großbritannen Mantra-artig von der ultrarechten „Conservative Party“ („Tories“) bemüht. So verwehren die inzwischen ultrarechten Tories dem neuen EU-Botschafter in London den Diplomatenstatus. Bezeichnenderweise lautet die Begründung, dass die Europäische Union ja „nur eine Organisation“ sei[376] - eine 180°-Wendung zur eigenen, bisher vertretenen Position, aber ganz im Sinne der derzeitigen russischen Regierung,

Tatsächlich zeigt sich gerade in Großbritannien und den USA besonders deutlich das Dilemma im Umgang mit einer durch Desinformationskampagnen verzerrten Debatte und psychologischer Kriegführung. Fällt man einmal auf sie herein, wird man entweder wider besseres Wissen zu ihrem Verteidiger und treuen Diener, oder man muss die Größe besitzen, seinen Fehler zuzugeben und zu korrigieren. Auch auf das Risiko hin, persönlich das Gesicht zu verlieren. Wenn man diese Größe nicht besitzt, läuft die Gesellschaft Gefahr, sich in Stellvertreterkämpfen sinnlos selbst zu zerfleischen und eine Atmosphäre des Misstrauens zu schaffen. Eine aufgeheizte Atmosphäre, in der die Selbstheilungskräfte der Gesellschaft gelähmt werden und jeder Versuch sachlicher Aufklärung, wie im Fall des berüchtigten Ex-Präsidenten Donald Trump, unter den Generalverdacht einer politisch motivierten „Hexenjagd“ gestellt wird[377].

Gut illustriert wird dieses Dilemma als Folge psychologischer Kriegführung im Lagebild des britischen Parlaments zur Rolle Russlands mit Blick auf das Vereinigte Königreich aus dem Jahr 2020[378]. Dort wird einerseits auf die umfangreiche allgemeine Berichterstattung zu russischem Einfluss insbesondere auf das Brexit-Referendum verwiesen, gleichzeitig beklagen die Abgeordneten die offenbare Unwilligkeit der britischen Sicherheitsbehörden, dem nachzugehen. So hätte der „MI5“ auf Anfrage lediglich eine Kurzantwort geliefert, die nicht mehr als sechs Zeilen umfasste: „*Diese Kürze zeigt uns zum wiederholten Mal die extreme Zurückhaltung der Nachrichten- und Sicherheitsdienste aus Sorge, den Eindruck irgendeiner Einflussnahme auf demokratische Prozesse des Vereinigten Königreichs zu erwecken, insbesondere bei einem so umstrittenen wie dem EU Referendum. Wir wiederholen, dass diese Haltung unlogisch ist; es geht um den Schutz der Prozesse vor Manipulation durch einen feindlich gesinnten Staat […]*.“[379] Gleichzeitig deckt der Bericht die lang andauernde und systematische Strategie der Einflussnahme durch Oligarchen aus dem Umfeld des russischen Präsidenten auf, in der London als „Geldwaschmaschine“ gedient habe: „*Das Geld wurde auch dazu verwendet, den Einfluss auf einen weiten Bereich britischer Einrichtungen auszudehnen – Werbeagenturen, Wohltätigkeitsorganisationen, politische Gruppen, Wissenschaft und Kultur waren alle willige Empfänger russischen Geldes und trugen damit dazu bei, die Weste Russlands reinzuwaschen [‚reputation laundering‘ process]. Kurz gesagt: Russische Einflussnahme im Vereinigten Königreich ist ‚die neue Normalität‘, und es gibt viele Russen mit sehr engen Verbindungen zu Putin, die gut integriert sind in Wirtschaft und Gesellschaft […].*“[380]

Auch wenn man meinen könnte, dass sich niemand mit einem Knüppel freiwillig selbst auf den Kopf schlägt, findet beispielsweise das auf Schwächung der europäischen und damit auch der deutschen Position abzielende Narrativ der russischen Führung auch in Deutschland seine treuen Anhänger und glühenden Verehrer. So trat die Partei „Alternative für Deutschland“ im Jahr 2019 ausgerechnet zu den Wahlen zum Europäischen Parlament mit dem Ziel an, das Europaparlament abzuschaffen, die Europäische Union im Sinne der derzeitigen russischen

376 J. Buchsteiner: „Kein Diplomatenstatus mehr für EU-Botschafter in London?“, Frankfurter Allgemeine Zeitung, 21.01.2021 (https://www.faz.net/aktuell/politik/ausland/kein-diplomatenstatus-mehr-fuer-eu-botschafter-in-london-17158263.html, zuletzt abgerufen Februar 2021)

377 Und möglicherweise im Fall Viktor Orbáns, der sich zunehmend in der Trump‘schen Ecke zu verrennen scheint.

378 Intelligence and Security Committee of Parliament; „Russia“, HC 632 (2020)

379 Ebd., S. 12f.

380 Ebd. S. 15

Führung in einen losen Staatenbund zu verwandeln und andernfalls den Austritt Deutschlands aus der Europäischen Union oder deren Auflösung zu fordern[381] und hat diese Forderungen im Anschluss an einen Besuch beim derzeitigen russischen Außenminister Lawrow in ihrem Wahlprogramm anläßlich der Bundestagswahl 2021 noch einmal wiederholt[382] ...wer solche „Freunde“ hat, braucht keine Feinde mehr[383].

Parallel zu der Verbreitung dieses Narrativs und anderer Akte psychologischer Kriegführung durch die russische Führung erfolgte eine Serie von Terror-Akten[384] mit Mitteln psychologischer Kriegsführung durch ein rechtsextremes Netzwerk um die US Amerikaner Stephen Bannon und Robert Mercer und deren Helfer wie Alexander Nix, die den Boden für schwere staatsgefährdende Straftaten wie die Ermordung des Regierungspräsidenten Walter Lübcke oder die Attentate in Wächtersbach, Halle und Hanau bereitet haben und eine Beseitigung der verfassungsmäßigen Ordnung anstreben. Dazwischen, als dankbaren Empfänger von Unterstützung, willigen Helfer und Bindeglied, gibt es eine inländische politische Gruppierung („Alternative für Deutschland“), die mit beiden Akteursfeldern eng verflochten ist und faktisch ihre politische Agenden bedient. Dadurch ist sie – unwissentlich oder wissentlich – zur Stellvertreterin dieser Akteursfelder im parlamentarischen System geworden.

Na gut, vermutlich wissentlich. Wenn man bedenkt, dass die Parteiführung der Partei „Alternative für Deutschland“ im Vorfeld von Land- und Bundestagswahlen im „Superwahljahr“ 2021 zweimal innerhalb weniger Monate der russischen Führung in Moskau ihre Aufwartung machte[385] [386] [387]. Während nebenan, im Nachbarland Belarus, mit russischer Schützen- und Propagandahilfe Hunderte im Gefängnis verschwanden, weil sie gegen gefälschte Wahlen und für Freiheit und Demokratie auf die Straße gingen, klagte in Moskau der Parteivorsitzende der Partei „Alternative für Deutschland“ als Mitglied des Deutschen Bundestags dem russischen Außenminister öffentlich sein Leid und ließ sich über „Diskreditierung und Diffamierung“[388] in Deutschland aus.

Mit anderen Worten: Er spielte brav die ihm von der derzeitigen russischen Führung in ihrer Inszenierung zugedachte Rolle. Eine Inszenierung, die auf Bild- und Tonmaterial für das Märchen eines hysterischen und heuchlerischen Deutschland abzielte, das seine Bürger unterdrücke und aus reiner Bosheit und anti-russischen Vorurteilen Sanktionen gegen die russische Führung verhängt habe. Denn es ist ja nun auch extrem unwahrscheinlich, dass der Einmarsch russischer Truppen in das Nachbarland Ukraine, also ein nicht erklärter Angriffskrieg, der Abschuss eines Passagierflugzeugs durch russische Luftabwehrraketen oder diverse Attentate auf der Staatsführung missliebige Personen durch den russischen Geheimdienst – gerne mit international geächteten chemischen Kampfstoffen – irgendetwas

381 Alternative für Deutschland: Europawahlprogramm für die Wahlen zum 9. Europäischen Parlament 2019

382 „Radikal in den Wahlkampf“, tagesschau online, 12.04.2021 (https://www.tagesschau.de/inland/innenpolitik/afd-parteitag-migration-corona-101.html, zuletzt abgerufen April 2021)

383 Ein „Fun Fact“ am Rande: Das Farbschema der Partei (weiß, blau und rot) ist lustigerweise dasgleiche wie das der russischen Fahne. Oder natürlich der niederländischen...

384 Dieser Begriff ist hier bewusst gewählt, weil es dem Netzwerk, wie oben beschrieben, darum geht, Angst zu verbreiten bzw. zu schüren mit dem politischen Ziel, die Integrität demokratischer Prozesse und damit die Grundlagen der freiheitlich-demokratischen Grundordnung zu untergraben. Mit ihren Akten psychischer Gewalt bereiten sie dabei Akte physischer Gewalt durch Dritte vor.

385 „AfD Delegation reist erneut nach Moskau“, 09.03.2021, Tagesschau.de (https://www.tagesschau.de/ausland/europa/afd-russland-107.html, zuletzt abgerufen März 2021)

386 „Alice Weidel reist mit AfD-Kollegen nach Moskau“, ZEIT Online, 09.03.2021 (https://www.zeit.de/politik/2021-03/afd-moskau-besuch-russland-alice-weidel-peter-bystron-robby-schlund, zuletzt abgerufen März 2021)

387 „Sergej Lawrow fordert bei Treffen mit AfD einen ‚Neustart‘“, 08.12.2020, ZEIT Online (https://www.zeit.de/politik/ausland/2020-12/russland-afd-moskau-sergej-lawrow-tino-chrupalla, zuletzt abgerufen März 2021)

388 Ebd.

damit zu tun haben könnten. Folgerichtig kritisierte der Parteivorsitzende der Partei „Alternative für Deutschland“ anlässlich seines Besuchs bei der russischen Führung artig die Sanktionen[389] [390]. Überflüssig zu erwähnen, dass die von der russischen Führung wohlwollend geförderte Partei seit 2017 im Deutschen Bundestag vertreten und damit an der Gesetzgebung beteiligt ist.

War sonst noch etwas?

Ach ja, eine für Teile der Bevölkerung tödliche Pandemie und deren Bekämpfung. Sie meinen: Eigentlich ein guter Anlass, sich auf gemeinsame Werte zu besinnen und die hybriden Angriffe für immer einzustellen? Nicht für die (K)alten Krieger in ihren durchgesessenen Sesseln der Macht und ihre Geschwister im Geiste.

Das Jahr 2020 sah im Kontext der Covid-19-Pandemie und den in diesem Zusammenhang getroffenen Schutzmaßnahmen eine offenbar gezielte Unterwanderung eines demokratischen Prozesses, nämlich von Demonstrationen und Meinungsäußerungen, durch rechtsextreme Akteure[391]. Begleitet wurde dies von einem Anschwellen von Verschwörungsmythen und der gezielten Online-Verbreitung von Des- und Falschinformation, die in vielen Fällen auf Akteure zurückzuführen sind, die der russischen Staatsführung nahestehen[392]. Es steht zu vermuten, dass hier neben breit gestreuten Desinformationskampagnen auch profilgestützte Techniken zur individualisierten Manipulation, Ausnutzung psychologischer Schwachstellen und

389 Ebd.

390 Vielleicht werden Sie, liebe Leserin und lieber Leser, zu bedenken geben, dass sich Anfang der 2000er Jahre die ultrarechte Regierung unter George Bush ja ihrerseits alle Mühe gegeben hat, die Friedensdividende der Nach-Wende-Zeit zu verzocken, und dass sie mit ihrer Umdeutung der Wende in ein Nullsummenspiel, ihrer Doktrin der Verachtung internationaler Organisationen und Verträge, „vorbeugender“ Angriffskriegen und Kanonenboot-Politik auf Basis unangefochtener militärischer Dominanz, der Legalisierung von Folter, dem gegeneinander Ausspielen von Partnern und dem Belügen der Weltgemeinschaft nicht speziell förderlich für das vertrauensvolle Zusammenwachsen der Welt in Frieden und Freiheit war. Das stimmt. Sie war eine Katastrophe. Nur - entscheidend sind wie immer nicht die Handlungen und Entscheidungen der Anderen sondern die eigenen. Es ist wie in jeder Beziehung: Wenn einer der Partner offensichtlich den Verstand verliert und sich niederträchtig und gemeingefährlich verhält, ist es weder Einladung noch Entschuldigung oder Freifahrtschein für die Anderen, sich genauso gemein und niederträchtig oder noch schäbiger zu verhalten. Hier trennt sich die Spreu vom Weizen: Wer die Anderen und die Beziehung grundsätzlich schätzt, wer die gemeinsamen Werte ernst meint und lebt - der wird schon aus Selbstachtung diese Werte, gerade wenn sie bedroht sind, umso mehr schätzen, sie bewahren und für sie einstehen. Er wird auf eine bessere Zukunft setzen und versuchen, durch Vorbild zu führen und notfalls Verantwortung für Zwei zu übernehmen. Das war im Großen und Ganzen der Ansatz der Europäischen Union.
Für wen dagegen Partnerschaft nur ungeliebte Einschränkung des eigenen Machtstrebens ist, wer die grundlegenden Werte als lästige Verpflichtung und Beiwerk ohne Bedeutung sieht, wer darauf lauert, die Beziehung scheitern zu sehen - der wird die Gelegenheit dankbar aufnehmen und voller Selbstgerechtigkeit nach Kräften versuchen, den Anderen an Niedertracht noch zu übertreffen, der wird den Schaden der Anderen als eigenen Nutzen betrachten und alle Hemmungen und Skrupel zusammen mit dem moralischen Kompass über Bord werfen. Die jetzige (und damalige) russische Führung unter Wladimir Putin ist leider diesen Weg gegangen statt des europäischen. Aber auch hier gilt zum Glück: Für eine Umkehr ist es nie zu spät. Auch wenn der Weg weit ist und jüngere Beine erfordert.

391 Vgl. Einschätzung des Berliner LfV (z.B Meldung „Rund 2500 Rechtsextreme bei Corona-Demo im August“, https://www.rbb24.de/politik/thema/2020/coronavirus/beitraege_neu/2020/09/berlin-ausschuss-verfassungsschutz-corona-demonstrationen.html, zuletzt abgerufen 16.09.2020) und der GdP (https://www.tagesschau.de/inland/corona-gegner-radikalisierung-101.html, zuletzt abgerufen 16.09.2020)

392 Siehe z.B. Seite des Europäischen Auswärtigen Dienstes zum Thema „Desinformation“: https://euvsdisinfo.eu, insbesondere die „Disinfo Database“ (Stichwort „Corona“)

Identifikation und Zusammenführung von Personen mit einer Disposition zu extremen Einstellungen[393] zum Einsatz kamen wie z.B. 2016 vor der US-Präsidentschaftswahl[394]:

Rufen wir uns das Verfahren in Erinnerung: Beginnend mit einem kleinen, relativ leicht manipulierbaren Personenkreis wird durch Vorspiegelung von dessen scheinbarer Normalität und Repräsentativität gezielt versucht, den Anschluss an und Einbettung in größere Bevölkerungskreise zu schaffen, so dass
1. die Verbreitung von gegen die freiheitlich-demokratische Grundordnung gerichteten Ansichten ein „Selbstläufer“ wird,
2. der Personenkreis statistisch so signifikant wird, dass die Ansichten sich in relevanter Weise auf Wahlergebnisse auswirken, d.h. die strategische, individualisierte Manipulation zu einer Beeinflussung demokratischer Prozesse führt und sie entweder in eine gewünschte Richtung lenkt oder delegitimiert,
3. gesellschaftliche Debatten verschoben und polarisiert und damit Ressourcen von anderen Themen abgezogen werden, so dass in der Gesellschaft möglichst tiefe Gräben aufgerissen werden bis hin zur äußeren Handlungsunfähigkeit der Gesellschaft; das Schwierige dabei ist, dass mittels profilgestützter Manipulation nach Belieben immer neue Gräben aufgerissen werden können, während die Gesellschaft noch damit beschäftigt ist, mühsam die alten zu überbrücken. Das zeigt sich z.B. beim Wechsel der Verschwörungsmythen und Desinformationskampagnen vom Thema „Migration“ zum Thema „Pandemie-Schutzmaßnahmen“.

Erster Schritt ist dabei immer die massenhafte Erstellung und Katalogisierung von Persönlichkeitsprofilen, um Menschen mit geeigneten Dispositionen zu identifizieren, zusammenzuführen und in manipulativer Weise zu adressieren. Bürger und Gesellschaft werden dabei vom Subjekt (des selbstbestimmten Handelns) zum Objekt (der Manipulation durch Dritte), in tiefem Widerspruch zum Grundprinzip einer freiheitlichen, demokratisch verfassten Gesellschaft. Diese ist aber Voraussetzung für die Sicherung unserer Grundrechte.

Dabei ist davon auszugehen, dass manipulative Botschaften nicht ungeplant oder zufällig platziert werden. Propagandabegriffe wie z.B. „Lügenpresse“ und „Wende 2.0“ oder auch das Raunen über eine Verschwörung von „Eliten“ gegen den „kleinen Mann“ entstehen nicht zufällig beim Plakatmalen am Küchentisch. Sie werden vielmehr ganz gezielt kreiert und beispielsweise zum Angriff auf die unter uns verwendet, die oder deren Eltern in der DDR aufwuchsen. Man kann davon ausgehen, dass hier extrem gezielt und planvoll versucht wird, die Lebensgeschichte von Menschen zu missbrauchen z.B. mit dem Versuch, eingeprägte psychologische Denk- und Verhaltensmuster aus der Vorwendezeit zu reaktivieren. Aus einer Zeit als ein Teil von uns in einem Staat lebte, in dem es ein offenes Geheimnis war, dass die Medien zensiert waren und die Staatsführung der DDR sich nicht um die Bürgerinnen und Bürger ihres Staates scherte, sie sie bespitzelte und an der innerdeutschen Grenze von Minen zerfetzen oder erschießen ließ.

Es ist also kein Zufall sondern Mittel der psychologischen Kriegführung, die Lebenserfahrungen der Menschen zu instrumentalisieren, um zu versuchen, sie unbewusst zurückzuversetzen in eine vergangene, möglichst negative Gefühlswelt. Und auch wenn nur ein winziger Bruchteil dieser Masche auf den Leim geht, ist es schlimm. Gefühle von Angst,

393 Ziel ist dabei, ihnen und den ihnen nahe gebrachten Ansichten in der Selbst- und Gesellschaftswahrnehmung ein scheinbar höheres Gewicht und damit ein vemeintlich höheres Maß an „Normalität“ zu verleihen, als sie tatsächlich besitzen. Das Verfahren hatte ich bereits in meinem früheren Vortrag beschrieben, u.a. mit Verweis auf die Darstellungen des ehemaligen Mitarbeiters von Cambridge Analytica, Christopher Wylie: Es werden beispielsweise Menschen mit extremistischen (und z.T. psychologisch auffälligen) Neigungen - die gesamtgesellschaftlich gesehen vermutlich weitgehend isolierte und statistisch insignifikante Einzelfälle darstellen - mittels Profilerstellung gezielt identifiziert, zusammengeführt und sich und Anderen als homogene Gruppe präsentiert, die vermeintlich repräsentativ für die Gesamtbevölkerung sei.

394 Und wie möglicherweise auch vor der vergangenen Bundestagswahl 2017.

Ohnmacht und Aggression beeinträchtigen die Wahrnehmung der Wirklichkeit und erleichtern die Manipulation. Davor müssen wir uns und unser Land schützen – wer entspannt und optimistisch in die Zukunft blickt, lässt sich nicht so leicht ein X für ein U vormachen.

Angriffe auf Institutionen der Demokratie

Jüngster Tiefpunkt der Entwicklung in Deutschland war der – meines Wissens seit den Unruhen in der Weimarer Republik nicht mehr dagewesene – Versuch von mehreren Hundert Personen am 29. August 2020 im Kontext entsprechender Demonstrationen, sich gewaltsam Zutritt zum Sitz des Parlaments, des Deutschen Bundestags zu verschaffen. Diese Mitbürgerinnen und Mitbürger standen dabei ganz offensichtlich unter massivem Einfluss von Verschwörungsmythen und Desinformation, so z.B. dem Glauben, dass amerikanische und russische Soldaten auf dem Weg nach Berlin, die Polizei „übergelaufen“ oder gar der US amerikanische Präsident Donald Trump zur Unterstützung vor Ort sei[395]. Die Gruppe von schließlich mehreren Hundert Personen führte dabei nicht nur demonstrativ Fahnen des Deutschen Kaiserreichs mit sich, die bekanntlich von Rechtsextremen als Stellvertretersymbol für die verbotene Hakenkreuzfahne verwendet werden und die dasselbe Farbschema aufweist. Auf Bildern des Vorgangs ist außerdem zu sehen, dass die Gruppe ausländische Hoheitssymbole mitführte, insbesondere mehrere russische Fahnen[396], wobei russische Fahnen auch im Rahmen des vorangegangenen Demonstrationszugs zu sehen waren. Dies liefert einen – bewussten oder unbewussten – Hinweis auf die Herkunft der die Gruppe motivierenden Desinformation und Verschwörungsmythen und der dazu gehörigen Verbreitungswege. Das alles gehört ebenfalls zum Kontext, in dem die Gesetzgebung ihre Wirkung entfaltet.

Diesem Vorgang, den der Bundespräsident als „Angriff auf das Herz der Demokratie“ charakterisierte, war eine Demonstration vorausgegangen, auf der neben offen rechtsextrem auftretenden Gruppen auch die im Bundestag vertretenen Partei „Alternative für Deutschland“ eine zumindest fragwürdige Rolle spielte[397]. Die Partei „Alternative für Deutschland“ bagatellisierte das versuchte gewaltsame Eindringen Rechtsextremer in den Sitz des Deutschen Bundestags und charakterisierte diesen 29. August 2020 öffentlich mit den Worten „ein guter Tag“[398].

International wurde dieser Tiefpunkt Anfang 2021 überraschend in den USA noch unterboten durch die gewaltsame Erstürmung des Kapitols und das Posieren von Extremisten oder Verblendeten im Herzen von demokratischen Institutionen am 6. Januar 2021. Dies weist offensichtliche Parallelen auf zu der versuchten Erstürmung des Sitzes des Deutschen Bundestags im Reichstagsgebäude, die von der Partei „Alternative für Deutschland“ mindestens wohlwollend betrachtet wurde, sowie zu der Einschleusung von extremistisch gesinnten, pöbelnden „Aktivisten“ in den Bundestag durch Abgeordnete der Partei „Alternative für Deutschland“. Nahezu könnte ein Beobachter den Eindruck gewinnen, die Ereignisse in Berlin seien Generalprobe oder zumindest Vorlage für die Ereignisse in Washington gewesen.

---

395 Meldung: „Mit gezielten Falschmeldungen aufgehetzt“ (https://www.tagesschau.de/faktenfinder/reichstag-berin-sturm-fakenews-101.html, zuletzt abgerufen 16.09.2020)

396 Zu sehen z.B. im Bildmaterial zur Online-Meldung auf Tagesschau.de: „Entsetzen über Eskalation am Reichstag“ (rechter Bildrand) oder Tagesschau-Sendung vom 06.09.2020, ca. bei der Zeitmarke 10‘40“ (Bildmitte), s.a. Tagesschau-Sendung vom 30.08.2020, ca. Zeitmarke 1‘03“ bis 1‘10“.

397 Jan Sternberg: "AfD mobilisiert Teilnehmer für Demonstration gegen Corona-Maßnahmen in Berlin“ (Redaktionsnetzwerk Deutschland, 23.08.2020, https://www.rnd.de/politik/afd-chef-tino-chrupalla-mobilisiert-teilnehmer-fuer-demonstration-gegen-corona-massnahmen-in-Berlin-2OBZJ44TBZBTPEM75BUBTYSJTE.html, zuletzt abgerufen 16.09.2020); „Ärztekammer Thüringen prüft berufsrechtliches Verfahren gegen Arzt und AfD-Abgeordneten“ (Ärzteblatt, 7.9.2020, https://www.aerzteblatt.de/nachrichten/116266/Aerztekammer-Thueringen-prueft-berufsrechtliches-Verfahren-gegen-Arzt-und-AfD-Abgeordneten, zuletzt abgerufen 16.09.2020)

398 Tagesschau-Sendung vom 30.08.2020, ab ca. Zeitmarke 4‘35“

Dabei muss klar gesagt werden: Die Bereitschaft zur Manipulation demokratischer Prozesse und zum Verrat an der Demokratie und der Verfassung seines Landes durch den gewählten Präsidenten Donald Trump zeigte sich auch dort nicht erst am Ende seiner Amtszeit. Vielmehr war, wie beschrieben, bereits der Vorlauf wie auch der Beginn seiner Präsidentschaft geprägt durch die Bereitschaft zur Manipulation des freien Willens der Wählerinnen und Wähler und zur Verbreitung von Verschwörungsmythen und Fehlinformationen, gerne mit tatkräftiger Unterstützung ausländischer Geheimdienste (vgl. z.B. seine Aufforderung im Wahlkampf: „*Russia, if you're listening*..."). In der Gesamtschau drängt sich die Frage auf, ob dies nicht in ähnlicher Weise gilt für die im Deutschen Bundestag vertretene Partei „Alternative für Deutschland" und u.a. ihren Bundestagswahlkampf 2017 und seitdem zu beobachtendes Verhalten.

Aktuell scheint es übrigens, als würde sich die Desinformations-Maschinerie der momentanen russischen Führung warmlaufen zu einem Versuch, an den „Erfolg" des oben erwähnten „Falls Lisa" (der keiner war) anzuknüpfen und eine neue Empörungswelle zu fabrizieren. Laut Europäischem Auswärtigem Dienst wird seit Februar 2021 eine Märchenkampagne aufgebaut. Sie stellt die richterlich angeordnete Begehung der Wohnung eines russischstämmigen Elternpaares durch das Berliner Jugendamt mit der Folge eines vorläufigen Entzugs des Sorgerechts wegen Kindswohlgefährdung aufgrund der vorgefundenen Situation wahlweise dar als Zeichen anti-russischer Vorurteile, eines dekadenten und pädophilenfreundlichen Staates oder einer Rache für die Inhaftierung des Vergiftungsopfers Nawalny[399]. Wobei man über die Plattheit eines vom Auswärtigen Dienst angeführten Zitats einer russisch-nationalistischen Website – nämlich dass „*in der Sowjetunion staatliche Autoritäten niemals so in eine Familie eingebrochen wären, wie es in den USA und Europa üblich sei*" - fast schon lachen könnte - wenn die Realität der politischen Zwangsadoptionen von Dissidentenkindern in der Sowjetunion wie der DDR und der Überwachung bis in den Familien- und Freundeskreis hinein nicht so tieftraurig wäre. So zeigt der Satz nur die Hirn- und Hemmungslosigkeit, mit der politische Desinformation versucht, vernunftbegabte Menschen in einen Zustand der Empörung zu treiben, in dem ihr Verhalten irrational und steuerbar wird. Und „gute" Desinformation braucht gute Daten und Profile, um effektiv zu sein. Zum Beispiel medizinische...

Dies alles macht die äußerst kritische Situation und den Kontext aus, in dem die betrachtete Gesetzgebung ihre Wirkung entfaltet. Ein Kontext, in dem der Gesetzgeber ohne Rücksicht auf die Gegebenheiten zentrale Sammlungen von Patientendaten aufbauen will, die den Effekt einer Zielscheibe für Hackerangriffe haben. Auch hier ist die Freiwilligkeit der Teilnahme keine hinreichende Bedingung um einen Flächenbrand oder eine Explosion des „Pulverfasses" zu verhindern, auf dem wir sitzen und das unsere freiheitlich-demokratische Grundordnung bedroht.

Bis auf die Daten wären die Zutaten für die Katastrophe da. Es liegt an uns, sie zu verhindern.

399 Europäischer Auswärtiger Dienst: „Vilifying Germany; wooing Germany", 09.03.2021 (https://euvsdisinfo.eu/villifying-germany-wooing-germany/, zuletzt abgerufen März 2021)

Nachwort

Lassen Sie uns, wenn Sie mögen, noch einmal auf das Recht auf informationelle Selbstbestimmung und das sogenannte „Volkszählungsurteils“ eingehen und einen zweiten Blick auf die aktuelle Lage werfen. Und ganz am Ende habe ich noch drei kleine Bitten an Sie...

Das „Volkszählungsurteil“ im 21. Jahrhundert

In seinem Grundsatzurteil zum Volkszählungsgesetz hat das Bundesverfassungsgericht 1983 neben den Grundsätzen der Verhältnismäßigkeit und Normenklarheit insbesondere das Recht auf informationelle Selbstbestimmung in den Mittelpunkt gestellt. Tatsächlich ist es instruktiv, die Aussagen der Grundsatzentscheidung in den Kontext der Rahmenbedingungen der frühen 80er Jahre des 20. Jahrhunderts zu stellen.

Im Jahr 1983 waren nicht nur das Internet, „Spyware“, „Hacking“, „Backdoors“, „Google“ und virtuelle „soziale Netzwerke“ unbekannt. Insbesondere lag das Monopol auf personenbezogene Daten der Bürgerinnen und Bürger faktisch beim Staat. Nur er hatte die grundsätzliche Möglichkeiten, in großem Maßstab personenbezogene Daten zu erheben, zu verarbeiten und daraus gegebenenfalls Persönlichkeitsprofile („Totalabbilder“, „Teilabbilder“) zu erstellen. Die Vorstellung, dass Bürgerinnen und Bürger in großem Umfang und ohne staatlichen Zwang Informationen über sich und ihre privaten Lebensbereiche preisgeben und sich dem „psychischen Druck öffentlicher Anteilnahme“ aussetzen würden, war nicht denkbar. Entsprechend richteten sich die damaligen Verfassungsbeschwerden konkret gegen einen als potentiell übergriffig und übermächtig betrachteten Staat, der im Prinzip die Zusammenführung zwangsweise erhobener, personenbezogener Daten zur Erstellung von Persönlichkeitsprofilen („Teilabbildern“/„Totalabbildern“), um die Freiheit des politischen Willens und der Entfaltung der Persönlichkeit zu beeinträchtigen.

Das Bundesverfassungsgericht stellte 1983 die Befugnis des Einzelnen fest, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebensverhältnisse offenbart werden“. Daraus mag der Gesetzgeber - und mögen Datenverwerter wie Facebook oder Google - geschlossen haben, dass durch eine formale Freiwilligkeit der Datenpreisgabe wie bei den Regelungen zur „elektronischen Patientenakte“ (erforderliche Zustimmung durch den Versicherten) eine Art „Freibrief“ zur uneingeschränkten Erhebung, Zusammenführung und Verarbeitung sensibelster personenbezogener Daten bzw. zu deren Beauftragung erlangt werden kann.

Tatsächlich stellte das Bundesverfassungsgericht die Freiheit, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebensverhältnisse offenbart werden“ aber im Bezug auf möglichen Zwang durch den Staat fest. Das heißt, es geht hier nur um die Freiheit, sich diesem Zwang zu verweigern. Der Umkehrschluss, dass das Bundesverfassungsgericht damit etwa festgestellt hätte, der Einzelne habe die uneingeschränkte Befugnis, zu jeder Zeit und ohne Rücksicht auf die Folgen für das Recht der anderen Bürgerinnen und Bürger auf freie Entfaltung ihrer Persönlichkeit hemmungslos sensible personenbezogene Daten zu offenbaren, gilt jedoch nicht. Hierzu trifft das genannte Grundsatzurteil keine Aussage. Die damals gegen das Volkszählungsgesetz vorgebrachten Beschwerden gaben *„keinen Anlaß zur erschöpfenden Erörterung des Rechts auf informationelle Selbstbestimmung.“*[400]

Wenn das Bundesverfassungsgericht 1983 bereits feststellte, dass der Einzelne als „eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit“ keine „absolute, uneinschränkbare Herrschaft über ‚seine‘ Daten“ habe und durchaus Einschränkungen seines Grundrechts auf informationelle Selbstbestimmung „im überwiegenden Allgemeininteresse“ hinnehmen müsse, so bezog sich das allerdings ebenfalls

400 Aus dem Urteil des Bundesverfassungsgerichts zu den Verfassungsbeschwerden gegen das Volkszählungsgesetz, 15.12.1983.

auf die zwangsweise Datenerhebung und -verarbeitung personenbezogener Daten durch den Staat.

Aufgrund des im Jahr 1983 gegebenen informationellen Kontexts ging das Bundesverfassungsgericht zeitgemäß von folgenden Annahmen aus:
- Nur der Staat besitze ein weitgehendes Datenmonopol und kann als einziger - im Prinzip - hinreichend viele Daten akkumulieren, um Persönlichkeitsprofile seiner Bürger zu erstellen.
- Nur der Staat könne es ausnutzen, wenn die Bürger nicht mehr einschätzen könnten, wer (=welche Behörde) wann was über sie wisse, indem er unerwünschtes Verhalten oder unerwünschte Ansichten sanktioniere oder durch Selbstzensur von vornherein unterdrücken lasse, nur er könne damit die freie Willensbildung der Bürger gezielt beeinträchtigen.
- Nur durch Androhung von Sanktionen könne basierend auf Profilen der Bürger deren freie Willensbildung und damit die freiheitlich-demokratische Grundordnung beeinträchtigt werden.

Im Jahr 2021 gilt keine dieser Einschränkungen mehr: Es gibt kein staatliches Datenmonopol mehr, allenfalls ein privatwirtschaftliches, wir befinden uns im Vergleich zu 1983 nahezu am entgegengesetzten Ende des Spektrums; Ausübung von Zwang durch Nötigung und Erpressung im Zusammenhang mit erbeuteten Daten nach Hackerangriffen durch Akteure aus Drittstaaten sind „an der Tagesordnung“; wir mussten feststellen, dass basierend auf Profilbildung ausgefeilte Kampagnen unter Ausnutzung von Desinformation und Mitteln psychologischer Kriegsführung genutzt wurden, um auch ohne Ausübung von Zwang Prozesse der freien Willensbildung zu beeinflussen.

Das überwiegende Allgemeininteresse liegt heute im Schutz der freiheitlich-demokratischen Grundordnung und der Integrität ihrer demokratischen Prozesse vor zerstörerischen Angriffen seitens staatlicher und nicht-staatlicher Akteure, die die datenbasierten Erstellung von immer genaueren Totalabbildern der Persönlichkeit betreiben bzw. nutzen.

Es existiert eine ausgeprägte privatwirtschaftliche Datenökonomie, die viele Lebensbereiche der Menschen durchzieht und auf der möglichst umfassenden und detaillierten Sammlung personenbezogener Daten und ihrer Verknüpfung zur Erstellung von Profilen basiert, die wieder Handelsware sind und zur möglichst effektiven und punktgenauen Beeinflussung individuellen Verhaltens verwertet werden. Für die vordergründig kostenlose Nutzung digitaler Dienstleistungen, deren Geschäftsmodell auf dieser Datenökonomie basiert, haben Bürgerinnen und Bürger wie beschrieben in großem Umfang persönliche Daten und Lebensverhältnisse preisgegeben und damit zur Erstellung umfangreicher, kommerziell verfügbarer Sammlungen personenbezogener Daten beigetragen, die zur Profilbildung genutzt und dabei mit neu hinzukommenden Daten, z.B. personenbezogenen medizinischen Daten, zusammengeführt und kombiniert ausgewertet werden können.

Dabei ist davon auszugehen, dass der Einzelne weder den Umfang noch die Konsequenzen dieser für freiheitlich-demokratische Gesellschaften völlig atypischen und nie dagewesenen Sammlung und Konzentration personenbezogener Daten überblickt. Die Verfügbarkeit und Verwertung großer Datensätze personenbezogener Daten, sowie die Möglichkeiten zur intransparenten und individuell abstimmbaren Beeinflussung und Manipulation von Bürgerinnen und Bürgern und ihres politischen Willens in großem Maßstab z. B. über virtuelle „soziale Netzwerke“ stellt eine Situation dar, die in der Vergangenheit in ähnlicher Weise nur in totalitären Systemen möglich und denkbar war. Und selbst dort nur mit großem personellen Aufwand, z.B. durch Inlandsgeheimdienste oder Parteigliederungen.

Die vergangenen Jahre haben gezeigt, dass bereits heute die aus Sammlungen personenbezogener Daten entstandenen Profile nicht nur zur zielgruppenorientierten Bewerbung von Produkten, sondern auch zur wirksamen manipulativen Beeinflussung des freien politischen Willens und demokratischer Prozesse bis hin zur individuellen Ebene genutzt werden. Genau das wurde bereits 1983 vom Bundesverfassungsgericht, damals allerdings unter staatlichen Vorzeichen, befürchtet.

Nichtsdestotrotz ist festzuhalten, dass der Aufbau dieser gigantischen Datensammlung, wie auch die angestrebte, staatlich beauftrage Erstellung einer zusätzlichen umfassenden Sammlung personenbezogener medizinischer Daten nicht auf staatlichem Zwang, sondern auf der freiwilligen Mitwirkung des Einzelnen beruht. Steht also Beides im Einklang mit dem Recht auf informationelle Selbstbestimmung?

Nein. Nur unter der stillschweigenden Voraussetzung, dass auch der oben genannte Umkehrschluss gilt. Das ist jedoch nicht der Fall.

Verantwortung des Einzelnen für seine Daten

Dies wird bereits aus Art. 2, Abs. 1 GG deutlich: „Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, *soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt*“. Es gibt also keinen Freibrief der oben beschriebenen Art für die unbegrenzte und beliebige Preisgabe, Erhebung und Verarbeitung personenbezogener Daten ohne Rücksicht auf die Gesellschaft, die verfassungsmäßige Ordnung oder das Sittengesetz.

Tatsächlich schützt Art. 2, Abs. 1 des Grundgesetzes das Recht auf freie Entfaltung der Persönlichkeit (und daraus abgeleitet auch das Recht auf informationelle Selbstbestimmung) unter zwei Aspekten. Zum Einen schützt es individuell das Recht *zur* freien Entfaltung der Persönlichkeit gegen Zwang und Einschränkung durch eine übergeordnete Stelle (z.B. den Staat), zum Anderen schützt es auf gesamtgesellschaftlicher Ebene das Freiheitsrecht des Einzelnen *vor* einer uneingeschränkten Entfaltung der Persönlichkeit der Anderen. Es schützt seine eigenen Grundvoraussetzungen wie die verfassungsmäßige, d.h. freiheitliche und demokratische Ordnung. Durch die wohlbedachte Formulierung dieses doppelten Schutzes haben die „Väter und Mütter“ des Grundgesetzes eine Modernität und Weitsicht bewiesen, die eine angemessene Formulierung der Freiheitsverletzung durch z.B. das ungehemmte Sammeln von Daten und Erstellen von Persönlichkeitsprofilen im 21. Jahrhundert erst möglich macht. Dies unterscheidet das Grundgesetz möglicherweise in einem wesentlichen Punkt von geschriebenen und ungeschriebenen Verfassungen anderer Länder, die weniger Handhabe bieten, wenn hier die Axt an die Wurzeln der freiheitlichen demokratischen Grundordnung gelegt wird[401]. Dies ist gleichzeitig Auszeichnung und Verpflichtung.

Gemäß Art. 2, Abs. 1 GG ist die Preisgabe der personenbezogenen Daten insbesondere dahingehend eingeschränkt, dass sie nicht zu einer Gefährdung und Beeinträchtigung der verfassungsmäßigen Ordnung führen darf. Wir hatten aber gesehen, dass Sammlungen personenbezogener Daten in jüngster Vergangenheit bereits zur Profilbildung und manipulativen Beeinflussung von Wahlen verwendet wurden, also zu Zwecken, die sich unmittelbar gegen die Grundlagen einer freiheitlich-demokratischen Ordnung richten, die auf dem freien Willen mündiger Bürgerinnen und Bürger beruht.

Auch die Bundesregierung stellt hier ein verfassungsrechtliches und gesamtgesellschaftliches Problem fest, wenn sie mit Blick auf den Cambridge Analytica-Skandal schreibt: „*Die mögliche Nutzung von Datenprofilen von Bürgerinnen und Bürgern zur Beeinflussung des demokratischen Meinungs- und Willensbildungsprozesses hat eine verfassungsrechtliche und gesamtgesellschaftliche Dimension. Es ist ein Kernelement der freiheitlichen Demokratie des Grundgesetzes, dass die Wählerinnen und Wähler ihr politisches Urteil in einem freien und offenen Prozess der Meinungsbildung fällen können.*“[402]

401 Allerdings findet sich schon in der Erklärung der Menschen- und Bürgerrechte von 1789 die Feststellung: „La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société la jouissance de ces mêmes droits.“.

402 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Katharina Dröge, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 19/1950 – vom 06.06.2018 (S. 3) https://dipbt.bundestag.de/dip21/btd/19/025/1902552.pdf

Wenn die angreifenden Akteure in Deutschland - trotz fortgesetzter Versuche und trotz aller schon angerichteten gesellschaftlichen Verwerfungen - bisher scheinbar geringeren Erfolg als in anderen Ländern hatten, so ist dies zu einem nicht unwesentlichen Teil auf den Datenschutz, also die bisher geringere Verfügbarkeit von umfassenden Sammlungen sensibler personenbezogener Daten zurückzuführen, bisher insbesondere auch medizinischer Daten. Hierzu gehört auch eine bisher hohe Resilienz von z.B. Arztpraxen gegen Angriffe über das Internet, von dem ihre Systeme mit behandlungsrelevanten Daten bis zur jüngeren Gesetzgebung isoliert waren.

Weitere Gründe mögen die Sprachbarriere und ein bisheriger Fokus auf englischsprachige Länder, insbesondere die USA und das Vereinigte Königreich, sein, sowie strengere Regulierungen, die z.B. eine direkte Ansprache per E-Mail erschweren und ein höheres Datenschutzniveau ermöglichen.

Aber hier muss man sich keinen Illusionen hingeben: Automatisierte Übersetzungen haben in den vergangenen Jahren dramatische Fortschritte erzielt, der jeweilige Fokus ist flexibel, eine Ansprache per E-Mail spielt bisher wohl ohnehin eine geringere Rolle als zielgerichtete verdeckte Manipulation über virtuelle „soziale Netzwerke“. Facebook hatte nach eigenen Angaben 2018 in Deutschland täglich mehr als 24 Millionen Nutzer, monatlich mehr als 32 Millionen[403]. Das entspricht täglich ca. 28,9 % bzw. monatlich ca. 38,5 % der Gesamtbevölkerung. Die Zahl der täglichen und monatlichen Nutzer hat dabei seit 2016 zugenommen (relativ zu 2016 um ca. 10...15 %).
Das Portal Heise berichtet im Juli 2018 unter der Überschrift: „Datenschutz bremst Umsatz nicht, Zuckerberg ‚ermutigt‘“: *‚Die DSGVO war ein wichtiger Moment für unsere Branche‘, sagte Facebook-Chef Mark Zuckerberg in einer Telefonkonferenz mit Finanzanalysten am Mittwochabend. ‚Als Folge davon haben wir einen Rückgang der monatlich aktiven Nutzer von etwa einer Million gesehen.‘ Gleichzeitig habe die weitaus überwiegende Mehrheit der User zugestimmt, dass Facebook sie auch auf anderen Seiten verfolgen darf, um ihnen ‚relevantere‘ Werbung und ‚verbesserte Kundenerfahrung‘ angedeihen lassen zu können. […] COO Sheryl Sandberg fügte später hinzu, dass die DSGVO ‚keine signifikanten Auswirkungen auf den Umsatz‘ gehabt hat.*“[404]
Hinzu kommen die Bürgerinnen und Bürger, die in virtuellen „sozialen Netzwerken“ wie VK oder Odnoklassniki vertreten und aktiv und dort verdeckt adressierbar sind, die sich einer Regulierung nicht nur faktisch sondern auch grundsätzlich entziehen.

Das wohl wesentliche Hemmnis für die genannten Akteure ist aber die bisher geringere Verfügbarkeit von umfassenden Sammlungen sensibler personenbezogener Daten.

Die virtuelle Patientenakte wie auch die Forschungsdatenbank sind als zentrale Sammlungen der denkbar sensibelsten und intimsten, personenbezogenen Daten die „optimale“ Grundlage für die effektive und gezielte Manipulation des Willens und des Verhaltens mit gesamtgesellschaftlicher Relevanz. Sei es individuell über virtuelle „soziale Netzwerke“ oder als über Massenmedien breiter gestreute aber an Zielgruppen angepasste Botschaften, die gezielt bestimmte Ängste, Befindlichkeiten oder Persönlichkeitsstörungen adressieren und verstärken, um ein bestimmtes Wählerverhalten zu bewirken. Ebenso ist die Kenntnis intimer personenbezogener Daten durch Dritte geeignet zur böswilligen „klassischen“ Verhaltensmanipulation durch psychischen Druck oder Erpressung.

Tatsächlich würde wohl schon die bloße Existenz einer solchen Datensammlung dazu führen, dass selbst eine nur (glaubhaft) behauptete Aneignung der Daten bereits das Vertrauen in die Integrität und Freiheit demokratischer Prozesse untergraben würde. Mit Blick auf die oben dokumentierten Beispiele erfolgreicher De-Anonymisierungen und irregulärer Datenzugriffe,

403 https://allfacebook.de/zahlen_fakten/offiziell-facebook-nutzerzahlen-deutschland, zuletzt abgerufen 29.02.2020.

404 https://www.heise.de/newsticker/meldung/facebook-verliert-in-Europa-User-4120628.html , zuletzt abgerufen 29.02.2020.

gerade auch auf Gesundheitsdaten, wäre eine entsprechend gestreute Behauptung praktisch immer glaubhaft.

Dabei ist für den Einzelnen nicht ersichtlich, ob ausgerechnet seine Datenpreisgabe mit der Folge seiner erhöhten Manipulierbarkeit unmittelbar oder in Zukunft zu einer Gefährdung der verfassungsmäßigen Ordnung führt. Es ist daher Aufgabe des Staates, hier gesamtgesellschaftlich regelnd einzugreifen und das Erstellen einer entsprechenden Datensammlung zu verhindern. Nicht, sie per Gesetz zu beauftragen. Statt dessen forciert das Gesundheitsministerium eine Salamigesetzgebung, die die potentielle Sammlung und Zusammenführung auch medizinischer Daten durch Angebote von Dienstleistern wie Google oder Facebook in einer eigenen virtuellen Patientenakte in keiner Weise einschränkt. Im Gegenteil können diese mit den digitalen Daten aus der virtuellen Patientenakte durch den Versicherten besonders komfortabel befüllt werden.

Bisher hatten die Akteure, deren Bestrebungen sich schon jetzt gegen die Grundlagen der verfassungsmäßigen Ordnung auch in Deutschland richten, zwar den Willen und Gelegenheiten, aber noch nicht die hinreichende Mittel zur effektiven Realisierung ihrer Absichten. Mit der Einführung einer virtuellen Patientenakte werden ihnen diese Mittel bereitgestellt. Die genannten Akteure brauchen sich dieses Mittel dann nur noch anzueignen. Oder die Aneignung zu behaupten.

Die Dystopie des profilierten und manipulierten Bürgers, die das Bundesverfassungsgericht 1983 mit seinem Grundsatzurteil zunächst abwehrte, beginnt heute durch die Hintertür Realität zu werden.

Die Naivität und Vehemenz, mit der Bundesregierung und Gesetzgeber u.a. die Erstellung zentralisierter digitaler Datensätze personenbezogener medizinischer Daten, deren Verfügbarkeit über Strukturen des Internets, ihre wirtschaftliche Nutzung und die Weitergabe von Daten im Rahmen der Kettengesetzgebung vorantreiben, zeigen, dass sie die Situation und den Kern des Problems nicht erkannt haben oder ignorieren. Auch das „Gesetz zur Verbesserung der Rechtsdurchstzung in sozialen Netzwerken (NetzDG)“ von 2017 beispielsweise bedeutet ja bei aller Bedeutung im Rahmen der Bemühung um Schadensbegrenzung letztlich ein „Herumkurieren an Symptomen“: Manipulative Techniken psychologischer Kriegführung kommen nicht im Gewand von „Hasskommentaren“ daher, diese sind bereits deren Folge.

Verschärfend hinzu kommt die problematische Dreiecksbeziehung zwischen rechtsextremen Netzwerken, einer gegen die freiheitlich-demokratische Grundordnung agierenden ausländischen Staatsführung und einer im Bundestag vertretenen Partei, die deren Nähe sucht und deren Agenden bedient. Eine Dreiecksbeziehung, die ebenfalls den Kontext der virtuellen Patentenakte bildet.

Es tut mir leid, aber es ist nicht davon auszugehen, dass eine ausländische Staatsführung oder ihr nahestehende Institutionen und Personen,

- die systematisch Desinformation betreibt[405],
- deren Manipulation demokratischer Prozesse und Hacker-Angriffe auf Institutionen der Demokratie dokumentiert sind[406],

405 Vgl. auch Beispiele auf der Anti-Desinformationsseite der Europäischen Union (euvsdisinfo.eu) und im Verfassungsschutzbericht 2019 (s.u.)

406 Z.B.: F. Flade und G. Mascolo: „Hackerangriff auf Bundestag – Bärenjagd“ - Meldung zum von der Bundesanwaltschaft erwirkten Haftbefehl gegen Dmitrij Sergejewitsch als mutmaßliches Mitglied des russischen Militärgeheimdienstes GRU (Süddeutsche Zeitung, 05.05.2020, https://www.sueddeutsche.de/politik/hack-Bundestag-angriff-russland-1.4891668, zuletzt abgerufen 16.09.2020); siehe Bericht des US amerikanischen Sonderermittler Robert S. Mueller, zusätzlich auch „Verfassungsschutzbericht 2019“ des BMI, S. 285ff.

- die auf Hunderte in Myanmar durch das Militär erschossene Pro-Demokratie-Demonstranten und Zivilisten in allen Altersstufen mit einem Ausbau der militärischen Zusammenarbeit reagiert[407],
- die selbst missliebige Personen im In- und Ausland mit radioaktiven Schwermetallen oder chemischen Kampfstoffen vergiften oder in Sichtweite des Bundeskanzleramts per Kopfschuss hinrichten lässt[408] und sie im Fall des unbotmäßigen Überlebens zur Strafe in Lagerhaft schickt[409],
- deren Agenda von einer im Bundestag vertretenen Partei gedeckt und unterstützt wird[410],

oder die

- Hunderttausende ihrer Bürger in geschlossene Lager zur totalen Kontrolle und politischen „Umerziehung“ („Gehirnwäsche“) sperrt und deren Existenz international leugnet[411],
- die Informationsfreiheit ihrer Bürgerinnen und Bürger quasi beliebig einschränkt, missliebige Themen aus der öffentlichen Debatte weitgehend löscht und Nachrichtenflüsse bis hin zum Internet aufwändig kontrolliert und zensiert[412],
- die Unfreiheit durch totale digitale Überwachung, Profilbildung und Verhaltensmanipulation ihrer Bürgerinnen und Bürger quasi zur Staatsraison erhebt[413],
- vor den Augen der Menschen in Hongkong der Demokratie und Freiheit planvoll Stück für Stück mit der Abrißbirne zuleibe rückt[414] [415]
- die Demokratie, Pressefreiheit, freiem Internet, wissenschaftlicher Geschichtsschreibung, Stärkung der Zivilgesellschaft, individueller Freiheit, Rechtsstaatlichkeit und Unabhängigkeit

---

407 „Russischer Minister bei Militärparade in Myanmar – Kreml sieht kein Problem“, 29.03.2021, Redaktionsnetwerk Deutschland (https://www.rnd.de/politik)

408 Z.B.: P. Gensing und S. Stöber: „Moskau und der Fall Nawalny - aus dem Lehrbuch der Desinformation“ (Tagesschau, 3.9.2020, https://www.tagesschau.de/faktenfinder/russland-nawalny-desinformation-101.html, zuletzt abgerufen 16.09.2020), aber auch Bundesministerium des Innern, für Bau und Heimat: „Verfassungsschutzbericht 2019“, S. 291.

409 S. Bigalke und F. Nienhuysen: „Nawalkny muss ins Straflager“, Süddeutsche Zeitung, 2. Februar 2021 (https://www.sueddeutsche.de/politik/russland-nawalny-muss-ins-straflager-1.5193913, zuletzt abgerufen 2021)

410 Vgl. Ausführungen oben und beispielsweise: die Äußerungen des Vorsitzenden der Partei „Alternative für Deutschland“ zum Fall Nawalny und der Rolle des russischen Staats im Deutschen Bundestag am 11. September 2020 (Plenarprotokoll des Deutschen Bundestags 19/174, S.. 21912, sowie unter der Überschrift „Bundesregierung verrät deutsche Interessen“ im Youtube-Kanal der Partei) sowie entsprechende Einträge in der Desinformations-Datenbank des Europäischen Auswärtigen Dienstes zu Narrativen der russischen Staatsführung im Fall Nawalny, z.B. unter https://euvsdisinfo.eu/report/navalny-novichok-secret-service; die auf die Schwächung der europäischen Integration und insbesondere der Europäischen Union und ihrer demokratischen Institutionen gerichtete Zielsetzung im Europawahl-Programm der Partei „Alternative für Deutschland“ des vergangenen Jahres inklusive der erklärten Absicht einer Auflösung des Europäischen Parlaments und ggf. eines Austritts Deutschlands aus der Europäischen Union; die Haltung der Partei zur Annexion der Krim, wie auch ihr Wechselspiel mit russischen Staatsmedien zu einer Zeit, als es sich noch um eine weitgehend unbedeutende Splitterpartei handelte.

411 „China Cables“ (https://projekte.sueddeutsche.de/artikel/politik/das-sind-die-china-cables-e185468

412 Z.B. L. Deuber: „Zum Fest gibt‘s langsame Ladebalken“ (Süddeutsche Zeitung, 20.9.2019, https://www.sueddeutsche.de/digital/zensur-china-internet-vpn-1.4607363, zuletzt abgerufen 16.09.2020)

413 Vgl. z.B. M. Settelen: „Chinas Social-Credit-System“ (Neue Zürcher Zeitung, 3.12.2019, https://www.nzz.ch/nzz-asien/chinas-social-credit-system-id.1525941,zuletzt abgerufen 16.09.2020), sowie die Wikipedia-Artikel zum Sozialkredit-System/social credit system (https://en.wikipedia.org/wiki/Social_Credit_System, https://de.wikipedia.org/wiki/Sozialkredit-System, zuletzt abgerufen 16.09.2020)

414 „Strengeres Wahlsystem für Hongkong beschlossen“, 11.03.2021, tagesschau.de (https://www.tagesschau.de/ausland/asien/china-volkskongress-wahlreform-hongkong-101.html, zuletzt abgerufen März 2021)

415 S. Wurzel: „China verschärft Hongkong-Wahlgesetz“, 30.03.2021, tagesschau online (https://www.tagesschau.de/ausland/asien/china-honkong-wahlgesetz-101.html, zuletzt abgerufen März 2021)

der Justiz als fundamentale Gefahr sieht und schon das Sprechen darüber als Tabu aus dem Bildungsbereich und der öffentlichen Debatte verbannt[416] [417],
- zunehmend Methoden psychologischer Kriegführung wie Desinformationskampagnen gegen westliche Staaten richtet[418] und auf eine möglichst weitgehende Gleichschaltung der globalen Wahrnehmung und Debatte abzielt[419],
- eine dokumentierte Vorgeschichte ausgefeilter, erfolgreicher Hacker-Angriffe hat[420] [421],

es ist nicht davon auszugehen, dass sie oder andere vergleichbare Akteure[422] nennenswerte Hemmungen oder Skrupel haben werden, unter Aufbietung aller ihnen zur Verfügung stehenden Mittel und Kreativität die Inhalte einer medizinischen Datenbank zu erbeuten[423]. Eine Datenbank, die intimste persönliche Informationen potentiell jedes einzelnen Bundesbürgers und jeder einzelnen Bundesbürgerin enthält, sei es eine virtuelle „elektronische Patientenakte“, sei es eine zentrale Vorratsdatenbank in einem Forschungsdatenzentrum, wenn sie auch noch so „freiwillig“ befüllt worden sein mag.[424] Und diese zum Schaden der freiheitlich-demokratischen Gesellschaft einsetzen wird.

Schutz der freiheitlich-demokratischen Grundordnung

Hier besteht aus meiner Sicht eine konkrete Gefährdung der Integrität von Wahlen z.B. zum Deutschen Bundestag. Die Beinahe-Erstürmung des Sitzes des Deutschen Bundestags, das Einschleusen extremistischer Aktivisten mit dem Ziel, deutsche Abgeordnete und Regierungsmitglieder zu bedrängen und die Erstürmung des Parlaments in den Vereinigten Staaten von Amerika sind Warnsignale, die an Deutlichkeit nicht zu überbieten sind.

Der US amerikanische Präsident Donald Trump sowie die ihn über Jahre und zum Teil jetzt noch stützenden Abgeordneten und Senatoren sind in demokratischen Prozessen gewählte Volksvertreter, obwohl er ein offensichtlicher Feind der Demokratie und Verfassung ist (und vielleicht auch im strafrechtlichen Sinn kriminell). In Deutschland ist aber ein Kerngedanke des Grundgesetzes mit Blick auf die Weimarer Verfassung, dass nie wieder ein „Marsch durch die Institutionen“ von Verfassungsfeinden möglich sein soll. Durch die Existenz massenhafter Sammlungen personenbezogener Daten, die massenhafte Erstellung immer weiter verfeinerter Persönlichkeitsprofile und die technischen Gegebenheiten der Digitalisierung mit den damit verbundenen Möglichkeiten zur massenhaften individuellen Manipulation hat sich hier nun aber eine offene Flanke aufgetan, die dringend und schnell geschlossen werden muss.
Anders als im Jahr 1983 geht es nicht mehr um eine hypothetische, eher theoretisch betrachtete dystopische Möglichkeit, sondern um eine konkrete Realität, die die Grundlagen der verfassungsmäßigen Ordnung angreift und damit die Möglichkeit zur freien Entfaltung meiner Persönlichkeit.

Welche Schlussfolgerungen ergeben sich aus den Betrachtungen in diesem Debattenbeitrag? Brauchen wir Öffentlich-Rechtliche Suchmaschinen und Soziale Netzwerke? Gebührenfinanzierte Angebote? Pflicht zur transparenten Finanzierung von nicht-

416 M. Naß: „Er hat das Sagen, immer und überall“, Die Zeit, 18.02.2021, S. 8
417 https://de.wikipedia.org/wiki/Dokument_Nummer_9 (zuletzt abgerufen Februar 2021).
418 Lagebild 2021 des estnischen Auslandsnachrichtendienstes Välisluureamet: „International Security and Estonia 2021“ (2021), S. 73ff.
419 Ebd., „silenced world“
420 Vgl. hierzu die Hinweise z.B. zum „Cloud Hopper“- Angriff, aber auch z.B. Bundesministerium des Innern, für Bau und Heimat: „Verfassungsschutzbericht 2019“, S. 296f.
421 J. Schmidt: „Exchange Lücken: BSI ruft ‚IT-Bedrohungslage rot‘ aus“, 09.03.2021, heise online (https://www.heise.de/news/Exchange-Luecken-BSI-ruft-IT-Bedrohungslage-rot-aus-5075457.html, zuletzt abgerufen März 2021).
422 Zu nennen wäre hier Beispielsweise SCL/Cambridge Analytica bzw. deren Nachfolger und Äquivalente, sowie ideologisch motivierte Täter aus dem Umfeld extremistischer Netzwerke wie der früher genannte Stephen Bannon.
423 Sei es zum unmittelbaren Gebrauch, sei es zum späteren Gebrauch z.B: nach erfolgter Entschlüsselung.
424 Z.B. nach § 26 der Datenschutz-Grundverordnung (DSGVO).

gemeinnützigen Online-Dienstleistungen über Beiträge oder Gebühren? Mehr Medienerziehung? Einen Ethikrat, der ethisch rät und moralisch handelt? Sachverständige, die ihre Sache verstehen und für die Bürgerinnen und Bürger eintreten?

Vielleicht. Aber das Wichtigste sind aus meiner Sicht drei Dinge, die ich gerne als Bitte an Sie, liebe Leserin und lieber Leser, formulieren möchte:

1. Machen Sie sich klar, dass eine sinnvolle Nutzung und Entwicklung des Internets und seiner Anwendungen auch ohne „Individualisierung“ und Erstellung von Persönlichkeitsprofilen prima funktioniert. Das ist nur ein Geschäftsmodell.

2. Bleiben Sie optimistisch.

3. Behalten Sie Ihre Daten bitte für sich.

Danke.

Anhang

Kommentar: ‚Viel hilft viel' – Salutismus und das Gutachten 2021 des Sachverständigenrats „Gesundheit"

Im März 2021 veröffentlichte der „Sachverständigenrat Gesundheit" sein turnusmäßiges Gutachten, diesmal unter dem Titel „Digitalisierung für Gesundheit". Der aktuelle Sachverständigenrat wurde Anfang 2019 durch den Bundesgesundheitsminister berufen, der damit den Wunsch verband, dass „*auch Themen wie Digitalisierung, Big Data und Künstliche Intelligenz noch stärker in den Blick genommen werden".*[425] Der Rat umfasst sieben Professorinnen und Professoren aus den Bereichen Wirtschaftswissenschaft, Politikwissenschaft, Pflegewissenschaften und Medizin.

In dem Gutachten werden auf knapp 400 Seiten verschiedene Aspekte digitaler Prozesse im Gesundheitswesen betrachtet. Insbesondere entwickeln die Gutachterinnen und Gutachter ein Wertesystem, auf dessen Grundlage sie sehr weit reichende Forderungen an den Gesetzgeber zur virtuellen „elektronischen Patientenakte" rechtfertigen. Sie stellen zudem Forderungen nach vermehrter Datenerzeugung und -speicherung auf und entwickeln eine bestimmte Sicht auf Fragen von Datensicherheit, Datenschutz und Datensparsamkeit, die im Widerspruch zur Auffassung des Bundesamtes für Sicherheit in der Informationstechnik steht[426].

Der fachliche Hintergrund des Sachverständigenrats deckt vielfältige Perspektiven auf das Gesundheitssystem ab. Die für den ersten Teil des Titels erforderliche Expertise ist nicht erkennbar[427]. Dies erklärt vielleicht auch die Verwendung des oft schlagwortartig verwendeten, unspezifischen Begriffs „Digitalisierung", unter dem oft ganz unterschiedliche Aspekte verstanden und manchmal auch vermischt werden. Beispielsweise die Digitalisierung von Dokumenten („Röntgentüte") mit zentraler Datenspeicherung, digitale Kommunikation mit Datenverwertung oder auch Datenschutz mit Datensicherheit.

Bei näherer Betrachtung zeigt sich, dass die Mitglieder des Sachverständigenrats beruflich ein Forschungsinteresse an der Nutzung und Verknüpfung großer Datenmengen haben[428] oder seit Jahren durchaus pointierte Thesen zu einem zu hebenden „Datenschatz" vertreten, verbunden mit sehr weit gehenden Forderungen bezüglich des Zugriffs auf persönliche medizinische Daten[429]. Diese in der Rolle als Wissenschaftler/in legitimen Eigeninteressen, Meinungen und Thesen könnten vor allem für die unbefangene Erörterung von Fragen zu Datenschutz und Datennutzung eine Rolle spielen.

Gerade in der aktiven Politikberatung mit gesetzlichem Auftrag ist es daher eine gute Idee, transparent auf mögliche Begrenzungen seiner Expertise und potentielle Interessenskonflikte hinzuweisen. Auch, um sich beispielsweise nicht selbst dem Verdacht auszusetzen, in der

425 „Sachverständigenrat Gesundheit wurde neu berufen", 31.01.2019, haufe online (https://www.haufe.de/sozialwesen/leistungen-sozialversicherung/sachverstaendigenrat-gesundheit-neu-berufen_242_482976.html, zuletzt abgerufen April 2021)

426 Ebd. S. 84f., vgl. auch Bundesamt für Sicherheit in der Informationstechnik: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen", BSI TR-02102-1, Version 2020-01 (2020), S. 16; in puncto Datensicherheit ist dem BSI zufolge der beste Schutz vertraulicher Daten die Beschränkung ihrer Übertragung und Speicherung.

427 Sie werden vielleicht einwenden, dass man ja auch nicht wissen müsse, wie ein Motor funktioniert, um Auto fahren zu können. Das stimmt. Allerdings würden Sie dann vermutlich nicht als Kfz-Sachverständige/r auftreten und im Alleingang Gutachten erstellen.

428 z.B. Projekt „Algorithmen und Analysen zu inadäquater Medikation/Unterversorgung" unter Leitung von Frau Prof. Dr. Thürmann im Rahmen der Medizininformatik-Initiative (https://www.gesundheitsforschung-bmbf.de/de/konsortien-ubergreifender-use-case-polar-mi-polypharmazie-arzneimittelwechselwirkungen-11056.php, zuletzt abgerufen April 2021)

429 Z.B. J. Schreyögg: „Big Data: Datenbestände für Wissenschaft und Patienteninformation effektiver nutzen", 12.4.2017, (https://blog.der-digitale-patient.de/big-data-datenbestaende-effektiver-nutzen/, zuletzt abgerufen April 2021)

Rolle als Gutachter/in „camouflierte Partikularinteressen“[430] zu vertreten und z.B. Einzelmeinungen wie einen wissenschaftlichen Konsens darzustellen.

Ich finde es schade, dass die Autorinnen und Autoren des Gutachtens auf diese Hinweise verzichtet haben. Statt dessen geht der Sachverständigenrat gleich „in die Vollen“ und sucht dabei ein nicht unproblematisches Fahrwasser auf. Als Ausgangspunkt seiner Argumentation stellt der Sachverständigenrat den Bedürfnissen und Rechten des individuellen Patienten das Heer aller anderen und zukünftigen Patienten gegenüber und legt und das „Wohl“ dieses überpersönlichen und überzeitlichen, sozusagen „ewigen Patientenkollektivs“ als obersten Maßstab fest: „*Zweck von Gesundheitspolitik und Gesundheitsversorgung ist das ‚Patientenwohl‘ […] verstanden als das Wohl aller aktuellen und aller zukünftigen Patientinnen und Patienten. Damit ist zugleich der Maßstab gegeben, an dem Digitalisierung im Gesundheitswesen ausgerichtet und beurteilt werden muss.*“[431]

Ein Maßstab, vor dem der Wunsch nach Schutz und Nicht-Offenbarung persönlicher Daten zu einem Akt des Egoismus‘ und der Verantwortungslosigkeit wird. Wenn nicht kriminell so doch zumindest moralisch verwerflich, geht es doch um „the Greater Good“ (oder als Service des Sachverständigenrats für die Nicht-Harry-Potter-Fans mit kurzer Aufmerksamkeitsspanne unter Ihnen nochmal in Reimform: „*Daten teilen – besser heilen*“[432]).

Wie man leicht feststellt, ist die Konstruktion eines „überpersönlichen“ und „überzeitlichen“ Kollektivs und dessen Wohls als höchstem Gut, gerne einhergehend mit Umdeutungen und der Umwertung von Werten, nicht ganz originell, sondern immer wieder vorgekommen. Unter verschiedenen Überschriften und zu verschiedenen Zeiten, die oft aus gutem Grund der Vergangenheit angehören.

Im politischen Bereich beispielsweise als gesellschaftliches Kollektiv, gegenüber dessen Wohl individuelle, persönliche Freiheiten und Rechte nachrangig seien („die Arbeiterklasse“, „die Nation“, „das Volk“ „die sozialistische Gemeinschaft“). Wobei insbesondere der Wunsch nach Schutz der Privatsphäre als asozial und höchst verdächtig gilt: „*Eine Unterscheidung zwischen privatem und öffentlichem Leben wird früher oder später zum Verrat am Kommunismus führen.*“[433]

Speziell im medizinischen Bereich gab es dieses „ewige Kollektiv“ mit seinen vorrangigen Ansprüchen unter anderem als Konstrukt eines gesunden „Volkskörpers“, mit Blick auf den sich vor einiger Zeit ein Arzt freute über die Entschlossenheit des Gesetzgebers und dessen „*Anfang der Vorsorge für das kommende Geschlecht, um [...] eine bessere und gesündere Zukunft zu gestalten. Die deutsche Regierung hat damit bewiesen, dass sie bereit ist, aufbauend auf den Grundsätzen der wissenschaftlichen Erkenntnisse, das Interesse des [...] Einzelwesens dem Gesamtwohl […] unterzuordnen.“*[434]
Wobei klargestellt wird, dass die anvisierten Maßnahmen nach der bisherigen „*Kleinmütigkeit einer überholten Weltanschauung*“ endlich eine wahre *„Tat der Nächstenliebe und Vorsorge für die kommenden Generationen […] eine wahrhaft soziale Tat für die betroffenen […] Familien [sind]*.“[435]

430 Ebd., S. 6
431 Ebd. S. 1
432 Gerlach et al.: „Digitalisierung für Gesundheit – Gutachten 2021“, S. 17
433 Lenins Frau Nadeshda Krupskaja, zitiert nach O. Figes: „Die Flüsterer – Leben in Stalins Russland“, Berlin Verlag, 2. Auflage (2008), S. 43
434 Dr. med. A. Gütt, Dr. med. E. Rüdin und Dr. jur. F. Ruttke: „Gesetz zur Verhütung des erbkranken Nachwuchses vom 14. Juli 1933 – Ausgabe für die Mitglieder der ärztlichen Spitzenverbände“, München (1934), S. 5
435 Ebd., S. 60

Da sich Geschichte nicht wiederholt und die angeführten Zitate auch nicht auf eine *politische* Nähe hinweisen sollen, soll die Haltung des Sachverständigenrats zur Abgrenzung als „Salutismus“ bezeichnet werden, in Anlehnung an das lateinische Wort für „Wohl“ (salus).

Salutismus ist dabei nicht mit Selbstlosigkeit oder Sorge für den Anderen („Altruismus“) zu verwechseln. Letztere ist ja immer auf das Individuum, also den einzelnen, konkreten Menschen bezogen und würde nie dessen Willen oder Autonomie in Frage stellen. Niemand könnte aus Altruismus von Ihnen oder gar dem Staat fordern, zugunsten eines abstrakten höheren Guts die unveräußerlichen Grund- und Freiheitsrechte des Einzelnen zu relativieren oder aufzugeben. Grundwerte, deren Wahrung und Verteidigung ja geradezu die Pflicht jedes Mitglieds einer freiheitlich-demokratisch verfassten Gemeinschaft ist.

Wohin führt die Haltung des Salutismus‘ den Sachverständigenrat, aus der heraus er „helfen“ möchte, „*den Tunnelblick*“ auf informationelle Selbstbestimmung „*zu überwinden*“[436] und ebenso die „*alte Maxime der unbedingten Datensparsamkeit*“[437]? Zumal Letztere ja durch die Entwicklungen im Bereich „künstlicher Intelligenz“ ohnehin längst überholt sei[438].

Zunächst einmal beginnen die Gutachterinnen und Gutachter mit einer etwas umständlichen Ausführung zum Thema Normen und Ethik[439]. Ihr Anliegen lässt sich in einem Satz dahingehend zusammenfassen, dass Normen – die man mitunter zu Gesetzen erhebe - auf sozialen Traditionen beruhen und wie die Gesellschaft dem geschichtlichen Wandel unterworfen seien, sich also natürlicherweise immer wieder ändern würden.

Es ist nicht uninteressant, dass eine ganz ähnliche Sicht bereits 2010 von Facebook-Chef Mark Zuckerberg im Rahmen einer besonders kecken Änderung der „Privatsphäre“-Einstellungen des Unternehmens[440] vertreten wurde. Die Änderung bestand darin, dass von heute auf morgen per Voreinstellung zahlenden Dritten automatisch der Zugriff auf die Profile der Nutzerinnen und Nutzer gestattet war, sofern die Nutzer dem nicht aktiv widersprachen („Wechsel vom Opt-in zum Opt-out“). Konfrontiert mit massiver Kritik behauptete Zuckerberg einfach, dass Privatsphäre doch ohnehin eine längst überholte soziale Norm sei und Facebook sich da nur als passiver Dienstleister der neuen sozialen Realität anpasse[441].

Ob man die vom Sachverständigenrat vorgetragene kleine Kulturgeschichte des Rechts als historisch-korrekt oder eher als kindlich-naiv betrachtet, ist dabei nicht entscheidend. Entscheidend ist, dass die Gutachterinnen und Gutachter ähnlich wie der Facebook-Boss eine kleine aber nicht ganz unbedeutende Kleinigkeit unter den Tisch fallen lassen.

Nämlich die, dass es - durchaus ernstzunehmende - Juristen gibt, die meinen, dass es jenseits von am Lagerfeuer vor der Höhle ausgehandelten Alltagsregeln so etwas wie unveräußerlichen Grundrechte gebe. Die man auch gerne mal in einer Charta oder Verfassung niederschreibe, wie beispielsweise dem Grundgesetz für die Bundesrepublik Deutschland. Aus denen sich unmittelbar Dinge wie das Recht auf Privatsphäre oder informationelle Selbstbestimmung ergeben. Und die also vielleicht gar keine historischen Anekdoten, kein Ausdruck der „Kleinmütigkeit einer überholten Weltanschauung“ sind, die

436 F. Gerlach et al.: „Digitalisierung für Gesundheit“, Gutachten 2021 des Sachverständigenrats zur Begutachtung der Entwicklung im Gesundheitswesen, Bonn/Berlin, März 2021; S. 17

437 Ebd. S. 52

438 Wogegen man natürlich zaghaft einwenden könnte, dass gerade die Möglichkeiten automatisierter Datenauswertung ein Grund für Datensparsamkeit sein könnten.

439 Ebd., S. 11ff.

440 Mir ist die Paradoxie des Ausdrucke „Privatsphäre-Einstellungen von Facebook“ bewusst, die etwas von „alkoholfreiem Schnaps“ oder „erfreulicher Krankheit“ hat.

441 z.B. B. Johnson: „Privacy no longer a social norm, says Facebook founder“, The Guardian, 11.01.2010 (https://www.theguardian.com/technology/2010/jan/11/facebook-privacy, zuletzt abgerufen April 2021)

man ablegen müsse wie ein Paar aus der Mode gekommener Kleidungsstücke. Die im Gegenteil die - oft eher ungern hergegebene - Haut unter der Kleidung sind.

Mit Blick auf Ihre medizinischen Daten und Ihre Verfügungsgewalt darüber als Patientin und Patient, führt der Salutismus die Gutachterinnen und Gutachter zu interessanten Schlussfolgerungen und Forderungen. Beispielsweise hinsichtlich der „elektronischen Patientenakte“ und der Nutzung medizinischer Daten durch Dritte.

Dabei sieht der Sachverständigenrat übrigens durchaus auch Risiken mit Blick auf die Nutzung einer umfassenden „elektronischen Patientenakte“ (ePA).

Zum Beispiel das Risiko, dass keine signifikante Zahl von Versicherten freiwillig mitmacht. Oder das Risiko, dass sie, wenn sie mitmachen, nicht freiwillig alle ihre Daten hergeben[442]. Beispielsweise aufgrund einer verzerrten Berichterstattung[443], oder weil sie zu weiblich[444], zu unaufgeklärt, zu alt, zu arm oder/und zu ungebildet sind, um die Chancen und das große Ganze zu verstehen oder mit einer kleinteiligen Vergabe zu Zugriffsrechten auf ihre Daten klarzukommen[445]. In dieser Sorge meint man das Echo der spitzen Ausrufe des Erschreckens zu hören, als Google & Co. nach Einführung der europäischen Pflicht zur Nachfrage vor dem Setzen von Cookies zum Tracken („opt-in“) überrascht feststellen mussten, dass die Leute ihre Rechte tatsächlich in Anspruch nehmen, wenn sie können. Unfassbar - die wollen ihre Daten gar nicht hergeben und auch nicht getrackt werden! Obwohl die Marketingabteilung doch immer so glaubhaft das Gegenteil behauptet hat. Glücklicherweise hat der Sachverständigenrat eine Lösung parat: „*Für alle Menschen sollte (in Zukunft: mit der Geburt) eine ePA eingerichtet werden. Der Einrichtung kann durch Patientinnen und Patienten bzw. deren Sorgeberechtigte widersprochen werden.*“[446].

Also nach dem guten Vorbild von Facebook ein Ersetzen des bisher geplanten „opt-in“ (Zustimmungsverfahren) durch ein „opt-out“ (Widerspruchsverfahren): „*Es wird für jede Person eine ePA angelegt, sofern nicht widersprochen wird (erste Opt -out-Option). Patientinnen und Patienten mit einer ePA können jederzeit dem Zugriff auf bestimmte Inhalte durch Leistungserbringer qua „Verschattung“ von ePA-Inhalten widersprechen (zweite Opt-out-Option). Mit der Verschattung, soll bewusst keine unwiderrufliche Löschung einzelner Inhalte vorgenommen werden.“*[447]

Vielleicht fragen Sie sich, warum Sie Ihre Daten nicht löschen können sollen? Naja, weil, wenn Sie es täten, Sie ja wahrscheinlich nicht wüssten, was Sie tun, sonst täten Sie es ja nicht. Zum Beispiel weil Ihnen anders als dem Sachverständigenrat der Über- und Weitblick fehlt[448]. Und warum wollen Sie ein Recht haben, mit dem Sie gar nicht ordentlich umgehen können? Hm?

Damit kein falscher Eindruck entsteht: Die Gutachterinnen und Gutachter haben das „Empowerment“ des Patienten und seine Souveränität durchaus vor Augen. Es ist ihnen sogar mehrere Abschnitte wert[449]. Nur ist das eher im väterlich-erzieherischen Sinn gemeint und vor allem dann wichtig und eine gute Sache, wenn man es als Nützlichkeitsargument für z.B. die eigenen salutistischen Vorstellungen gebrauchen kann. Ansonsten muss man es mit der Autonomie des Patienten ja nun wahrlich nicht übertreiben. Na ja, macht der Sachverständigenrat ja auch nicht.

---

442 Ebd. S. 80
443 Ebd. S. 79
444 Ebd. S. 84
445 Ebd. S. 86.88; vielleicht erinnern Sie sich, was wir in der Einleitung hinsichtlich der Adepten und Jünger einer technologischen „Heilslehre“ festgestellt hatten.
446 Ebd. S. 89
447 Ebd., S. 126
448 Ebd. S. 89, S. 312
449 z.B. Ebd. S. 72f.

Sie wollen zumindest bei der Verwendung Ihrer Daten mitreden, wenn Sie sie schon nicht löschen dürfen? Zumal Sie das Gesundheitssystem mit Ihren Steuern und Beiträgen finanzieren? Jetzt werden Sie aber ein wenig unverschämt, es geht im Salutismus immerhin um das große Ganze. Ganz im Gegenteil: „*Vorrangig sollte geprüft werden, ob für Versorgungsdaten, die als besonders relevant für die Gesundheitsforschung gelten, die Möglichkeit einer Verarbeitung auf gesetzlicher Grundlage ohne Zustimmungserfordernis oder Opt-out-Möglichkeit geschaffen werden kann […].*“[450] Gut, dass der Sachverständigenrat das große Ganze im Blick hat - der Staat möge Ihnen Ihren Egoismus austreiben!

Denn schon die Gründer großer Tech-Unternehmen wussten, dass personenbezogene Daten wie Nachtisch sind: Je mehr, desto besser und am besten viele verschiedene zum Kombinieren. Aber natürlich schön getrennt auf dem Teller - oder bekommen Sie gerne Ihr Mousse au Chocolat vermischt mit den Kaviarschnittchen und der Käseplatte vorgesetzt? Eben. Und genau so wäre zum Beispiel die Anonymisierung von Daten ausgesprochen unappetitlich, schließlich „*ist zu beachten, dass für den Großteil der Forschungsfragen pseudonymisierte Daten benötigt werden [...]. Mit einer Anonymisierung oder Aggregation hingegen ist ein hoher Informationsverlust verbunden. Weitere Informationen aus anderen Datenquellen könnten nicht hinzugefügt werden.*“[451] Stellen Sie sich nur mal vor, Facebook und Google müssten anhand anonymisierter Daten Ihr Profil erstellen oder Sie tracken – das würde doch gar nicht funktionieren! Es ist doch nur konsequent und zu Ihrem Besten, dass der Sachverständigenrat fordert, dass „Ihre“ Daten für die Forschung grundsätzlich *nicht* anonymisiert werden sollten[452].

Um welche Daten geht es, die der Sachverständigenrat speichern, zusammenführen und auswerten will? Da ist er nicht wählerisch. „Wünschenswerte Datenbestände“ wären neben amtlichen statistischen Daten z.B. Behandlungsdaten aus Krankenhäusern, die Daten aus der „elektronischen Patientenakte“ („*Befunde, Diagnosen, durchgeführte und geplante Therapiemaßnahmen […] und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen*“[453]), sowie „*Daten kommerzieller Anbieter und Daten, Daten aus sozialen Medien etc.*“[454]. Also in erster Näherung: Einfach alle Daten, das lässt sich ja auch leichter merken.

Nicht lumpen lassen sich die Gutachterinnen und Gutachter auch mit Blick auf den Personenkreis, der auf Ihre pseudonymisierten Daten zugreifen kann: „*Der Kreis der antragsberechtigten Institutionen, die berechtigt sind, Zugang zu auf gesetzlicher Grundlage bereitgestellten bzw. durch öffentliche Gelder geförderten Forschungsdatensätze zu beantragen, sollte unter bestimmten Voraussetzungen um forschende Unternehmen aus dem Bereich Pharmazie, Medizintechnik und Gesundheits-IT erweitert werden.*“[455]. Also beispielsweise kleine Start-ups, die digitale Gesundheitsanwendungen entwickeln und Google Health oder Microsoft-Nuance, die an der Verbesserung ihrer Algorithmen forschen.

---

450 Ebd. S. 232

451 Ebd. z.B. S. XXVII, S. 93

452 Der Sachverständenrat weist auch darauf hin, dass mit einer Anonymisierung die Möglichkeit verloren gehe, einzelne Patienten bezüglich ihrer Daten zu kontaktieren, für den Fall, dass sich für ihre Gesundheit wichtige Erkenntnisse ergäben. Das ist aus meiner Sicht ein vorgeschobenes Nützlichkeitsargument ohne Grundlage: Wissenschaftliche Erkenntnisse durchlaufen einen Begutachtungsprozess und werden mit der Fachwelt, d.h. den Ärztinnen und Ärzten geteilt, die sie wiederum in die Behandlung von Patienten integrieren, für die die Erkenntnisse relevant sind. Es dürfte praktisch nie der Fall sein, dass einem Einzelnen notfallmäßig und unbedingt vorläufige Ergebnisse einer wissenschaftlichen Studie mitgeteilt werden müssten, die nicht ggf. auch als allgemeine wichtige Information verbreitet werden könnte.

453 §341 SGB V (Stand zum April 2021)

454 SVR-Gutachten, S. 241

455 Ebd. S. 251

Dabei müssen Sie sich übrigens keine Sorgen machen, dass Ihre Daten „auf Abwege“ geraten könnten. Auch daran hat der Sachverständigenrat gedacht und eine Lösung: „*So sollte […] verboten werden, einen Personenbezug für andere als medizinische Behandlungs - und Forschungszwecke herzustellen […]*.“[456] Eine geniale Idee. Warum ist eigentlich nie jemand auf die Idee gekommen, auch Wohnungseinbrüche und Raubüberfälle einfach zu verbieten? Das wäre doch das Einfachste! Gut, dass es zumindest in der Medizin praktisch denkende Sachverständige gibt.

Es kann also gar nichts passieren. Zumal Arbeitgeber, Versicherungen und Banken wie Google und Facebook nach den Daten sowieso nicht fragen oder zumindest „*keinen Gebrauch von solchen Daten und daraus abgeleiteten Erkenntnissen […] machen dürfen.*“[457] Also, zumindest sofern nicht irgendein kommerzieller Datenverwerter oder -händler, an die Daten gekommen ist und „data washing“ betreibt, bloß weil er damit sein Geld verdient. Aber das wird ja sicher nicht passieren. Vermutlich.

Aber eigentlich geht Sie ja sowieso nichts an, was im Einzelnen mit Ihren Daten passiert. Daher fordert der Sachverständigenrat richtigerweise für „Ihre“ Daten die „*Nutzung zu Forschungszwecken standardmäßig bis auf Widerruf ohne spezifische Bindung an Forschungsfragen*“[458]. Wobei ihm im Sinne des Salutismus‘ ja ohnehin am liebsten wäre, auch das Widerrufsrecht zu streichen und zu ersetzen durch „*die Möglichkeit einer Verarbeitung von Versorgungsdaten auf gesetzlicher Grundlage [...] ohne Zustimmungserfordernis oder Opt-out-Möglichkeit […].*“[459]

Und natürlich ist es wichtig, hinsichtlich der Zugriffs- und Auswertungsmöglichkeiten die „*Schaffung eines Fernzugriffs auf den Volldatensatz für möglichst viele Datenbestände*“ zu ermöglichen, um „*auch komplexe statistische Auswertungen vom Arbeitsplatz des Forschenden aus zu erlauben. Das heißt, die Forschenden sollten den Datensatz sehen und direkt auf diesem arbeiten können*.“[460]. Es wäre ja noch schöner, wenn der hochbezahlte Doktorand, Master-Student oder Industriepartner für den Zugriff auf hochsensible Daten extra irgendwohin fahren müsste. Auch der große Naturforscher Darwin hat sich ja bekanntlich seine Finken mit der Post von den Galapagos-Inseln auf seinen Schreibtisch schicken lassen; oder so ähnlich.

Sicher haben Sie sich beim Lesen der Zitate spontan dieselbe Frage gestellt, die auch mir kam: Wie schaffen es die Gutachterinnen und Gutachter, eine derart unglaubliche Zurückhaltung an den Tag zu legen, die schon an Selbstverleugnung grenzt? Wenn sie schon einmal in zwei Jahren den direkten Draht zum Minister haben? Das ist doch unbegreiflich! Warum kein Reichen von Kaltgetränken am Schreibtisch der Forschenden? Wo bleibt das Entrichten eines kleinen Obulus‘ als Bearbeitungsgebühr durch die Versicherten, mit deren Daten sich der Forschende herumschlägt?

Mit Blick auf die Wissenschaft ist den Gutachterinnen und Gutachtern hoch anzurechnen, dass sie neben dem Verweis auf auf diverse Studien[461] auch mit einer eigenen Studie ein schönes und ganz praktisches Beispiel wissenschaftlicher Forschung beisteuern. Dabei ist ein beeindruckendes Ergebnis, dass „*immerhin 63 % der Befragten einer ePA-Nutzung positiv gegenüber[standen]*“[462].

456 Ebd. S. 236
457 Ebd.
458 Ebd. S. 93
459 Ebd. S. 91
460 Ebd. S. 237
461 z.B. die bereits früher diskutierte Studie der Bertelsmann-Stiftung, die völlig offensichtlich politisch motivierte und als „Debattenmunition“ gedachte, einseitige „Studie“ der Stiftung Münch von 2018, in der das Wort „Datenschutz“ praktisch nicht vorkommt, oder Befragungen des Interessenverbands „Bitkom“; vgl. z.B. SVR-Gutachten S. 96, S. 84
462 Ebd. S. 84

Gut, schaut man in die Umfrageergebnisse, steht das genau genommen unter dem Vorbehalt der Freiwilligkeit einer „elektronischen Patientenakte“[463]. Und es sind ganz genau genommen nur 19 %, die der Frage „*Die Nutzung einer elektronischen Patientenakte ist freiwillig. Kommt für Sie die Nutzung der elektronischen Patientenakte grundsätzlich in Frage?*“ uneingeschränkt zustimmen. Während die restlichen 44 % die eher unbestimmte Option „ja, möglicherweise“ wählen, also vielleicht lieber eine elektronische Patientenakte als ein gebrochenes Bein hätten. Aber das ist ja auch eigentlich unwichtig.

Es ist ohnehin nur der Bescheidenheit und Zurückhaltung der Gutachterinnen und Gutachter des Sachverständigenrats zuzurechnen, dass sie nicht näher auf die Umfrage eingehen. Obwohl es natürlich andererseits auch ein bisschen schade ist. Deshalb holen wir das hier ein klein wenig nach.

So findet sich ein besonders klares Antwortverhalten in der Frage zut Freigabe der Gesundheitsdaten in einer (freiwilligen) „elektronischen Patientenakte“ für nicht näher definierte „Forschungszwecke“[464]. Hier meinen immerhin knapp drei Viertel aller Befragten, dass wenn, dann die Patientinnen und Patienten zumindest um Erlaubnis gefragt werden und aktiv einwilligen sollten („opt in“), während weitere rund 10 % der Befragten die Freigabe grundsätzlich ablehnen. Nicht, dass das im Kontext der Gutachtervorschläge weiter erwähnenswert wäre.

Was allerdings doch etwas überrascht, ist, dass rund 15 % der Befragten angeben, sie würden bereits eine Form der „elektronischen Patientenakte“ benutzen[465]. Denn zum Zeitpunkt der Umfrage gab es ja noch keine elektronische Patientenakte im Sinne des Sachverständigenrats[466], und selbst mehrere Monate später, im März 2021, bewegte sich der Anteil der Versicherten mit „elektronischer Patientenakte“ laut Berichterstattung im Sub-Prozentbereich[467]. Auch Vorläufer wie die Anwendung „tk safe“ der Techniker Krankenkasse wurde noch einige Monate vor der Umfrage von weniger als 3 % der Versicherten genutzt[468].

Mit anderen Worten, mit der Studie des Sachverständigenrats *kann* etwas nicht stimmen. Entweder wussten die Befragten nicht, wovon genau die Rede ist, oder die Auswahl war nicht repräsentativ oder beides. Dass ein Auswahleffekt („bias“) zumindest auch eine Rolle gespielt haben könnte, legt die Auswahl der Befragten nahe: Dabei handelte es sich um einen Personenkreis, der einer regelmäßigen Teilnahme an Umfragen eines kommerziellen Marktforschungsinstituts zugestimmt hat und gegen Bezahlung („Aufwandsentschädigung“) an bis zu zwei Umfragen im Monat teilnehmen kann[469].

Möglicherweise gelten in der Medizin oder „Gesundheitsforschung“ andere Regeln als in allen anderen wissenschaftlichen Disziplinen. Aber in allen anderen Wissenschaften würde man die tendenziöse Auswahl und Darstellung von Ergebnisse und das Verschweigen oder Ignorieren von „unerwünschten“ Ergebnissen durch den Sachverständigenrat als das Gegenteil guter Wissenschaft bezeichnen. Man tut sicher gut daran, sich das bewusst zu machen bei der Einschätzung der Argumente und Forderungen der Gutachterinnen und Gutachter nach Zugriff auf *Ihre* Daten für wissenschaftliche Zwecke und die große Sache.

---

463 Sachverständigenrat „Gesundheit“: „Anhang IV - Bericht zur Online-Befragung für das SVR-Gutachten“ (2021), S. 9

464 Ebd. S. 14

465 Ebd. S. 8

466 Vgl. z.B. Gutachten, S. 70

467 K. Schiebold: „Digitale Patientenakte – Top oder Flop?“, Braunschweiger Zeitung, 7.4.2021

468 https://www.ibm.com/de-de/blogs/think/2019/12/13/elektronische-patientenakte/ (zuletzt abgerufen 07.02.2020)

469 Sachverständigenrat „Gesundheit“: „Anhang IV - Bericht zur Online-Befragung für das SVR-Gutachten“ (2021), S. 1

Warum allerdings der Sachverständigenrat in seinem Gutachten fortwährend die Befürchtung formuliert, dass die Umsetzung seiner Forderungen ausgerechnet am *politischen Willen* scheitern werde[470], wird wohl das Geheimnis der Gutachterinnen und Gutachter bleiben. In Würdigung der bisherigen Gesetze und öffentlichen Äußerungen aus dem Bundesgesundheitsministerium würde ich mich nur deswegen auf die Charakterisierung „offene Türen einrennen“ beschränken, weil mir keine Steigerung dazu einfällt. Auch seitens der großen kommerziellen Datenverwerter und Tech-Konzerne wird ihnen der Beifall gewiss sein.

Es ist daher etwas rätselhaft, weshalb sich die Gutachterinnen und Gutachter in der Rolle der einsamen und unverstandenen aber dennoch unerschrockenen Avantgarde des Fortschritts gefallen, die allen politischen Widerständen und persönlichen Risiken zum Trotz und zum Wohl der großen Sache einfach mal sage, was gesagt werden müsse.

Um der Sache willen erscheint es mir sinnvoll, dieses Selbstbild etwas zu korrigieren.

Nein, sie sind nicht die „Avant-Garde“, sie sind die „Derriere-Garde“. Die Nachhut eines Trosses, der sich, angeführt von den großen Tech-Konzernen, längst wie ein Mahlstrom immer tiefer in die Privatsphäre und Grundrechte der Bürgerinnen und Bürger fräst und inzwischen einen immer größeren Appetit auch auf medizinische Daten entwickelt. Die Gutachterinnen und Gutachter trotten ihm gewissermaßen nur beifällig nickend hinterher. Ohne auch nur den Versuch zu unternehmen, den Angriff auf die Privatsphäre der Bürgerinnen und Bürger aufzuhalten und sie zu schützen.

Im Gegenteil. Die Gutachterinnen und Gutachter versuchen faktisch, die vorgegebene Marschrichtung argumentativ abzusichern und die Aufmerksamkeit des zunehmend von Unbehagen erfüllten Publikums auf bizarre Nebenschauplätze zu lenken. Anders lässt sich die ausführliche und wiederholt aufgeworfene Frage eines erhöhten Stromverbrauchs infolge der „unvermeidbaren“ umfassenden zentralen Speicherung und Verwertung[471] Ihrer medizinischen Daten kaum erklären. Es sei denn, dass es ein Missverständnis bezüglich des Unterschieds von Originalität und Absurdität gibt oder der Verweis auf die globalen Ziele nachhaltiger Entwicklung (sustainable development goals, SDGs) in jedem noch so unpassenden Zusammenhang verwechselt wird mit Verantwortungsbewusstsein oder Weltläufigkeit.

Der Sachverständigenrat geht weder auf Grenzen der eigenen Expertise noch auf Interessenskonflikte ein und zeigt im eigenen wissenschaftlichen Beitrag einen problematischen Umgang mit den eigenen Ergebnissen. Er konstruiert als Grundlage seiner Argumentation ein überpersönliches und überzeitliches Patientenkollektiv. Gegenüber dem von den Gutachterinnen und Gutachtern interpretiertem Wohl des „ewigen Kollektivs“ werden hart erkämpfte individuelle Freiheiten und Grundrechte als unmoralisch umgedeutet, relativiert und sollen faktisch ausgehebelt werden, nach Möglichkeit durch den Staat per Gesetz. Damit vertreten die Gutachterinnen und Gutachter in ihrem Text eine Grundhaltung, die als salutistisch bezeichnet werden muss.

Die von den Gutachterinnen und Gutachtern vertretene Haltung ist aus meiner Sicht rechts- und verfassungswidrig und steht im Widerspruch zu den Grundlagen einer freiheitlich-demokratisch verfassten Gesellschaft. Im wissenschaftlichen Kontext können zweifellos auch bewusst provokante Thesen und Einzelmeinungen vertreten werden. Im Rahmen der aktiven, gesetzlich beauftragten[472] Politkberatung aber sind das Verhalten und die Argumentation des Sachverständigenrats nicht akzeptabel und der Verantwortung ihres Auftrags in keiner Weise angemessen. Als Akademiker, Versicherter und Bürger erfüllt es mich mit Scham und macht mich traurig. Zum Wohl.

---

470 Ebd., z.B. S. 7, S. 82, ...
471 Ebd., z.B. S. XXIV, S. 30, S. 53, S. 121, ...
472 § 142 SGB V