DATEN RETTEN LEBEN
DatenRettenLeben.net

Eine Initiative für die effektive Nutzung von Daten in der Medizin von:

BiM BUNDESVERBAND INTERNETMEDIZIN QuR.digital VORBERG.law

Daten retten Leben – Whitepaper

Hamburg, 28. Januar 2022

Daten retten Leben! Das ist keine Medizinromantik, sondern einfache Realität. Die beste Medizin benötigt möglichst umfassende Informationen über und für den Patienten. Verbessern kann sich die Medizin ausschließlich im Rahmen von Forschung und Entwicklung. Und Grundlage jeder Forschung und Entwicklung ist die Erhebung, Sammlung und Auswertung von Daten. Dabei gilt der Grundsatz: „je mehr, desto besser“, weil eine breite Datensammlung bessere und genauere Erkenntnisse ermöglicht.

Smartphones, Fitness-Tracker und Co. sammeln ständig Daten beziehungsweise können dies tun. Solche Datensätze können sinnvoll genutzt werden, wenn eine entsprechende Verfügbarkeit und Auswertung gewährleistet ist. Dabei geht es nicht nur um Gesundheitsdaten und die direkte Auswertung von gemessenen Vitalparametern (Herzfrequenz, Blutsauerstoff, Atem usw.). Gute Datenmedizin ist gute Medizin.

Aber auch die Verwendung und Auswertung von nicht-Gesundheitsdaten wie Bewegungs- und Kontaktdaten können einen erheblichen Nutzen haben und indirekt die Gesundheit schützen. So war es immer eine Kernstrategie im Rahmen der Corona-Pandemie, Hot-Spots und Infektionsherde frühzeitig zu erkennen und Risikokontakte nachvollziehbar zu machen und entsprechende Warnungen und Quarantäne-Anordnungen auszugeben. Digitale Lösungen wurden dabei zunächst gar nicht und später nur sehr zögerlich und zurückhaltend eingesetzt. Das Ergebnis sind in Deutschland bislang 90.000 Todesfälle, die direkt oder indirekt mit dem Corona-Virus in Zusammenhang gebracht werden und massive, historische Grundrechtseinschränkungen inklusive monatelangen „Lockdowns“, Fortgang ungewiss.

Doch warum nutzen wir die Möglichkeiten der Digitalisierung so zögerlich zur Verbesserung der Gesundheitsversorgung und zur besseren Bewältigung großer Krisen? Festzustellen ist immer wieder eine besondere Affinität zum Datenschutz, die bereits im Rahmen der Diskussion neuer Lösungsansätze viele gute Vorschläge im Keim erstickt. Doch wie verhält es sich eigentlich genau mit dem Datenschutz, wenn doch die Verwendung der Daten so kostbar sein kann, dass Leben gerettet werden können? Muss der Staat hier Mechanismen bereitstellen, um eine aktive Datenteilung zu ermöglichen? Ist der Staat sogar verpflichtet, zum Schutze der Gesundheit der Bevölkerung ein Recht auf Datenteilung zu etablieren?

Dieses Whitepaper ist zugleich ein Plädoyer für eine neue datenschutzrechtliche Bewertung allen staatlichen und behördlichen Handelns. Wo Risiken und Eingriffe diskutiert werden, müssen immer auch zwingend die Mengen aller methodischen, konzeptionellen, organisatorischen und technischen Maßnahmen und Verfahren zur Behandlung der Ressource „Daten“ mit dem Ziel, sie mit ihrem

maximalen Nutzungspotenzial in die Geschäftsprozesse einzubringen und im laufenden Betrieb deren optimale Nutzung zu gewährleisten, diskutiert werden.

Das Whitepaper soll auch Sie dazu ermutigen, eine Datennutzung- und Verbreitung aktiv zu betreiben und Ihre vielleicht skeptische Denkweise kritisch zu hinterfragen.

I. Medizin braucht Daten – Patienten brauchen Daten

Um auch seltene Nebenwirkungen eines Impfstoffes oder Medikamentes zu entdecken, sind Studien mit einer großen Vielzahl von Teilnehmern nötig. Um Behandlungsmöglichkeiten gefährlicher Krankheiten zu verbessern, müssen Therapieansätze möglichst in der Breite verglichen werden. Wenn jeder Arzt isoliert seine eigenen Erkenntnisse sammelte und kein Arzneimittel in Studien getestet werden könnte, wird die Medizin auf der Stelle stehen bleiben. Niemals will ein Arzt eine Therapie beginnen, ein Medikament verschreiben oder eine Diagnose stellen, ohne dabei auf das gesammelte Wissen der bisherigen medizinischen Forschung zurückblicken zu können. Je umfangreicher das gesammelte Wissen und die Datenlage ist, desto besser und genauer kann die individuell beste Behandlung erfolgen.

Wie würde die Behandlung eines bösartigen Krebstumors aussehen, wenn in den letzten 20 Jahren akribisch und weltweit jede Behandlung und jede Reaktion des Patienten auf Eingriffe, Medikamente und Verfahren digital dokumentiert worden wäre? Eine solche Datenbank ließe es zu, dass für jeden Pateinten eine immer genauere individuelle Behandlung möglich gemacht werden könnte. Aus der Schnittmenge des Weltwissens der Medizin und den individuellen Symptomen und Anamnesedaten des jeweiligen Patienten ließe sich eine viel effizientere Therapie ermöglichen.

Einige weitere Beispiele sollen das Potenzial einer umfangreicheren Datennutzung offenlegen.

„Risiken und Nebenwirkungen“

Studienauswertungen zu den Ursachen von Krankenhausaufenthalten ermittelten einen Anteil von 7 % schwerer Arzneimittelnebenwirkungen als Einweisungsgrund oder Ursache längerer stationärer Aufenthalte[1]. Bei älteren Menschen lag der Anteil unerwünschter Arzneimittelwirkungen als Grund für eine stationäre Aufnahme sogar bei 10 Prozent[2].

Durch den Einsatz von elektronischen Dateninformationssystemen zur Erfassung der Arzneimittelinformationen anstatt von handschriftlicher Dokumentation kann in einem höheren Maß auf die Arzneimittelinteraktion Rücksicht genommen und mit wenig Aufwand dem Arzt und Apotheker mögliche Neben- und Wechselwirkungen angezeigt werden. So wird nicht nur die Arbeit des Arztes erleichtert, sondern auch die Sicherheit der Patienten verbessert und die Belastung der Krankenhäuser reduziert. In einer dazu durchgeführten Studie konnte die Zahl von Interaktionen von 66 % auf 54 % sowie von unerwünschten Ereignissen von 44 % auf 25 % gesenkt werden[3].

---

[1] https://www.aerzteblatt.de/archiv/160376/Arzneimittelinteraktionen-Prinzipien-Beispiele-und-klinische-Folgen

[2] Davies EC, Green CF, Taylor S, Williamson PR, Mottram DR, Pirmohamed M: Adverse drug reactions in hospital in-patients: a prospective analysis of 3695 patient-episodes. PLoS One 2009; 4: e4439.

[3] Bertsche T, Pfaff J, Schiller P, et al.: Prevention of adverse drug reactions in intensive care patients by personal intervention based on an electronic clinical decision support system. Intensive Care Med 2010; 36: 665–72.

„Digitale Diagnose“
Falsche Diagnosen sind im deutschen Gesundheitswesen an der Tagesordnung. Zum einen ist es für den Arzt schwierig, die richtige Diagnose zu erstellen, wenn er in der Anamnese weitestgehend auf das Wissen über den Patienten angewiesen ist, welches er von diesem in der Sprechstunde erfährt. Zum anderen kann kein Arzt der Welt alle bekannten Krankheiten und entsprechenden Symptome im Kopf speichern. Auch hier kann die bessere Datennutzung und Digitalisierung Abhilfe schaffen. Zunächst muss dem Arzt die gesamte Vita des Patienten zugänglich gemacht werden. Nur dann kann er auf Basis der gesamten Patienten-Vita Entscheidungen treffen. Insoweit war die nun eingeführte elektronische Patientenakte (ePA) ein mehr als überflüssiger Anfang. Zum anderen können computergestützte Diagnose-Tools helfen, die richtigen Entscheidungen zu treffen. Diese können nicht nur ermittelte Symptome und Vitalparameter möglichen Diagnose zuordnen. Auch die automatisierte Auswertung von Röntgenbildern, Aufnahmen von Hautveränderungen usw. kann von gut programmierten Algorithmen deutlich genauer und auf einer unendlich breiten Basis von gespeicherten Vergleichsbildern vorgenommen werden. Die persönliche Erfahrung des Arztes kann im Anschluss immer noch eingebracht werden. Das nützt dem Arzt und vor allem dem Patienten.

All diese Beispiel verdeutlichen, dass umfangreiche Datennutzungen direkten Einfluss auf die Verbesserung der Medizin, wenn nicht gar auf die Rettung von Menschenleben haben können. Welche Rolle kommt in diesem Zusammenhang der Datenschutz zu?

II. Datenschutz und Verhältnismäßigkeit

Zu den fundamentalen Grundrechten jedes Einzelnen zählt das Recht auf Leben und körperliche Unversehrtheit (Art. 2 Abs. 2 GG). Dieses Grundrecht ist – wie im Übrigen jedes Grundrecht – bei allem staatlichen Handeln zu berücksichtigen und in die Abwägungen von möglichen Handlungsalternativen einzubeziehen. Das Grundrecht schützt den Einzelnen vornehmlich vor staatlichen Eingriffen in sein Leben und seine Gesundheit (sog. Abwehrrecht).

Darüber hinaus ist aber anerkannt, dass aus diesem Grundrecht auch eine staatliche Schutzpflicht erwächst. So muss der Staat bei bestimmten Sachverhalten aktiv eingreifen, z.B. durch Gesetze oder Verwaltungsakte, um die Gesundheit der Bürger zu schützen und aktiv auf die Verbesserung der Gesundheit hinzuwirken. Ein Beispiel dafür ist das Nachtflugverbot, welches vor krankmachendem Fluglärm schützen soll und dabei aber die Fluglinienbetreiber in ihrer wirtschaftlichen Entfaltungsmöglichkeit eingrenzt. Ebenso ist das Rauchverbot zu nennen, welches alle Besucher vor den Risiken des Passivrauchens schützt, dabei aber ebenso in die Freiheiten der Raucher und Restaurantbetreiber eingreift.

Letztlich waren auch die sog. Corona-Einschränkungen Maßnahmen des Staates zum Gesundheits-Schutz der Bevölkerung beziehungsweise einem funktionsfähigem Gesundheitssystem. So wurde die Maskenpflicht in öffentlichen Räumen und Verkehrsmitteln als verhältnismäßige Freiheitseinschränkung beschlossen, genauso wie Ausgangssperren, Schließungen von öffentlichen und privaten Geschäften und Einrichtungen und so weiter. Solche Maßnahmen müssen einer umfangreichen Abwägung von Eingriff und Nutzen getroffen werden. Kein Grundrecht – mit Ausnahme der Menschenwürde aus Art. 1 GG – genießt dabei aus Sicht der Verfassung einen absoluten Schutz. Jedes Grundrecht ist also einschränkbar.

Auch der Schutz persönlicher Daten ist grundrechtlich verankert. Im Volkszählungsurteil des Bundesverfassungsgerichts von 1983 wurde das Recht des Bürgers gegenüber dem Staat auf informationelle Selbstbestimmung hervorgehoben. Anlass hierzu war die Entwicklung der elektronischen Datenverarbeitung. Das Bundesverfassungsgericht urteilte: „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Artikel 2 Abs. 1 in Verbindung mit Artikel l Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“[4]

Das Recht auf informationelle Selbstbestimmung schützt den Einzelnen also vor Eingriffen in seine Privatsphäre durch nicht notwendige, willkürlich oder unverhältnismäßige Erhebung, Verarbeitung und Nutzung von Daten. Das klingt erst einmal nach einem absoluten Datenschutz. Vor dem Hintergrund rechtsstaatlicher Grundsätze lassen sich diese Maßgaben aber auf alle Grundrechte übertragen. Selbstverständlich schützt das Grundrecht auf Versammlungsfreiheit (Art. 8 GG) vor nicht notwendigen, willkürlichen oder unverhältnismäßigen Versammlungsverboten, das Grundrecht auf Berufsfreiheit vor nicht notwendigen, willkürlichen oder unverhältnismäßigen Ladenschließungen usw.

Man gewinnt allerdings zu oft den Eindruck, der Datenschutz wird in Deutschland als ein höher und heilig gehaltenes Grundrecht für unantastbar erklärt. Einen absoluten Datenschutz gibt es aber nicht. Der Datenschutz ist einschränkbar, was im Rahmen einer Abwägung mit anderen Grundrechten geschehen darf und manchmal auch geschehen muss. Es sind immer Situationen denkbar, in denen andere Rechte vor dem individuellen Datenschutz Vorrang genießen oder die Datenverarbeitung notwendig ist, um den Staat überhaupt zu organisieren. Komplette Anonymität ist in Bezug auf die hoheitliche Organisation von Steuern, Verwaltung und Gesundheitssystem schlicht undenkbar.

Auch die EU-Datenschutzgrundverordnung (DSGVO) kann und will keinen absoluten Datenschutz etablieren. Sie stellt zwar verschiedene Grundsätze der Datenverarbeitung klar. So sollen immer nur die im Einzelfall notwendige Daten gespeichert und verarbeitet werden („Datenminimierung“) und jede Verarbeitung muss rechtmäßig sein, nach Treu und Glauben erfolgen und transparent gemacht werden (vgl. Erwägungsgrund 39 DSGVO). Datenschutz ist also eines von vielen Rechten bzw. eine Rechtsposition, die es im Einzelfall mit anderen Rechten und Rechtspositionen abzustimmen gilt. Auch der Datenschutz kann also zurückstehen müssen. Gerade im Bereich der Gesundheit kann es wichtiger und damit auch rechtmäßig sein, die Verbesserung des Gesundheitssystems und der Medizin zu fördern, als Daten um jeden Preis zu schützen. Wie gezeigt, gibt es sogar die staatliche Pflicht, den Schutz der Gesundheit aktiv durch Regulationen zu fördern.

In diesem Sinne hält auch die DSGVO ausdrückliche Bestimmungen vor. Gesundheitsdaten können beispielsweise auch dann und im Zweifel ohne Einwilligung des Betroffenen verarbeitet werden, wenn dies aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, erforderlich ist. Jegliche Verarbeitungen und die entsprechenden Gesetze der Mitgliedstaaten müssen dann angemessen sein und spezifisch diese Datenverarbeitung benennen und ermöglichen.

Der Datenschutz bzw. das Recht auf informationelle Selbstbestimmung muss von staatlicher Seite und Behörden also als das gesehen werden, was es ist: ein Grundrecht von vielen, das im Rahmen einer

[4] BVerfGE 65, 1.

sachlichen und verhältnismäßigen Abwägung berücksichtigt werden muss und nicht als heiliger Gral auf eine höhere Stufe gestellt werden, die bei nüchterner Betrachtung nicht begründet werden kann.

Die Behörden für den Datenschutz sind meist die „Datenschutzbeauftragten“. Diese bringen sich gerne als unnachgiebige Wächter eines für heilig erklärten Datenschutzes und Hüter eines vermeintlichen Rechts auf vollständige Anonymität und Verbotes jeglicher Datenverarbeitung in den Diskurs ein und verletzen mit dieser einseitigen Position die rechtstaatliche Pflicht, den Datenschutz im Rahmen einer Abwägung auch mit Blick auf die Chancen und den Nutzen einer Datenverarbeitung zu bewerten.

Das ist zumindest dann kritisch zu sehen, wenn im Rahmen einer Verhältnismäßigkeits-Abwägung eine falsche Gewichtung vorgenommen wird.

„Datenschutz und Verhältnismäßigkeit“ (1)
In einem Interview ganz zu Beginn der Corona-Epidemie gibt die Landesdatenschutzbeauftragte Schleswig-Holstein Frau Marit Hansen auf die Frage: „Welche konkreten Gefahren sehen Sie, wenn wir Datenschutzstandards in einer Krise, wie wir sie aktuell erleben, absenken?“ folgende Antwort:

„Akute Probleme entstehen jetzt schon, wenn gesammelte Daten nicht gegen die unbefugte Nutzung geschützt sind. Das betrifft schon Daten in ausliegenden Listen in Restaurants, aber erst recht Gesundheitsdaten. Man muss sich bewusstmachen, dass es um Leben und Tod gehen kann, wenn Daten manipuliert oder fragwürdig ausgewertet werden. Das Szenario, dass anhand von Daten entschieden wird, wer später ein Beatmungsgerät erhält und wer nicht, ist nicht fernliegend.“[5]

Auch wenn sich Frau Hansen zu Beginn des Interviews deutlich positiver im Sinne einer Datenverwendung zur umfangreichen Pandemiebekämpfung äußert, ist es doch die hier zitierte Passage, welche im Gedächtnis bleibt und beinahe sinnbildlich für das angesprochene Aufgabenverständnis eines behördlichen Datenschutzauftrages steht. Hier wird in Windeseile die Nutzung von persönlichen Daten zum Restaurantbesuch mit einer Manipulation von Gesundheitsdaten in heimtückischer Mordabsicht verwoben. Wie soll denn nun eine sachliche Diskussion zur verhältnismäßigen, sinnvollen und sicheren Nutzung von Gesundheitsdaten mit der behördlichen Datenschutzbeauftragten Frau Hansen geführt werden, wenn diese Geschütze aufgefahren werden? Eine sachliche Diskussion über die Risiken und den Nutzen einer sinnvollen Datennutzug wird durch solche – im wahrsten Sinne des Wortes – Totschlagsargumente im Keim erstickt.

„Datenschutz und Verhältnismäßigkeit“ (2)
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Professor Ulrich Kelber äußerte sich im Sommer 2020 zum Start der Corona-Warn-App (CWA) unter anderem wie folgt: „Aus Sicht des Datenschutzes sehe ich keinen Grund, der gegen eine Installation spricht“. Im Weiteren sprach er dann aber eine als Warnung gemeinte Botschaft aus: „Es ist in keinem Fall zulässig, dass Dritte Einblick in die App fordern. Ich kann die Inhaber von Geschäften oder öffentlichen Verkehrsmitteln nur dringend warnen: Versucht es erst gar nicht!“[6].

[5] https://www.forschung-it-sicherheit-kommunikationssysteme.de/service/aktuelles/interview-datenschutzgrundsaetze

[6] https://www.datenschutz-praxis.de/verarbeitungstaetigkeiten/datenschutz-bei-der-corona-warn-app-die-wichtigsten-fakten/

Diese Aussage ist in zweierlei Hinsicht bemerkenswert. Zum einen steckt ein stark bevormundendes Element in der Warnung. Denn warum sollten Geschäftsbetreiber nicht Einblick in die App fordern dürfen? Der Inhaber eines Ladengeschäftes beispielsweise ist grundsätzlich für die Verkehrssicherheit in seinen Räumen verantwortlich. In Zeiten einer Pandemie gibt es die Möglichkeit, ein Geschäft gar nicht zu öffnen, oder aber so zu öffnen, dass die Sicherheit der Kundschaft grundsätzlich gewährleistet ist. Wenn es nun eine App geben würde, die zuverlässig vor Risikokontakten warnen könnte, wäre es aus Sicht des Geschäftsbetreibers sogar eine Pflicht, den Einblick in diese App zu fordern, um Risikopersonen von dem Zutritt auszuschließen. Die CWA und die gesammelten Daten würden also einer nachvollziehbaren und sinnvollen Nutzung zugeführt. Nichts anderes wird derzeit gemacht mit Pflichtnachweisen zu den „ggg" (getestet, genesen, geimpft). Die allermeisten Menschen wollen nicht an Covid erkranken und auch keine anderen Personen anstecken. Die Möglichkeit, sich testen zu lassen, wird daher gerne in Anspruch genommen. Der Nachweis, dass dann ein sehr geringes Ansteckungsrisiko von einem ausgeht, gerne erbracht. Die Forderung, einen entsprechenden Nachweis zu erbringen, bevor z.B. größere Veranstaltungen besucht werden, ist gesellschaftlich sozialadäquat. Wie kann dann eine solche behördliche „Warnung" hilfreich sein und bestehen?
Daneben zeigt der Ansatz von Herrn Kelber die bereits zuvor kritisierte falsch verstandene kompromisslose Schutzmentalität bezüglich der Daten, die sich nicht in die ansonsten etablierte rechtliche Ordnung aus Abwägung und Verhältnismäßigkeit einreiht. Überspitzt gefragt: Soll ein Geschäft schließen, bevor es bestimmte Gesundheitsdaten seiner Besucher fordert?

Am Beispiel der Corona-Warn-App werden die praktischen Folgen einer Fehlgewichtung von Datenschutz zu anderen Grundrechten ebenso deutlich. Die Idee, unsere ohnehin allgegenwärtig genutzten Smartphones über eine passende App für die Pandemie-Bekämpfung technisch einzusetzen, war grundsätzlich richtig. Möglich gewesen wären automatisierte Benachrichtigungen über Kontakte mit Infektionen, die Identifizierung von Hot Spots und andere hilfreiche Module. Im Zuge der Entwicklung der CWA wurde immer wieder der Datenschutz als zentraler Baustein betont, was grundsätzlich nachvollziehbar ist. Letztlich führte dies dann zu der Entwicklung einer App, welche Daten dezentral auf den Geräten verarbeitet. Dieser Ansatz ist zwar höchst datensicher, verhindert aber eine umfangreiche Vernetzung und den Austausch von Kontaktdaten über einen zentralen Speicherort. So können Infektionsdaten nur dann weitergegeben werden, wenn sich zwei aktivierte Smartphones auch tatsächlich begegneten. Damit wurde das Potential einer wirklich umfangreichen und überregionalen Warn-Möglichkeit dem Datenschutz geopfert. Der Programm-Code wurde indes im Rahmen des „Open Source"-Modells veröffentlicht. Am Ende stand dann eine so datenschutzsichere App, an dem nicht einmal die Hacker vom Chaos Computer Club etwas auszusetzen hatten. So sicher wie CWA dann war, so nutzlos war sie allerdings auch. Laut einem Interview aus dem Sommer 2020 mit Frau Ute Teichert, der Vorsitzenden des Bundesverbandes der Ärztinnen und Ärzte des Öffentlichen Gesundheitsdienstes, spielte die CWA zum damaligen Zeitpunkt praktisch keine Rolle in der täglichen Arbeit der Gesundheitsämter. So haben die Politik entschieden, den Datenschutz über den Pandemieschutz zu stellen, was man akzeptieren müsse. Hilfreich wäre es laut Teichert, wenn die App eine Funktion haben würde, mit der die Anwender eine direkte Weitergabe von Warnhinweisen an das Gesundheitsamt zumindest freiwillig zulassen könnten. Damit würden die zuständigen Behörden wesentlich schneller über Infektionsfälle informiert und könnten zügig Maßnahmen ergreifen, um einen Corona-Ausbruch einzudämmen[7].

Man gewinnt den Eindruck, Politik und Gesellschaft gehen lieber anonym und datengeschützt in den monatelangen Lockdown, als sich mit einer technischen Lösung zu befassen, die auf Grundlage einer sicheren, aber weitergehenden Datenauswertung eine bessere Bewältigung der Pandemie mit

[7] https://www.tagesschau.de/inland/corona-warnapp-gesundheitsamt-kritik-101.html

möglicherweisen weniger Toten und einem kürzeren Lockdown ermöglicht hätte. Dafür wäre es nötig gewesen, die Nutzung von persönlichen Daten zu akzeptieren. Angesichts der schwersten Folgen der Pandemie sollte doch eine partielle Verringerung des Datenschutzes weniger riskant und schwerwiegend sein als ein langer Lockdown und die unbeobachtete Entwicklung von Ansteckungsketten einer todbringenden Krankheit?

Doch noch nicht einmal eine freiwillige Möglichkeit zur besseren Datennutzung der CWA wurde geboten. Zum Schutze der Bevölkerung wurden Gottesdienste und Versammlungen verboten oder stark eingeschränkt, Restaurants und Bars über Monate geschlossen, Ausgangssperren verhängt und Risikogruppen praktisch isoliert. Solche Maßnahmen müssen gut überlegt sein und sind mit Blick auf die betroffenen Grundrechte nur sehr schwer zu begründen und aufrecht zu erhalten. Es gab aber im Digitalen nicht einmal die Chance für die Bürgerinnen und Bürger, eine freiwillige und offene Kontaktverfolgung einzuschalten und eine weitgehende Automatisierung dieser Prozesse in Gang zu bringen. Noch einmal: der Staat und seine Behörden sind dazu verpflichtet, das Leben der Bevölkerung zu schützen. Das Leben als Grundrecht kann denklogisch nur einen höheren Stellenwert haben als die informationelle Selbstbestimmung. Denn Toten nützt der Datenschutz sicher gar nichts. Der Datenschutz geschieht damit auf Basis einer Bevormundung der Bevölkerung und unter Missachtung staatlicher Schutzpflichten.

III. Recht auf Daten

Die Nutzung von Daten zur Verbesserung der Medizin und der Behandlung soll niemandem eine Gesundheit aufdrängen, die er oder sie nicht möchte. Es geht vielmehr darum, all jenen eine Gesundheit zu ermöglichen, die krank oder durch eine Krankheit vom Leben bedroht sind und durch bessere Medizin geheilt oder gar gerettet werden können und wollen. In diese Situation kann jeder kommen.

Die staatlichen Schutzpflichten und die Chancen einer umfangreichen Datennutzung für Medizin und Gesundheit bedingen einen Anspruch auf staatliche Etablierung einer umfangreichen und sinnvollen Datennutzung. Denkt man sich den Datenschutzbeauftragten einmal als „Datennutzungsbeauftragten“ oder einfach als „Datenbeauftragten“ wird die eigentliche Funktion dieser Behörde schon begrifflich klarer. Dies kann helfen, einem übereifrigen, sinnlosen oder gar rechtswidrig unverhältnismäßigen Datenschutz vorzubeugen und den Fokus wegzulenken von einem vermeintlich bedingungslos zu gewährenden Anspruch auf Anonymität. Eine bessere Datennutzung kann dann möglich sein, ohne den wirklichen Kerngedanken des Datenschutzes zu verletzen: den Schutz vor ungesetzlicher staatlicher Ausforschung und vor wirklich schädigenden Verletzungen des Persönlichkeitsrechts.

Jeder Bürger hat das Recht darauf, dass die Behandlung der Ressource „Daten“ mit dem Ziel erfolgt, sie mit ihrem maximalen Nutzungspotenzial einzubringen und in der laufenden staatlichen Regulation und Verwaltung deren optimale Nutzung zu gewährleisten.