

Medizin und Digitalisierung (E-Health)

Eric Hilgendorf

Eine neue Herausforderung für das Technikrecht

Mit dem Jubilar **Christian Schwarzenegger** verbindet mich nicht nur eine jahrzehntelange Freundschaft, sondern auch ein gemeinsames Interesse für das Technikrecht. Dabei geht es insbesondere um das Informations- und Telekommunikationsrecht in seinen vielfältigen und sich immer mehr erweiternden Anwendungsbereichen einerseits, und das kaum weniger innovationsgetriebene Medizin(straf)recht andererseits. Die nachfolgenden, zugegebenermaßen noch durchaus skizzenhaften Ausführungen verstehe ich als Einladung, unsere Kooperation um ein weiteres Zukunftsfeld zu erweitern – die Digitalisierung der Medizin.¹

¹ Im Folgenden orientiere ich mich exemplarisch an der Situation Deutschland. Über die aktuelle Lage der Digitalisierung der Medizin in der Schweiz berichtet die Strategie eHealth Schweiz 2.0, 2018 – 2022, vom 14. Dezember 2018, im Internet unter https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2018/D/181214_Strategie-eHealth-Suisse-2.0_d.pdf.

I. Einführung

Die Digitalisierung der Medizin schreitet rasch voran.² Im Juni 2019 legte die deutsche Bundesregierung den Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation, das sogenannte **Digitale-Versorgung-Gesetz** (DVG), vor.³ Ziel des Gesetzes ist es, die Digitalisierung im deutschen Gesund-

² Literaturauswahl: **Böttiger/zu Putlitz** (Hrsg.), Die Zukunft der Medizin. Disruptive Innovationen revolutionieren Medizin und Gesundheit, Berlin 2019; **Bogdan**, MedRevolution. Neue Technologien am Puls der Patienten, Berlin 2018; **von Grätz** (Hrsg.), Vernetzte Medizin. Patientenempowerment und Netzinfrastrukturen in der Medizin des 21. Jahrhunderts, Hannover 2004; **Haring** (Hrsg.), Gesundheit digital. Perspektiven zur Digitalisierung im Gesundheitswesen, Berlin 2019; **Huss**, Künstliche Intelligenz, Robotik und Big Data in der Medizin, Berlin 2019; **Jörg**, Digitalisierung in der Medizin. Wie Gesundheits-Apps, Telemedizin, künstliche Intelligenz und Robotik das Gesundheitswesen revolutionieren, Berlin 2018; **Matusiewicz/Pittelkau/Elmer** (Hrsg.), Die Digitale Transformation im Gesundheitswesen. Transformation, Innovation, Disruption, Berlin 2017; **Müller-Mielitz/Lux** (Hrsg.), E-Health-Ökonomie, Berlin 2017; **Schulz**, Zukunftsmedizin. Wie das Silicon Valley Krankheiten besiegen und unser Leben verlängern will, München 2018; **Topol**, Deep Medicine. How Artificial Intelligence Can Make Healthcare Human Again, New York 2019; **Trill** (Hrsg.), Praxisbuch eHealth. Von der Idee zur Umsetzung, 2. Aufl., Stuttgart 2018; **Wachter**, The Digital Doctor. Hope, Hype and Harm at the Dawn of Medicine's Computer-Age, New York 2017.

³ https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/D/Digitale-Versorgung-Gesetz_DVG_Kabinett.pdf.

heitswesen voranzutreiben⁴ und rechtliche Rahmenbedingungen zu schaffen, die eine rasche «Implementierung digitaler Lösungen und neuer innovativer Formen der Zusammenarbeit» ermöglichen.⁵ Mit der Digitalisierung des Gesundheitswesens soll «den Herausforderungen der alternden Gesellschaft, der Zunahme der Anzahl chronisch Kranker, dem Fachkräftemangel sowie der Unterversorgung in strukturschwachen Regionen» entgegengetreten werden.⁶ Der Gesetzgeber macht deutlich, dass der Gesetzentwurf lediglich einen Schritt in einer langen Reihe von Aktivitäten darstellt, die die Digitalisierung des Gesundheitswesens durchsetzen sollen. Dabei sei ein «stetes Ausbalancieren im Spannungsfeld zwischen der gesellschaftlichen Verantwortung, dem Nutzen für die Versorgung und dem Machbaren» erforderlich.⁷

Der Entwurf sieht insbesondere vor, digitale Gesundheitsanwendungen, d.h. vor allem sogenannte Gesundheitsapps, den Patienten zur Verfügung zu stellen. Versicherte sollen einen Anspruch auf digitale Gesundheitsanwendungen erhalten. Die erforderliche Sichtung des Angebots und die Auswahl der verschreibungspflichtigen Anwendungen soll durch das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) erfolgen. Des Weiteren zielt der Gesetzentwurf darauf ab, mehr Leistungserbringer als bisher an die bereits existierende Telematik-Infrastruktur im Gesundheitswesen⁸ anzuschließen. Außerdem soll die Telemedizin gestärkt werden, etwa durch die Ausweitung von sogenannten Telekonzilien⁹ und eine Vereinfachung der Durchführung von Videosprech-

stunden. Darüber hinaus sollen die Verwaltungsprozesse durch Digitalisierung vereinfacht werden.

Den Krankenkassen sollen mehr Möglichkeiten zur Förderung digitaler Innovationen gegeben werden. Der Innovationsfonds des Bundes soll mit 200 Millionen Euro pro Jahr fortgeführt und weiterentwickelt werden und es soll ein Verfahren zur Überführung erfolgreicher Ansätze aus Projekten des Innovationsfonds in die Regelversorgung geschaffen werden. Ein weiteres Ziel ist eine bessere Nutzbarkeit von Gesundheitsdaten für Forschungszwecke. Insgesamt handelt es sich um eine durchaus ehrgeizige, ein weites Spektrum von Maßnahmen umfassende Initiative, um die Digitalisierung der Medizin in der Bundesrepublik Deutschland wirksam voranzutreiben.

Die Medizin ist offenkundig im Zeitalter der Computer, des Internets und der Künstlichen Intelligenz angekommen. Dies bedeutet aber auch, dass sich das Gesundheitswesen zu einem neuen Anwendungsfeld der **Computer- und Internetkriminalität** entwickeln wird. Der Gesetzgeber sieht durchaus die Gefahren, die eine Vernetzung und Digitalisierung im Gesundheitswesen mit sich bringt. Deswegen werden im neuen § 75b des SGB V die kassenärztlichen Bundesvereinigungen verpflichtet, bis zum 31. März 2020 in einer Richtlinie die Anforderungen «zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung» festzulegen. In Abs. 2 heißt es, die in der Richtlinie festzulegenden Anforderungen müssten «geeignet sein, abgestuft im Verhältnis zum Gefährdungspotenzial, Störungen der informationstechnischen Systeme, Komponenten oder Prozesse der vertragsärztlichen Leistungserbringung in Bezug auf Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu vermeiden.»¹⁰

⁴ Siehe in diesem Zusammenhang auch schon das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health Gesetz) vom 21.12.2015, BGBl I, 2408 ff.

⁵ DVG-Entwurf (Fn. 3), 1.

⁶ Ebenda.

⁷ Ebenda.

⁸ Siehe dazu die aktuelle Broschüre der Kassenärztlichen Bundesvereinigung, im Internet unter https://www.kbv.de/media/sp/PraxisWissen_Telematikinfrastruktur.pdf.

⁹ Unter «Telekonzil» (gelegentlich auch «Telekonsil») wird die zeitversetzte Beratung mit einem oder mehreren anderen Ärzten mittels elektronischen Austauschs verstanden.

¹⁰ DVG-Entwurf (Fn. 3), 10.

II. Was ist E-Health?

A. Begriff

«E-Health» ist die Abkürzung für «Electronic Health». Unter diesem Oberbegriff werden alle Vorgänge im Gesundheitswesen erfasst, bei denen der Patient oder die Patientin unter Einbeziehung digitaler Informations- und Kommunikationstechnologien (IKT) behandelt oder betreut wird.¹¹ Der Begriff bezeichnete zunächst nur die Digitalisierung klassischer Tätigkeitsbereiche, etwa das Führen **digitaler Patientenakten**. Die Fortentwicklung der Informations- und Kommunikationstechnologie ermöglicht jedoch heute eine Vielzahl von Anwendungen im Gesundheitsbereich, die ebenfalls unter dem Oberbegriff E-Health zusammengefasst werden.

Das Thema E-Health liegt im Schnittpunkt verschiedener Disziplinen, etwa der Medizin, der Rechtswissenschaft, der Gesundheitsökonomie, aber auch der Medizinethik. Technische Grundlage von E-Health jeder Art ist die Digitalisierung medizinischer Informationen, also die Darstellung in binärer Form als Folge von «Nullen» und «Einsen».¹² Dies erlaubt es, beliebige Informationen in vorher nie gekannter Geschwindigkeit und Menge zu speichern, zu übertragen und zu bearbeiten. Dabei lassen sich Datenspeicher heute auch über weite Entfernungen hinweg so vernetzen, dass der Datenaustausch zwischen ihnen quasi in Echtzeit möglich ist. Dies ist die Grundlage des **Internets der Dinge** (Internet of Things, IoT), also der Vernetzung von beliebigen Gegenständen, so dass diese selbständig über das Internet miteinander kommunizieren können.¹³

Ein neuer, erst in den letzten Jahren im Medizinsektor in breiterem Umfang relevant werdender Faktor ist das zunehmende Auftreten autonomer Systeme, die eigenständig Informationen aufnehmen, sie austauschen und Ent-

scheidungen treffen können. Es handelt sich um eine neue Form von Akteuren, deren theoretische Erfassung Ethik und Rechtswissenschaft vor erhebliche Herausforderungen stellt.¹⁴ Derartige Systeme übernehmen auch im medizinischen Bereich immer mehr Entscheidungen, ohne dass bislang z.B. die Verteilung von Verantwortung für Fehlentscheidungen als geklärt gelten kann. Auch wenn Systeme mit Künstlicher Intelligenz dem menschlichen Arzt bereits heute z.B. bei der Bilderkennung weit überlegen sind,¹⁵ dürfte es noch eine Zeit lang dauern, bis Computer eigenständig umfassende ärztliche Aufgaben übernehmen können.¹⁶

B. Formen des E-Health

Die verschiedenen Anwendungsbereiche des E-Health lassen sich in folgende Gruppen aufteilen: Information, Kommunikation, Interaktion, Transaktion und Integration.¹⁷

- **Information:** Darunter fallen z.B. spezielle Informationsportale, mit denen Ärzten oder Patienten Informationen vermittelt werden. Ein Sonderfall sind Krankenhausinformationssysteme (KIS), also alle IKT-Systeme innerhalb eines Krankenhauses, die Informationen und Daten innerhalb eines Krankenhauses erfassen, bearbeiten, speichern und nutzbar machen.
- **Kommunikation:** In diese Kategorie fallen Systeme, welche den Austausch von Informationen zwischen zwei oder mehr Beteiligten, also zwischen Arzt - Patient, Arzt - Arzt, Patient - Patient usw. ermöglichen, bei denen aber keine direkte oder zeitnahe Reaktion des Kommunikationspartners erfolgt.
- **Interaktion:** Mit Interaktion wird der Austausch von Informationen und Daten bezeichnet, wobei eine direkte Reaktion des

¹¹ Umfassend Lux, in: Müller-Mielitz/Lux (Fn. 2), 3 ff.

¹² Einführend zu den technischen Grundlagen und Trends Hilgendorf, Digitalisierung in der Medizin, medstra 2017, 257 f.

¹³ Bogdan (Fn. 2), 63 ff.

¹⁴ Hilgendorf, Autonome Systeme, künstliche Intelligenz und Roboter, in: Barton et al. (Hrsg.), Festschrift für Thomas Fischer, München 2018, 101 ff.

¹⁵ Wachter (Fn. 2), 47 ff.

¹⁶ Topol (Fn. 2), insbes. 255 ff.; 283 ff.; Wachter (Fn. 2), 93 ff.

¹⁷ <https://www.egovernment-computing.de/was-ist-ehealth-a-570980/>.

Kommunikationspartners erfolgt. Als Beispiel kann das «Home-Monitoring» von Patienten dienen.

- **Transaktion:** Zu dieser Form von E-Health zählen Anwendungen, die den gezielten Datenaustausch zwischen verschiedenen Beteiligten zum Inhalt haben und damit die elektronische Abbildung und Abwicklung aller erbrachten medizinischen Leistungen ermöglichen. Ein Beispiel ist die Elektronische Gesundheitskarte.¹⁸
- **Integration:** Zur Integration gehören alle Anwendungen, die auf die lebenslange zentrale Speicherung von Patientendaten abzielen, indem alle Gesundheitsdaten eines Patienten zusammengeführt werden. Dazu gehört etwa die Elektronische Patientenakte.¹⁹

Eine andere Einteilung²⁰ unterscheidet nach dem **Zweck der Nutzung** zwischen E-Health-Angeboten der Konsumentenebene, der professionellen Ebene und der Makroebene. Zur **Konsumentenebene** gehören alle Angebote des kommerziellen Gesundheitsmarktes, wie z.B. Gesundheitsapps, Mess- und Assistenzsysteme oder digitale Fitnesstools. Die **professionelle Ebene** erstreckt sich auf Anwendungen, die von Angehörigen des Gesundheitswesens (Ärzten, Krankenkassen) finanziert werden, also vor allem die Angebote der Telemedizin. Die **Makroebene** betrifft diejenigen Angebote, für die eine Vernetzung verschiedener Akteure erforderlich ist. Hierzu gehören die bereits erwähnte Elektronische Gesundheitskarte und die Elektronische Patientenakte.

C. Telemedizin

«Telemedizin» bezeichnet medizinische Diagnostik oder Therapie, die unter Überbrückung einer räumlichen oder zeitlichen Distanz zwischen dem Arzt/Therapeut/Apotheker und dem Patienten mit den Mitteln der Telekom-

munikation erfolgt.²¹ Eingesetzt wird die Telemedizin bereits seit den 1980er Jahren, wo sie zunächst die räumliche Entfernung zwischen Arzt und Patient bei militärischen Einsätzen oder in der Raumfahrt überbrücken sollte.²² Von großer Bedeutung ist die Telemedizin in Ländern mit einer geringen Bevölkerungsdichte, wo relativ wenige Menschen über eine große Fläche medizinisch versorgt werden müssen. Heute ist die Telemedizin auch in Deutschland weit verbreitet und erfasst nahezu alle medizinischen Fachgebiete.²³

Viele Telemedizin-Projekte werden in Deutschland staatlich unterstützt. Zur Bündelung des telemedizinischen Wissens wurden beispielsweise in Bayern mehrere telemedizinische Zentren gegründet, welche die Entwicklung neuer Projekte fördern. Ziel ist, dass die Telemedizin sowohl von Seiten der Heilberufe als auch von Seiten der Patienten zum selbstverständlichen Bestandteil der medizinischen Versorgung wird (sog. Telemedizin-Offensive Bayerns).²⁴

Ein anderes Beispiel für Telemedizin sind die in mehreren Bundesländern eingeführten «Tele-Stroke-Units», mit denen Schlaganfallpatienten behandelt werden.²⁵ Eine «Stroke-Unit» ist eine zertifizierte Spezialabteilung für die Behandlung eines Schlaganfalls. Doch nicht jedes Krankenhaus in Deutschland verfügt über eine solche Abteilung. Zur Verbesserung der Versorgung insbesondere im ländlichen Raum wurden deshalb neue «Tele-Stroke-Units» gegründet. Dabei erfolgt die medizinische Versorgung des Patienten in der Klinik vor Ort;

¹⁸ <https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/egk.html>. Siehe auch Trill, in: ders. (Fn. 2), 48 ff.

¹⁹ <https://www.kbv.de/html/epa.php>.

²⁰ <https://ehealthblog.de/ehealth/>.

²¹ Bogdan (Fn. 2), 185 ff.; Jörg (Fn. 2), 65 ff.

²² Bogdan (Fn. 2), 187 f. zu noch älteren Anwendungsszenarien.

²³ <http://www.bundesaerztekammer.de/aerzte/telematiktelemedizin/telemedizin/>.

²⁴ <https://www.stmgp.bayern.de/meine-themen/fuer-krankenhausbetreiber/telemedizin/>.

²⁵ <https://www.netdokter.de/krankheiten/schlaganfall/stroke-unit/>.

die Spezialisten werden über eine Live-Video-Konferenz zugeschaltet.²⁶

Ein weiteres Beispiel ist der von mehreren Krankenkassen angebotene Chat mit einem Arzt. In dem Modellprojekt «DocDirekt» der KV Baden-Württemberg²⁷ können sich Patienten telefonisch, per App oder im Chat an einen Telearzt, meist einen Allgemeinmediziner, wenden und sich von ihm beraten lassen. Diese verweisen die Patienten bei Bedarf an eine patientennah erreichbare Praxis, bei der der Patient noch am selben Tag einen Termin erhält. Auf diese Weise soll u.a. die Überlastung der Notfallambulanzen verringert werden. Der beteiligte Arzt erhält für jeden Anruf eine Vergütung von 25 Euro.

Ein Unterfall der Telemedizin ist das **Telemonitoring**, also die Fernüberwachung von Patientinnen und Patienten.²⁸ Gängige Praxis ist z.B. die Kontrolle von Herzschrittmachern, die automatisch Vitalparameter (z.B. Herzrhythmus, Sauerstoffgehalt des Blutes) an ein Datencenter übersenden. Diese Daten werden durch Ärzte bzw. geschultes Personal überwacht und ausgewertet. Bei einer Gesundheitsverschlechterung kann der Patient so frühzeitig gewarnt und behandelt werden.

Die Telemedizin ermöglicht auch **neue Geschäftsmodelle** für Ärzte: Für Patienten, die einen Herzinfarkt erlitten haben, bietet beispielsweise ein Hamburger Arzt eine spezielle App an²⁹ und mehrere Kardiologen betreiben den Bereitschaftsdienst CARDIOGO³⁰. Gegen Bezahlung wird dabei den Patienten ein mobiles EKG-Gerät zur Verfügung gestellt und der Patient erhält (ggf. gegen eine zusätzliche Ge-

bühr) die Möglichkeit, jederzeit durch einen Kardiologen telefonisch beraten zu werden. CARDIOGO legt eine elektronische Patientenakte an, auf die die beteiligten Ärzte jederzeit zugreifen können.

D. Mobile Health

Unter dem Begriff des Mobile Health wird derjenige Bereich des E-Health zusammengefasst, in welchem mobile Geräte eingesetzt werden. Insbesondere der Markt für Fitness- und Gesundheitsapps ist in den letzten Jahren rasant gewachsen. Schon heute sind weit über 100.000 Apps verfügbar, die sich mit Gesundheit oder Fitness befassen. Sie werden oft in Verbindung mit einem «Activity-Tracker» eingesetzt, welcher als Armband oder Uhr getragen wird und Aufzeichnungen über die Bewegung (z.B. Anzahl der Schritte), Kalorienverbrauch und Herzfrequenz vornimmt. Sind die Geräte mit einem GPS-Element verbunden, wird auch die zurückgelegte Strecke aufgezeichnet. Über eine zum jeweiligen Fitnesstracker gehörende App lässt sich das Fitnessverhalten des Benutzers auswerten. Die Fitness- und Gesundheitsdaten des Konsumenten werden in einer Cloud gespeichert.

Ein neuer, über den reinen Fitnessaspekt hinausgehender Trend aus den USA ist das **SelfTracking**.³¹ Offenbar verspüren immer mehr Menschen das Bedürfnis, ihre Lebensgewohnheiten zu analysieren, um diese zu optimieren, indem sie die relevanten Daten über einen längeren Zeitraum hinweg sammeln und durch eine App auswerten lassen. Häufig werden die Daten außerdem in sozialen Netzwerken geteilt. Sie beziehen sich zum Beispiel auf die Schlaf- und Essgewohnheiten, den Konsum von Zigaretten und Alkohol, biometrische Fakten wie Puls, Blutdruck und Blutzuckerwerte, aber auch auf «weiche» Fakten wie das momentane Wohlbefinden. Offenbar werden vor allem junge,

²⁶ Zu älteren Projekten dieser Art Kiefer et al., in: von Grätz (Fn. 2), 105 ff.

²⁷ https://www.aerztezeitung.de/praxis_wirtschaft/e-health/telemedizin/article/968458/telemedizin-projekt-docdirekt-oft-geschattet-arzt.html.

²⁸ Jörg (Fn. 2), 9 ff.

²⁹ <https://www.abendblatt.de/hamburg/article226302031/Herzinfarkt-Diagnose-Kardiologie-UKE-Forschung.html>.

³⁰ <https://ehealthblog.de/2015/02/20/cardiogo-eine-app-die-leben-retten-kann/>.

³¹ Hilgendorf, Zur Steuerung technischer Entwicklungen durch Recht und Moral – am Beispiel der Informationstechnik in der Medizin, in: Spiecker gen. Döhmman/Wallrabenstein (Hrsg.), IT-Entwicklungen im Gesundheitswesen, Bern 2016, 75 (76).

technikaffine Männer von diesen Apps angesprochen.³²

Junge Unternehmen nutzen diesen Trend und entwickeln immer mehr Apps, um die besonderen Wünsche ihrer Klientel zu befriedigen. So entwickelten IT-Spezialisten eines Heidelberger Start-Ups einen digitalen Urintest, mit dem durch Messung von Urinwerten (pH-Wert, Glykose) Krankheiten frühzeitig erkannt werden sollen. Das System besteht aus einem Sensor, der in die Toilette eingebaut wird, einer App und einem Serversystem. In der Testphase haben mehrere Heidelberger Gaststätten ihre Toiletten mit einem derartigen Sensor ausgestattet.³³

Weiterhin werden Methoden erarbeitet, die Gesundheitstracker nicht nur als Armband zu tragen, sondern fest mit dem Körper zu verbinden. So entwickelte das US-Startup Chaotic Moon Studios ein Tech-Tattoo, das den menschlichen Körper als Leiterplatte nutzt und Puls, Stresslevel und Körpertemperatur messen kann. Das Wearable wird dabei wie ein Abziehbild auf die Haut aufgetragen. Die Messwerte werden per Bluetooth oder Wifi an den PC oder eine App übertragen und ausgewertet. Interessant sind diese Tech-Tattoos vor allem in der Medizin und im Militär.³⁴ Durch den direkten Hautkontakt sind die Tattoos funktionaler als die bisherigen Smartwatches. Sie sind außerdem auch deutlich günstiger und umweltfreundlicher.

Das Sammeln von Daten, auch und gerade von Gesundheitsdaten, gehört für immer mehr Menschen zum Lebensalltag. In den USA wird in vielen Kliniken die von Apple entwickelte App «Healthkit» genutzt.³⁵ Diese speichert die

Gesundheitsdaten des Anwenders, die über verschiedene Apps gesammelt werden (z.B. Pulssensoren, Personenwaage usw.) und macht sie verfügbar. Es steht zu erwarten, dass Gesundheitsapps in der Medizin immer mehr an Bedeutung gewinnen und in Zukunft sogar genauso wie ein Medikament verordnet werden. Dies würde allerdings voraussetzen, dass der Arzt den Patienten über den Einsatz und die Anwendung sinnvoller Apps beraten kann.³⁶ Wie in der Strategie eHealth Schweiz 2.0³⁷ zu Recht betont wird, müssen überdies auch die Patienten über digitale Grundfertigkeiten sowie über eine hinreichende allgemeine Gesundheitskompetenz verfügen, wenn die Digitalisierung der Medizin gelingen soll.

III. Vorteile und Nachteile

Die Vorteile der neuen Technologien liegen auf der Hand:³⁸ Die medizinische Versorgung wird verbessert, Krankheiten können früher erkannt und durch Vorsorge verhindert werden. Dies führt zu einer erheblichen Einsparung von Kosten, was wiederum für eine Verbesserung der Gesundheitspflege genutzt werden kann. Besondere Chancen bietet die sog. personalisierte Medizin, bei der Diagnostik und Therapie speziell auf das betroffene Individuum zugeschnitten sind – bis zu passend für den einzelnen Empfänger erzeugten Spenderorganen.³⁹ Derartige Angebote setzen die Erfassung und Analyse gewaltiger Datenmengen über das individuelle Krankheitsbild voraus.

Aber wer sammelt die Daten bzw. wer gerät mit ihnen in Kontakt? In Frage kommen die Gesundheitsdienstleister und IT-Provider, aber auch Abrechnungsstellen, Kontroll- und Qualitätssicherungseinrichtungen, Forschungseinrichtungen, soziale Netzwerke bis hin zu Selbsthilfeforen. Es ist kaum zu kontrollieren, wie

³² <https://www.wissen.de/self-tracking-das-vermessene-ich>.

³³ <https://ehealthblog.de/news-trends/e-health-startup-entwickelt-einen-digitalen-urintest/>.

³⁴ <https://www.trendsderzukunft.de/biowearables-neues-tech-tattoo-misst-koerper-und-umweltdaten-und-warnt-vor-unsichtbaren-gefahren/>.

³⁵ https://www.aerztezeitung.de/praxis_wirtschaft/w_specials/gesundheitsapps2011/article/910754/zukunft-e-health-wenn-aerzte-apps-verordnen-pillen.html.

³⁶ https://www.aerztezeitung.de/praxis_wirtschaft/w_specials/gesundheitsapps2011/article/910754/zukunft-e-health-wenn-aerzte-apps-verordnen-pillen.html.

³⁷ Strategie eHealth Schweiz (Fn. 1), 39.

³⁸ Siehe auch die Strategie eHealth Schweiz (Fn. 1), 13 f.

³⁹ Gelegentlich ist auch von einer «precision medicine» die Rede, vgl. etwa Bogdan (Fn. 2), 231 ff.

dort mit den Patientendaten umgegangen wird, vor allem dann, wenn die Anbieter aus dem Ausland agieren. Besonders problematisch ist, wenn Daten in großem Umfang gesammelt und ausgewertet werden können (Big Data). Das Geschäftsprinzip vieler (Gesundheits-)Apps beruht darauf, dass sie für den Nutzer zwar kostenlos oder sehr günstig sind, er aber quasi mit seinen Daten «bezahlt», die dann weitergenutzt oder an Dritte verkauft werden. Schon heute sammeln Dritte Daten und werten diese mit Algorithmen aus, um z.B. auf den Einzelnen zugeschnittene Werbeprojekte zu erstellen oder um ihre Produkte (z.B. Medikamente) zu verbessern. Wie das letztgenannte Beispiel zeigt, sind derartige Geschäftsmodelle keineswegs von vornherein negativ zu bewerten.

Gerade im Gesundheitsbereich droht aber die Herausbildung nicht mehr zu kontrollierender internationaler Monopole;⁴⁰ aus gut nachvollziehbaren Gründen werden sich vor allem schwer oder gar lebensbedrohlich erkrankte Menschen nicht mit dem zweitbesten Anbieter zufrieden geben, sondern unter Inkaufnahme sämtlicher Kosten das (wirklich oder bloß vermeintlich) beste Angebot wählen.

Die Auswertung der besonders sensiblen Gesundheitsdaten ermöglicht einen tiefen Einblick in den persönlichen Lebensbereich. Sie geben Auskunft über Lebenserwartung und allgemeinen Gesundheitszustand, der nicht nur für die Werbebranche, sondern insbesondere für Versicherungen, Kreditunternehmen und (zukünftige) Arbeitgeber äußerst interessant ist. Darüber hinaus lassen sich gerade Gesundheitsdaten nutzen, um das Verhalten nicht bloß zu analysieren, sondern auch zu steuern, vom bloßen «Nudging» bis hin zur handfesten Manipulation,⁴¹ von illegalen Zugriffen auf Datenbestände etwa zum Zweck von Erpressung ganz zu schweigen.

⁴⁰ Schulz (Fn. 2), 92 ff.

⁴¹ Dies gilt für alle Daten, die einen Einblick in die Motive von Akteuren erlauben. Nicht zuletzt deshalb ist die Herausbildung von Datenmonopolen ein außerordentlich wichtiges gesamtgesellschaftliches Thema.

IV. Rechtliche Herausforderungen – ein Ausblick

Diese neuen Entwicklungen bergen erhebliche rechtliche Herausforderungen. Das Spektrum reicht vom Verfassungsrecht über das Medizinprodukterecht, das zivile Haftungsrecht, das Versicherungsrecht, das Recht des Datenschutzes⁴² bis hin zum Strafrecht. Auch die europa- und völkerrechtlichen Vorgaben sind zu beachten.⁴³ Im Folgenden soll nur ein Problemfeld herausgegriffen werden, nämlich die **strafrechtliche Verantwortlichkeit bei Hackerangriffen**:

Gesundheitsdaten sind besonders sensibel und müssen daher in besonderem Maße geschützt werden. Neben dem Hacker, der sich aus finanziellen Interessen in ein System einhackt und die so erlangten Daten verkauft, sind auch andere Szenarien denkbar, etwa mutwillige Veränderungen von Daten mit der Folge von Fehldiagnosen oder die gezielte Manipulation von App-gesteuerten Herzschrittmachern oder Insulinspritzen, welche zu Körperverletzungen oder sogar zum Tod von Patienten führen könnten. Von besonderer Brisanz sind Hackerangriffe auf Informationssysteme, die eine große Zahl von Patienten betreffen, etwa auf Datenbanken von Krankenhäusern, die Daten von Krankenkassen oder die elektronische Patientenakte.

A. Verantwortlichkeit des Hackers

Strafrechtlich verantwortlich ist zunächst der Hacker selbst. Er kann sich v.a. nach § 202a dStGB (Ausspähen von Daten) strafbar machen, im Fall der Manipulation von Daten auch nach § 303a dStGB (Datenveränderung) oder nach § 303b dStGB (Computersabotage), wenn die Datenverarbeitung für einen anderen von wesentlicher Bedeutung ist. Dies dürfte etwa bei einem Angriff auf den zentralen Rechner eines Krankenhauses oder einer Krankenkasse anzunehmen sein. Wird infolge einer Manipula-

⁴² Dazu umfassend Stiftung Datenschutz (Hrsg.), Big Data und E-Health, 2017.

⁴³ Herzog, in: Böttiger/zu Putlitz (Fn. 2), 337 ff.

tion ein Mensch verletzt oder getötet, kommen die Körperverletzungsdelikte (§§ 223 ff. dStGB) oder Tötungsdelikte (§§ 211 ff. dStGB) in Betracht. Der Ankäufer von Daten kann wegen Datenhehlerei (§ 202d dStGB) strafbar sein.

Zusätzliche Probleme ergeben sich bei Fällen mit Auslandsbezug, etwa wenn der Hacker oder das angegriffene Unternehmen oder beide im Ausland agieren. Das deutsche Strafrecht gilt gemäß § 3 dStGB für Taten, die im Inland begangen werden, d.h. Taten, deren Tathandlung im Inland vorgenommen wird oder deren Taterfolg im Inland eintritt (§ 9 dStGB). Wird die Tat im Ausland gegen einen Deutschen begangen, so ist nach § 7 Abs. 1 dStGB das deutsche Strafrecht anwendbar, wenn die Tat im Ausland ebenfalls mit Strafe bedroht ist.⁴⁴

B. Verantwortlichkeit des Unternehmens, bei dem die Daten gehackt werden

Das deutsche Strafrecht kennt bislang keine Unternehmensstrafbarkeit. Strafbar sein können nur natürliche Personen, also etwa die im Unternehmen für das Speichern der Daten und die Datensicherheit verantwortlichen Fachkräfte. Delikte wie das Ausspähen von Daten, § 202a dStGB, oder die Computersabotage, § 303a dStGB können allerdings nur vorsätzlich verwirklicht werden, eine Mittäterschaft oder die Beihilfe von Unternehmensmitarbeitern an diesen Taten scheiden daher in der Regel mangels Vorsatzes aus. Stehen z.B. eine Körperverletzung, § 223 dStGB oder gar eine Tötung, §§ 212, 211 dStGB, im Raum, so kommt aber auch die fahrlässige Begehung, §§ 229, 222 dStGB, in Betracht.

Maß für die anzuwendenden Sorgfaltspflichten sind dabei die akzeptierten Sicherheitsstandards. Wenn diese nicht eingehalten wurden und so der Hackerangriff ermöglicht wurde,

liegt eine Sorgfaltspflichtverletzung vor.⁴⁵ Es kommt dann auf die Vorhersehbarkeit und Vermeidbarkeit an. Die Klärung der damit angesprochenen **Haftung für Sabotagesicherheit** und die damit verbundene Gefahr einer **Verantwortungsdiffusion**⁴⁶ stellt eine der größten juristischen Herausforderungen im Internet der Dinge dar.

C. Providerhaftung

Von besonderer Bedeutung ist die Verantwortlichkeit der Provider. Üblicherweise unterscheidet man Content-, Host- und Service-Provider, wobei zu Letzteren insbesondere die Access-Provider zählen. In Deutschland ist die Providerhaftung im Telemediengesetz (TMG) geregelt. Die §§ 7 ff. TMG enthalten eine sehr weitgehende haftungsrechtliche Privilegierung der Provider, die in den Anfangsjahren des Internets sinnvoll war, um die neu entstehenden Geschäftsmodelle zu schützen. Heute erscheinen die Privilegien angesichts der Vernetzung in so sensiblen Bereichen wie dem Straßenverkehr oder dem medizinischen Bereich kaum mehr zeitgemäß und bedürfen dringend der Überprüfung.

Dies gilt insbesondere für die faktische Haftungsfreistellung der Accessprovider, die nach in Deutschland verbreiteter Ansicht selbst dann greifen soll, wenn ein Accessprovider von kriminellen Aktivitäten eines bestimmten Nutzers erfährt und diesen trotz Aufforderung (z.B. durch die Polizei) nicht vom Netz nimmt. Richtigerweise ist hier zumindest eine Beihilfestrafbarkeit anzunehmen (z.B. wenn der in Frage stehende Nutzer, nachdem der Provider sich trotz Wissen um dessen Tatpläne geweigert hatte, ihn vom Netz zu nehmen, eine medizinische Einrichtung mittels Schadsoftware angreift und dadurch vorsätzlich Menschen

⁴⁴ Rechtsvergleichend Schwarzenegger, Der räumliche Geltungsbereich des Strafrechts im Internet, ZStrR 2000, 109 ff.

⁴⁵ Hilgendorf, Verantwortungsdiffusion und selbstlernende Systeme in der Industrie 4.0 – ein Problemaufriss aus strafrechtlicher Perspektive, in: Hornung (Hrsg.), Rechtsfragen der Industrie 4.0. Datenhoheit, Verantwortlichkeit, rechtliche Grenzen der Vernetzung, Baden-Baden 2018, 119 (126).

⁴⁶ Hilgendorf (Fn. 46), 119 (120 f., 129 ff.).

verletzt).⁴⁷ Das deutsche Netzwerkdurchsetzungsgesetz vom 1. September 2017⁴⁸ weist in die richtige Richtung, geht aber nicht weit genug.

*

Wie die Beispiele zeigen, sind die durch die Digitalisierung der Medizin aufgeworfenen rechtlichen Probleme durchaus auf der Basis des geltenden Rechts, u.U. mit Fortbildungen

de lege ferenda, zu lösen. Eines gänzlich neuen «**Rechts der Digitalisierung**» bedarf es nicht. Der Revolution in der IT, die zu einer fortschreitenden Digitalisierung unserer gesamten Lebens- und Arbeitswelt unter Einschluss des Gesundheitswesens geführt hat,⁴⁹ sollte man nicht durch eine juristische Revolution zu begegnen versuchen, sondern durch eine reflektierte **Evolution des geltenden Rechts**.⁵⁰

⁴⁷ Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. Aufl., Berlin/Heidelberg 2012, Rn. 215 ff.

⁴⁸ BGBl. I, 3352 ff.; im Internet unter https://www.bmjv.de/Shared-Docs/Gesetzgebungsverfahren/Dokumente/BGBl_NetzDG.pdf?__blob=publicationFile&v=2.

⁴⁹ Nicht wenige sprechen deshalb sogar von der «digitalen Transformation», vgl. bereits den Titel des Werkes von Matusiewicz et al. (Fn. 2) sowie Lohmann, in Matusiewicz et al. (Fn. 2), 7 ff.

⁵⁰ Hilgendorf, FS Fischer (Fn. 14), 101 (113).

