Elektronische Patientenakte liefert sensible Daten – nicht nur für Behandler:innen

Bernd Kuck

Google macht weiterhin Werbung für Spionage Software. Wer bei Google „Freundin, Handy“ (1) eingibt, der kommt zu einer Spionagesoftware, mit der dem Grunde nach digitale Gewalt ausgeübt werden kann. Daran lässt sich bereits ermessen, wie krank das System Google ist. Die grundsätzliche Methode von Datenkraken besteht ja darin, mittels immer besserer Algorithmen möglichst viel über die Nutzer der Angebote der Big Five „GAFAM“ Google, Amazon, Facebook, Apple und Microsoft in Erfahrung zu bringen. Der sogenannte Big-Other-Kapitalismus (2) ist die Steigerung von Big Brother, der sich dagegen wie ein Weisenknabe ausnimmt. Inzwischen wird immer deutlicher, welche Macht sich da neben den Regierungen entwickelt, besonders bringen die Konzerne unsere Demokratie in Gefahr. „Nackt im Netz“, eine Dokumentation im ZDF gibt einigen Einblick in das Geschehen.

Wie dabei die Nutzer:innen eingefangen werden ist ziemlich subtil und raffiniert, wird doch vor allem mit der Bequemlichkeit geködert und mit der Suggestion: Das machen wir nur für dich, damit du schnell an Informationen kommst und es leichter im Leben hast. Aber wozu um alles in der Welt braucht meine Körperwaage einen Internetzugriff? Und vor allem funktioniert sie nicht richtig, wenn ich die zugehörige App nicht installiere und der Übertragung von Daten, wohin-auch-immer, nicht zustimme. Beim Einkauf vor Ort wird unter Umständen ungefragt ein Kundenkonto angelegt. Über das Payback System muss mensch wohl kein Wort mehr verlieren, es soll aber immer noch Menschen geben, die glauben, ihnen werden aus lauter Freundlichkeit und Nächstenliebe oder als Kundenservice Punkte gutgeschrieben, die sie dann als Rabatt einlösen können. Das war mal so vor langer Zeit, als es noch die Rabattmarkenhefte gab und da gab es noch nicht den schwunghaften Handelt mit Adressen oder noch subtileren Daten. Und die Behörden spielen mit, wollen am liebsten alles vernetzen. Das es inzwischen nur noch einen Personalausweis mit Fingerabdruck gibt, ist einfach von den Bürger:innen geschluckt worden. Ist doch klar, dass Bürger:innen grundsätzlich erst einmal potenzielle Kriminelle sind. So kommt zu den drei Affen (nichts sehen, nichts hören, nichts sagen) noch ein vierter hinzu: ich habe nichts zu verbergen.

Zuboff (3) nennt dies (‚ist doch nur zu deinem Besten‘) den offiziellen Text. Im Subtext heißt es: Wir wollen alles über dich wissen, damit wir dieses Wissen zu Geld machen können. Das begann mit immer besser passender personalisierter Werbung, mündet dem Grunde nach jedoch in den Diebstahl der Identität und stellt einen tiefen Eingriff in die informationelle Selbstbestimmung dar, führt letztlich zum Schulterschluss zwischen Überwachungskaptitalismus und Überwachungstaat. Denn auch der Staat sammelt Daten, stellt Überwachungskameras auf und experimentiert mit Gesichtserkennungssoftware. „Etwa am Bahnhof Berlin-Südkreuz. Dort ist 2019 die intelligente Videoüberwachung in die zweite Pilotphase gestartet. Eine Software soll gefährliche Situationen automatisch erkennen – etwa, wenn jemand am Boden liegt oder es zu einer plötzlichen Menschenansammlung kommt. Dazu sind auf dem Bahnhofsgelände rund 80 Kameras installiert. Anders als beim ersten Test im vergangenen Jahr kommt dieses Mal keine Gesichtserkennung zum Einsatz. Datenschützer hatten damals scharf kritisiert, dass die Software der Bundespolizei automatisch Personen identifiziere und abgleiche (4). Dennoch könnte ein solches System bald Schule machen. Hinsichtlich einer breiten Einführung sei man zuversichtlich, erklärte das zuständige Bundesinnenministerium zum Abschluss des Tests. Die Fehlerquote lag bei durchschnittlich unter 0,1 Prozent. Einen aus tausend Fahrgästen hat die Software also mit einer anderen Person verwechselt“ (5). Auch die Gesichtserkennung wird mit dem Spaßfaktor den Leuten schmackhaft gemacht. Mit „FaceApp“ kann mensch schon mal sehen, wie ersie in 10, 20 oder 30 Jahren aussehen wird (6). Das ist lustig – oder doch nicht? Biometrische Daten (Gesichtserkennung, Iris, Fingerabdruck) sind unveränderlich. Welches Desaster entsteht wohl für einen Menschen, wenn ihm diese Daten gestohlen werden? Der Chaos Computer Club (7) hat schon 2005 gezeigt, dass es kein Hexenwerk ist, eine Attrappe des Fingerabdrucks eines anderen Menschen herzustellen und sich so eine zweite Identität zuzulegen.

Selbst ohne diesen direkten Identitätsdiebstahl, mensch braucht immerhin einen original Fingerabdruck, etwa von einem Glas, lassen sich aus den Spuren im Netz Identitäten ermitteln. Am Beispiel der Apps, die mensch so nutzt, lassen sich Gewohnheiten ausspionieren. Neuerdings müssen die Nutzer:innen zwar der Speicherung von Cookies zustimmen. Tut mensch dies nicht, funktioniert die Seite oder die App nicht richtig oder gar nicht. Angeblich lassen sich bestimmte Tracker abschalten. Ein Blick in die Rubrik „berechtigte Interessen“ offenbart allerdings eine ungeheure Masse an Firmen mit „berechtigten Interessen“, die alle einzeln abgestellt werden müssen. Digitalcourage e. V.

hat sich die Mühe gemacht, bei den Diensten nachzuschauen, wozu sie eigentlich gehören. Hinter unglaublich vielen stecken die Big Five (8). Digitalcourage empfiehlt dann Dienste, bei deren Nutzung mensch an den Big Five vorbeikommt. Zuboff wies allerdings schon darauf hin, dass diese Art der Selbstverteidigung aufwändig ist und das Problem nicht wirklich löst. Die Hinweise von Frau Zotzmann-Koch (9), wie mensch sich bei der Bewegung im Netz, egal ob mit Smartphone, Tablett oder PC schützen kann, sind hilfreich, gehen jedoch an der grundsätzlichen Problematik der unregulierten Macht der „GAFAM“ vorbei. Hier wäre die Politik gefragt. Die ist aber z. Z. im Digitalisierungswahn. Alles soll digitalisiert werden, egal wie sinnvoll; und der Datenschutz bleibt auf der Strecke. Die aktuellen Wahlprogramme der Parteien bleiben in ihren Aussagen hinsichtlich des Datenschutzes leider vage. Widerstand von einzelnen oder auch Gruppe verpufft leider. Die „GAFAM“ pflegen einzulenken – bzw. sie tun so und warten ab, bis sich die Wogen wieder glätten. So lenkte Apple kürzlich ein, indem sie den kleinen App-Entwicklern geringere Provision zubilligten, wenn sie ihre App in den Apple-Store einstellen (10). Zuboff hatte dies bereits als Taktik entlarvt. Wir dürfen auch nicht vergessen, dass Apple und Google eine Markt beherrschende Position haben. Wer ein Smartphone nutzen will, kommt an deren Stores nicht vorbei! Zwar gibt es inzwischen einige Alternativen (zum Beispiel F-Droid für freie Apps auf Android) – aber doch noch recht spärlich und oft nicht besonders komfortabel. Alle möglichen Apps sammeln Daten und verkaufen sie weiter. So offenbarte ein Datencheck von Liefer-Apps (Lieferando, Volt und Gorillas), dass sie noch ein Nebengeschäft mit den Daten ihrer Kunden etabliert haben. Sie übermitteln neben den Standortdaten die Werbe-ID an diverse Analysedienste. „Wir sehen in unseren Analysen aber regelmäßig, dass die Werbe-ID gemeinsam mit eindeutigen Nutzerinformationen wie dem Namen oder der E-Mail-Adresse erhoben wird. In dem Moment verliert sie ihre Anonymität und lässt eindeutig auf Personen schließen“ (11).

Wer wissen möchte, was heute schon möglich ist, der sei auf das Experiment „Made to Measure“ hingewiesen, wozu es derzeit eine Dokumentation in der ARD-Mediathek (12) zu sehen gibt. Problematisch in dieser Doku bleibt aber, dass die Macher kein Problem darin sehen, anhand von Suchanfragen Rückschlüsse darauf zu ziehen, ob jemand etwa suizidal ist oder gerade einen Amoklauf plant. Gleichwohl wollen sie dies nicht den gewinnorientierten Konzernen überlassen. Es könnte durchaus hilfreich sein, wenn statt Werbung Hilfsangebote eingeblendet werden. Nur ist hierbei immer noch die Verfolgung und Auswertung von Suchanfragen die Voraussetzung. Und wer reguliert und wer kontrolliert hier. Derzeit ist es gleichwohl unverantwortlich, wenn etwa für Menschen

mit einer Essstörung, auf die sich schließen lässt aufgrund ihrer Suchanfragen, Diätwerbung und weitere Möglichkeiten der Gewichtsreduktion eingeblendet werden.

Die elektronische Patientenakte (ePA)

Damit bin ich bei dem Thema der elektronischen Patientenakte (ePA), die seit dem 1. Januar 2021 als neues Angebot der Krankenkassen durch gesetzliche Vorgabe eingeführt wurde. Die ePA wiederum wird über die sogenannte Telematikinfrastruktur (TI) betrieben, ein von der GEMATIK (Hauptgesellschafter ist das Bundesgesundheitsministerium) betreutes Netzwerk, an dass sich alle Akteure des Gesundheitswesen anzuschließen haben. Für Ärzte und Psychotherapeuten gilt bereits, dass bei Nichtanschluss eine Strafe in Höhe von 2, Prozent des Umsatzes mit den KVen (Kassenärztliche Vereinigungen, die die Leistungen mit den Krankenkassen abrechnen) zu zahlen ist. „Die Kassenärztliche Vereinigung (KV) Berlin (hat) im vergangenen Jahr (...) von Mitgliedern, die nicht an die Telematikinfrastruktur (TI) angeschlossen sind, 780.000 Euro einbehalten“ (13). Nun hat die jüngste Vergangenheit bereits gezeigt, dass die TI recht anfällig gegen Ausfälle ist, was für Chaos in den Praxen gesorgt hat. Zwar wurde die Installation des sogenannten Konnektors von den Krankenkassen gegenfinanziert. Auf den Kosten für die Serviceleistungen der IT-Firmen, die bei Ausfällen tätig werden, bleiben die Praxen jedoch sitzen. Abgesehen davon ist die Handhabung der ePA an Smartphone oder Tablett gebunden. Wer also wissen will, was in seiner Patientenakte steht und kein Smartphone oder Tablett besitzt, bleibt im Dunkeln. Der Bundesbeauftragte für den Datenschutz, Ulrich Kelber, hat dies scharf kritisiert (14). Dass die Patienten in den Praxen oder bei den Krankenkassen die Daten einsehen können sollen, erhöht wiederum den Aufwand und macht es unwahrscheinlich, dass Patienten davon überhaupt Gebrauch machen. Was ja möglicherweise so gewollt ist.

Besonders problematisch ist auch das Hosting der Datenbank in einer Cloud. Und hier kommen darüber hinaus private Anbieter ins Spiel, doch wohl getreu der politischen Linie der letzten Jahre, möglichst viele staatliche – und das heißt doch eigentlich am Gemeinwohl orientierte – Leistungen zu privatisieren. Mit der Cloud basierten Speicherung wurde IBM beauftragt (15). Bekanntlich ein amerikanisches Unternehmen, das den USA per Gesetz Zugang zu ihren Daten ermöglichen muss.

Nichts gegen Digitalisierung, die immer wieder im Bundesgesundheitsministerium von J(ott) Spahn gefordert wird; jedoch sind täglich Meldung von Datenlecks zu verzeichnen, gerade auch im Gesundheitsbereich. Diese äußerst sensiblen Daten sind bei Kriminellen sehr begehrt, denn sie lassen sich gut verkaufen. Das wird in Zukunft noch wichtiger werden, wenn etwa Versicherungen oder Kreditgeber sich dafür interessieren, um ihre Risiken weiter zu minimieren. Hier nur ein paar Beispiele der letzten Zeit: „Das Klinikum Wolfenbüttel ist Ziel einer Hackerattacke geworden. Bisher deuten die ersten Hinweise darauf hin, dass es sich bei dem IT-Angriff um einen Erpressungsversuch handelt. Die Staatsanwaltschaft Göttingen hat die Ermittlungen übernommen“ (16). „Laut einer Umfrage von *BR* und "Zeit Online" ist es Tätern in mehr als 100 Fällen gelungen, IT-Systeme von Behörden und öffentlichen Einrichtungen zu verschlüsseln. Die Bundesregierung hat über die Fälle keinen Überblick“ (17). Kriminelle haben die Daten des irischen Gesundheitsdiensts verschlüsselt. Sie wollen 20 Millionen Euro erpressen (18). Frankreich: Daten von fast 500.000 Patienten gestohlen und im Internet veröffentlicht (19). „Datenleck: 600.000 Patienten der DuPage Medical Group betroffen. Die DuPage Medical Group, die größte Gruppe unabhängiger Ärzte im Bundesstaat Illinois, hat damit begonnen, etwa 600.000 Patienten über eine Sicherheitsverletzung zu informieren, bei der ihre persönlichen und geschützten Gesundheitsdaten möglicherweise kompromittiert wurden. San Andreas Regional Center Opfer eines Ransomware-Angriffs. Das San Andreas Regional Center in San Jose, Kalifornien, hat damit begonnen, Patienten darüber zu informieren, dass ihr PHI möglicherweise bei einem Ransomware-Angriff im Juli 2021 kompromittiert wurde“ (20). Das ließe sich seitenlang fortsetzen. Das heißt nun mit Blick auf sensible Gesundheits- bzw. Krankheitsdaten, dass sie besonders geschützt werden müssen. Dazu bräuchte es ein anderes Vorgehen als bislang mit der Einführung der ePA vorgesehen.

„Eine elektronische Patientenakte ist ja z.B. 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“ Kopie gegen Datenverlust gesichert, die vielleicht am einfachsten beim Hausarzt lokal und isoliert gespeichert ist. Geeignet gestaltet wiederum impliziert beispielsweise eine spezielle, zertifizierte und gesetzlich geschützte Hardware-Schnittstelle und hinreichenden Speicherplatz, wie ihn jede micro-SD-Karte aufweist (21). Man würde also vermuten, dass es dem Bundesministerium für Gesundheit darum geht,

z.B. die Spezifikationen der Gesundheitskarte mit ihrer Speicherbegrenzung auf wenige Kilobyte den 2020er Jahren anzupassen. Dies legt ja auch die zur „elektronischen Gesundheitskarte“analoge Bezeichnung ‚elektronische Patientenakte‘ nahe“ (22).

Dies wäre auch mit einem Stick möglich, falls mensch sich sorgt, nicht genug Speicherplatz zur Verfügung zu haben. Aber weit gefehlt. Es geht ja auch nicht um Datensicherheit, sondern um ein neues Geschäftsmodell. Der Bereich der „Gesundheitsindustrie“ ist in 2019 mit einer Bruttowertschöpfung in Höhe von 81,2 Mrd. Euro einer der größten deutschen Wirtschaftszweige und macht 7,5 Prozent aller deutschen Exporte aus (23). Entsprechend fordert der Bundesverband der Deutschen Industrie (BDI) einen leichteren Zugang zu den Gesundheitsdaten: „Deutschland und die EU müssen jetzt die Weichen für eine nachhaltige Innovationsförderung, einen gemeinsamen europäischen Gesundheitsdatenraum und ein digitalisiertes Gesundheitswesen stellen, in dem der Zugang und die Nutzung von Daten zu Forschungszwecken auch für die industrielle Forschung gewährleistet sind“ (24). Dies ist generell das zum Mantra gewordene Argument: Die Forschung benötigt den Zugang. Mag sein, dass es etwas umständlicher für „die Forschung“ ist, relevante Daten zu erhalten, wenn die Patienten eigens und ausdrücklich ihre Zustimmung geben müssen. Die Industrie sei ja bereit, hier Verantwortung zu übernehmen. Entsprechend seien durch das Digitale-Versorgungs-Gesetz (DVG), dem Patientendaten-Schutz-Gesetz (PDSG) Voraussetzungen geschaffen worden, sowie die Einführung von erstattungsfähigen digitalen Gesundheitsanwendungen (DiGA). Dieser Weg müsse „konsequent fortgesetzt“ und ausgedehnt werden. Widerstände wurden während der Pandemie „gebrochen“ und zum Beispiel die Videosprechstunde erfreue sich großer Akzeptanz bei Ärzt:innen und Patient:innen. Auch hier ist der Datenschutz nicht gewährleistet, wenn Anbieter zum Beispiel in den USA gehostet sind oder Google Cloud nutzen. Und natürlich ist der zu erwartende (Geld-)Segen der elektronischen Patientenakte (ePA) nicht zu vergessen. „Entscheidend hierbei sind Daten“, um die medizintechnischen Entwicklungen voran zu bringen. Da ist wohl wenig umstritten, dass die digitale Überwachung von Herzoperierten oder Diabetikern Vorteile mit sich bringen kann, sieht mensch mal vom Problem der Gewährleistung der Datensicherheit und der Hackbarkeit von Herzschrittmachern ab (25). „Auch der Datenschutz bzw. insbesondere die einheitliche Umsetzung bestehender Regeln, können für Forscher besondere Hürden schaffen, wodurch Deutschland und Europa im digitalen Wettlauf im Vergleich zu USA und China de facto ins Hintertreffen geraten“ (26). Erfreulicherweise habe ja J. Spahn für einen europäischen Gesundheitsdatenraum plädiert, da „die Datenverfügbarkeit zunehmend über die

Wettbewerbsfähigkeit eines Standortes entscheidet“. Daher beansprucht die Industrie „gleiche Berechtigung wie andere forschende Akteure beim Zugang zu Daten«. Natürlich soll das Grundprinzip des Freihandels erhalten bleiben (27). Neue Bedrohung geht von der Europäischen Kommission mit ihrem Vorschlag der E-Evidence für die Datensicherheit aus. Internetdienstanbieter sollen verpflichtet werden, bei strafrechtlichen Verfahren Daten ihrer Kunden zu übermitteln. „Dies gilt auch für Daten aus anderen Mitgliedsstaaten und auch für Fälle bei denen nach dem Recht der anderen Mitgliedstaaten überhaupt keine strafbaren Handlungen vorliegen. Cloud-Anbieter und Internetdienstleister müssten also Daten ihrer Kund*innen an Ermittlungsbehörden der EU-Mitgliedsstaaten weitergeben“ (28).

Sehr gerne sähe die industrielle Gesundheitswirtschaft (iGW) auch die Etablierung von Public Private Partnerships (PPP). Das die für Steuerzahler und Kommunen deutlich teurer sind, ist inzwischen mehrfach belegt, Kostendämpfung eine Mär darstellt, wie sie von Kapitalinteressen gerne verkündet wird (29). „‘Personalized Healthcare’ unter Berücksichtigung aller Daten eines Patienten aus unterschiedlichen Etappen der ‚Patient Journey‘“ sind da natürlich besonders interessant. Auch der Einsatz von künstlicher Intelligenz (KI) und digitaler Assistenzsysteme. Das kann für die Diagnostik sicherlich interessant sein; von Datenschutz ist hier aber nicht die Rede. Denn »für eine digitale Transformation sind vor allem Investitionen in eine digitale Gesundheitsinfrastruktur sowie die schnelle Vernetzung aller Akteure im Gesundheitswesen innerhalb der Telematikinfrastruktur entscheidend (Hervorhebung, BK)« (30).

Dadurch, dass das Gesundheitsministerium Hauptgesellschafter der Gematik ist, sollen die Entscheidungen beschleunigt werden. „Dies scheint bisher auch gut zu gelingen“. Und im Sinne der Akzeptanzförderung bei Patienten und Ärzten soll der Nutzen früh sichtbar werden (was ja nicht so recht gelingt). Leider, leider, machen die „hohen Hürden im Bereich des offenen Austausches von Daten in Deutschland (…) viele dieser Lösungen nicht möglich“ (31). Der Begriff der wissenschaftlichen Forschung sollte so weit gefasst werden, dass die Industrie ebenfalls den Datenzugriff hat. In dem Zusammenhang wird auch Prof. Dr. med. Ferdinand M. Gerlach erwähnt, der sich gegen „falsch verstandenen Datenschutz ausspricht (…) Daten teilen heißt (…) besser heilen“ (32). Ergo: „Dafür braucht die private Forschung einen gleichberechtigten Zugang zu Forschungsdaten“. Als beispielhaft werden Finnland, Dänemark und Estland genannt, die ja in jüngster Zeit durch Datenhacks zweifelhafte Berühmtheit erlangten (33). Die iGW werde gesellschaftlich hauptsächlich als Kostentreiber wahrgenommen. Mensch sollte

doch eher darauf schauen, dass sie einen wesentlichen Beitrag zum BIP leistet – und vor allem Arbeitsplätze schafft.

Und da wir ja schon so gute Erfahrungen mit einklagbaren Ansprüchen aus den Handelsabkommen haben, sollten in solchen Handelsabkommen die Standards für klinische Studien „und Markzulassungen – einklagbar – verankert werden“. Und ganz wichtig: Unternehmen sollten von Steuern entlastet werden, da in anderen Ländern weniger Steuern anfallen, was sich zum Nachteil des Wirtschaftsstandortes Deutschland, auch für die iGW, auswirkt (34). Schließlich ist „Gesundheit (…) einer der Megatrends der Zukunft“. Deutlicher wird der Sinn – auch der ePA - wohl kaum. Der Druck, mit dem die TI und die ePA eingeführt werden, lässt sich als Ausdruck der dahinter liegenden Geschäftsinteressen verstehen. Denn der Nutzen für Patienten und für Ärzte/Psychotherapeuten ist eher marginal. Wie schon bei den Angeboten von „GAFAM“ sollen die Anwender und Versicherten mit Vergünstigungen und Kosteneinsparungen gelockt werden, „die ‚signifikant genug‘ sein sollten, um die Leute dazu zu bewegen, hinsichtlich ihrer Sorge um die Privatsphäre ‚einen Kompromiss einzugehen‘ – ‚trotz anhaltender Bedenken‘“ (35). Solche Angebote sind etwa günstigere Versicherungstarife bei der Krankenversicherung, wenn mensch seine Gesundheitsdaten zur Verfügung stellt. McKinsey sprechen denn auch von »völlig neuen Geschäftsbereiche(n)« in den »Datenmärkten«. So lasse sich etwa »Gesundheitsüberschuss« durch »relevante Empfehlungen monetarisieren« (36).

Der Sachverständigenrat Gesundheit greift denn auch die Praxis der Nutzer auf. Da die sowieso schon die Daten tracken lassen und ‚freiwillig‘ die Daten ihrer Gesundheitsapps den Konzernen zur Verfügung stellen, sollen sie sich doch nun nicht so anstellen, wenn die Daten über die TI abgegriffen werden. Und damit nicht genug, sollen doch bitteschön alle Neugeborenen direkt eine ePA erhalten, ebenso wie neu Zugezogene – es sei denn, sie widersprechen aktiv (opt-out Verfahren) (37). Dieser Automatismus wird von vielen Seiten heftig kritisiert. Besonders ist damit das höchste Gut der ärztlichen/psychotherapeutischen Beziehung zur Disposition gestellt: Die Schweigepflicht. Das Bündnis für Datenschutz und Schweigepflicht (BfDS, 38) stellt daher klar: „Datenschutz ist kein lästiges Hindernis für technologischen Fortschritt, sondern eine vertrauensbildende Notwendigkeit und damit die Grundlage für Entwicklung. Heute können wir Ärzte und Psychotherapeuten integer versichern, dass Daten bei uns verwahrt bleiben, solange die Patienten uns nicht von unserer Schweigepflicht entbinden. Mit der ePA, noch dazu automatisch angelegt per Geburt oder Zuzug, entziehen Sie uns den Boden

für eine vertrauensvolle Zusammenarbeit mit unseren Patienten. Die therapeutische Beziehung ist, vielfach nachgewiesen, einer der größten Wirkfaktoren unserer Arbeit. Für den Nutzen digitaler Gesundheitsanwendungen, die Sie ebenfalls so sehr empfehlen und verbreitet wissen möchten, gibt es unserer Kenntnis nach noch keinen einzigen tragfähigen Nachweis“ (39).

Über all dies werden die Betroffenen nicht offen informiert. Und da die Krankenkassen mehr und mehr zu kapitalistischen Wirtschaftsbetrieben mutieren, packen sie denn auch gleich allerlei Werbung in ihre Gesundheits-App. So sind zum Beispiel die „Serviceangebote“ auf der APP der Techniker Krankenkasse nicht von der ePA getrennt. Und vor allem: Mensch bekommt entweder alles oder nichts. Die ePA ist ein Modul der APP.

Sebastian Raupach (22) bringt es auf drei Punkte:

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.

Dem ist nichts hinzuzufügen.

Anmerkungen:

(1) Zugriff 11.9.2021, 15:30
(2) Zuboff, Shoshana (2018): Das Zeitalter des Überwachungskapitalismus, Campus 2018
(3) ebd.
(4) Siehe etwa den 29. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit 2020; Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI); https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/29TB_20.html
(5) Der Tagesspiegel, 22.7.2019, https://www.tagesspiegel.de/politik/faceapp-voll-im-trend-die-vor-und-nachteile-der-automatischen-gesichtserkennung/24684654.html
(6) ebd.
(7) Chaosradio, Zugriff 11.9.2021, 16:38
(8) Zugriff 10.9.21, 14:30
(9) Zotzmann-Koch, Klaudia: Dann haben die halt meine Daten. Na und! Edition Silbenreich 2021

(10) Handelsblatt, 27.8.2021, Zugriff 14:20
(11) Mobilsicher, Apps gecheckt: Liefer-Apps (Android), https://mobilsicher.de/ratgeber/apps-gecheckt-liefer-apps-android (Ausdruck vom 09.09.2021).
(12) verfügbar bis 20.8.2022
(13) Ärztenachrichtendienst, 4.9.2021, https://www.aend.de/article/214033
(14) 29. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit 2020; Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), S. 36
(15) Bündnis für Datenschutz und Schweigepflicht, https://www.gesundheitsdaten-in-gefahr.de/ (Zugriff: 1.9.2021, 19 Uhr)
(16) Deutsches Psychotherapeuten Netzwerk (DPNW) Newsletter 16.7.2021
(17) 29.6.2021, https://www.tagesschau.de/investigativ/br-recherche/ransomware-103.html; https://www.br.de/nachrichten/bayern/cyberangriff-aufs-rathaus-der-gemeinde-kammeltal,SV0z6s3
(18) https://taz.de/Cyberattacke-in-Irland/!5773456/ (Zugriff 18.5.2021)
(19) https://www.nzz.ch/technologie/cyberkriminalitaet-in-frankreich-patientendaten-von-wohl-500-000-personen-im-netz-veroeffentlicht-ld.1604042 (Zugriff: 26.2.2021)
(20) Deutsches Psychotherapeuten Netzwerk (DPNW) Newsletter 10.9.2021
(21) „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 beschriebener DIN A4 Seiten Text plus Tausend unkomprimierten Bildern mit einer Auflösung von 12 Megapixeln bei 24 Bit pro Pixel. Das sollte erstmal reichen“ (Raupach, 2021, Fußnote 15).
(22) Raupach, Daten oder Freiheit, Februar 2021, https://www.europahelden.eu/archiv_datenfreiheit.html
(23) Strategie für die industrielle Gesundheitswirtschaft, Positionspapier des BDI (Bundesverband der Deutschen Industrie), März 2021
(24) a. a. O., S. 8
(25) https://www.deutschlandfunk.de/medizinische-geraete-wenn-hacker-herzschrittmacher.684.de.html?dram:article_id=465318 (Zugriff: 7.12.2019)
(26) a. a. O., S. 11
(27) zur Problematik der Freihandelsabkommen: https://www.attac-netzwerk.de/freiburg/archiv/protest-gegen-freihandelsabkommen; https://www.cicero.de/aussenpolitik/freihandelsabkommen-die-gutenachtgeschichte-der-oekonomen/59158, Zugriff: 12.9.2021, 16 Uhr.
(28) aus der Petition der DPNW, https://www.change.org/p/europa-parlament-kein-zugriff-auf-medizinische-daten-durch-die-e-evidence-verordnung?signed=true
(29) "Riskantes Geschäft mit Investoren" https://www.wiwo.de/politik/deutschland/oeffentlich-private-partnerschaft-fundamentale-nachteile/6496008-1.html; "Für Kommunen, Länder und den Bund gelten öffentlich-private Partnerschaften als ein Ausweg, um notwendige Investitionen zu leisten. Allerdings zieht der Bundesrechnungshof eine vernichtende Bilanz. Viele Projekte wurden am Ende teurer als durch eine rein öffentliche Finanzierung." https://www.deutschlandfunkkultur.de/oeffentlich-private-partnerschaften-pleiten-pech-und-pannen.976.de.html?dram:article_id=310179, Zugriff: 13.4.2012, 19 Uhr.
(30) Strategie für die industrielle Gesundheitswirtschaft, Positionspapier des BDI (Bundesverband der Deutschen Industrie), März 2021, S. 58
(31) a.a.O., S. 60
(32) Hier wird Bezug genommen auf das Gutachten des Sachverständigenrates Gesundheit (SVR), https://www.svr-gesundheit.de/
(33) http://www.dtoday.de/startseite/panorama_artikel,-Vertrauliche-Psychotherapie-Notizen-von-Zehntausenden-in-Finnland-gehackt-_arid,752420.html; in Dänemark, das als Telematik- Vorreiter

gilt, wurden schon im Jahr 2005 CD´s mit fast alle dänischen Patientenakten „aus Versehen“ an die chinesische Botschaft (Visumstelle) in Koperhagen geschickt; https://patientenrechte-datenschutz.de/2017/10/18/estland-estland-ueber-alles-oder-ueber-die-folgen-der-digitalisierung-aller-lebensbereiche-fuer-den-schutz-von-gesundheitsdaten/.
(34) Strategie für die industrielle Gesundheitswirtschaft, Positionspapier des BDI , S. 73
(35) Zuboff, 2018, S. 250
(36) a. a. O., S. 252
(37) s. (20)
(38) https://www.gesundheitsdaten-in-gefahr.de/
(39) Offener Brief an den Sachverständigenrat Gesundheit, Juni 2021; https://patientenrechte-datenschutz.de/offener-brief-an-den-sachverstaendigenrat-gesundheit-svr-elektronische-patientenakte-epa-von-geburt-an-das-ist-das-ende-der-selbstbestimmung-ueber-die-eigenen-gesundheitsdaten/