Rechtliche Herausforderungen der Digitalisierung des Gesundheitswesens

Benedikt Buchner
Institut für Informations-, Gesundheits- und Medizinrecht, Universität Bremen

Mitte Juni 2017 fand in Ludwigshafen der Digitalgipfel der Bundesregierung statt, in dessen Zentrum diesmal die Digitalisierung des Gesundheitswesens stand [1]. Allseits betont und beschworen wurden wieder einmal die Chancen, die mit einer Digitalisierung des Gesundheitswesens und der Vernetzung und Zentralisierung von Patientendaten einhergehen: Sie sollen der Schlüssel für eine personalisierte Medizin sein, mehr Wissen und damit bessere Behandlungsmethoden schaffen und eine Vielzahl von Möglichkeiten eröffnen, angefangen bei der Videosprechstunde bis hin zum jederzeit verfügbaren Medikationsplan [2]. Wie mit fast jeder Innovation gehen mit der Digitalisierung des Gesundheitswesens aber auch Risiken und neue Herausforderungen einher, die im Folgenden aus rechtlicher Perspektive beleuchtet werden sollen. Je mehr (personenbezogenes) Wissen geschaffen und geteilt wird, desto mehr rücken Aspekte des Datenschutzes und der Datensicherheit in das Zentrum der rechtlichen Betrachtung. Ebenso geht es um Fragen des sog. Rechts auf Nichtwissen, welches sich mit dem stetigen Wissenszuwachs nur noch schwer vereinbaren und gegenüber diesem absichern lässt. Und nicht zuletzt stellt sich die Frage, inwieweit die Digitalisierung des Gesundheitswesens möglicherweise auch zu einer Aushöhlung des bislang unser Gesundheitswesen prägenden Solidarprinzips führt.

Datenschutz und Datensicherheit

Das Projekt elektronische Gesundheitskarte ist ein Beispiel dafür, dass die Digitalisierung des Gesundheitswesens in vielerlei Hinsicht nicht so sehr eine rechtliche Herausforderung des Datenschutzes, sondern vielmehr eine technische Herausforderung der Datensicherheit ist. Aus datenschutzrechtlicher Perspektive hat der deutsche Gesetzgeber mit § 291a SGB V einen Regelungsrahmen konzipiert, der den datenschutzrechtlichen Idealvorstellungen schon sehr nahe kommt. Zu Recht wird gesagt, dass die gesetzliche Regelung der elektronischen Gesundheitskarte und der Telematik-Infrastruktur aus Datenschutzsicht „fast vorbildlich" ist [3]. Die Prinzipien der Patientenautonomie und der informationellen Selbstbestimmung haben in § 291a SGB V eine konsequente Umsetzung gefunden. Die Regelung zielt darauf ab, das Recht auf informationelle Selbstbestimmung bestmöglich abzusichern, indem die Einwilligung des Versicherten als Legitimationsgrundlage für eine Datenverarbeitung in das Zentrum gestellt wird und die Voraussetzungen für eine wirksame Einwilligung (Informiertheit, Bestimmtheit, Freiwilligkeit) ebenso wie die klassischen Betroffenenrechte (Widerruf, Löschung) in vielerlei Hinsicht eine rechtliche Absicherung erfahren [4: 662f.].

> Das zentrale Problem der elektronischen Gesundheitskarte ist und bleibt aber die technische Umsetzung dieses rechtlich vorgegebenen Datenschutzes, also die Datensicherheit. Gerade weil es sich bei Gesundheitsdaten um besonders sensible Daten handelt und diese Daten in einem digitalisierten Gesundheitssystem zentralisiert zusammengeführt werden sollen, sind die Anforderungen an die Datensicherheit so hoch an- und damit aber offensichtlich auch so schwierig umzusetzen.

Betrachtet man den ursprünglichen Fahrplan, den der Gesetzgeber bei Inkrafttreten des § 291a SGB V Anfang 2004 vor Augen hatte, muss man ernüchtert feststellen, dass dieser Fahrplan mittlerweile um mehr als zehn Jahre überschritten worden ist, ohne dass absehbar wäre, wann all die anvisierten Funktionen der Karte wie etwa das elektronische Rezept oder das Patientenfach Realität werden.

§ 291a SGB V a.F.

Nach § 291a SGB V sollte die elektronische Gesundheitskarte „bis spätestens zum 1. Januar 2006" inkl. aller Zusatzfunktionen einsatzbereit sein.

Knieps F | Pfaff H (Hrsg.) "Digitale Arbeit - Digitale Gesundheit". BKK Gesundheitsreport 2017.
ISBN 978-3-95466-354-5, urheberrechtlich geschützt

Und nur einen Tag nach dem eingangs erwähnten Digitalgipfel mit all seinen rosigen Prognosen für das digitalisierte Gesundheitswesen war zum Projekt elektronische Gesundheitskarte nachzulesen, dass es – wieder einmal – zu technischen Umsetzungsschwierigkeiten gekommen ist, aktuell weil die rechtzeitige und flächendeckende Versorgung der Arztpraxen mit den Kartenlesegeräten offensichtlich nicht gewährleistet werden kann [5].

Vor diesem Hintergrund ist es naheliegend und auch sachgerecht, dass sich das E-Health-Gesetz von 2015 vornehmlich darauf konzentriert, die technische Umsetzung des Projekts elektronische Gesundheitskarte voranzutreiben. Soweit es um die datenschutzrechtliche Fest- und Fortschreibung eines angemessenen Datenschutzniveaus geht, hat der Gesetzgeber seine „Hausaufgaben" bereits erledigt. Die eigentliche Herausforderung ist beim Projekt elektronische Gesundheitskarte nunmehr darin zu sehen, auch einen Regelungsrahmen zu finden, der die Akteure im Gesundheitswesen dazu anhält, die technische Umsetzung des Datenschutzes, die Datensicherheit, zu realisieren. Beim E-Health-Gesetz stützt sich der Gesetzgeber hierfür auf verschiedene Regelungsansätze; ob diese die technische Umsetzung erfolgreicher voranbringen werden, bleibt abzuwarten. Zu begrüßen ist jedenfalls, dass sich das E-Health-Gesetz nicht nur darauf beschränkt, die technischen Zielvorgaben ganz klassisch mittels Fristen und Sanktionen einzufordern, sondern darüber hinaus auch andere Wege beschritten werden [4: 662f.]. So setzt das E-Health-Gesetz etwa auch darauf, mittels positiver Anreize die Akteure zum Einsatz neuer Techniken zu bewegen.

Beispiel

§ 291f Abs. 1 SGB V: zusätzliche Honorierung einer Übermittlung elektronischer Briefe von Arzt zu Arzt.

Ebenso sollen Entscheidungen forciert werden, soweit diese bislang an Abstimmungs- und Einigungsschwierigkeiten zwischen den Institutionen im Gesundheitswesen gescheitert sind.

Beispiel

§ 87 Abs. 2a SGB V: Sanktionen für den Fall, dass der einheitliche Bewertungsmaßstab nicht fristgerecht angepasst wird.

Digitalisierung auf dem „zweiten Gesundheitsmarkt"

Zu kurz gegriffen wäre es, die bisherigen Schwierigkeiten und Verzögerungen beim Projekt elektronische Gesundheitskarte lediglich als einen weiteren Beleg für das Scheitern staatlicher Großprojekte in Deutschland zu werten. Gedeutet werden sollten die bisherigen Misserfolge vielmehr dahingehend, dass bei der Datensicherheit bislang eben trotz aller Schwierigkeiten keine Abstriche gemacht worden sind und die hohen datenschutzrechtlichen Anforderungen nicht gelockert worden sind.

> Der weiteren Digitalisierung des Gesundheitswesens soll gerade nicht um jeden Preis der Weg geebnet werden.

Private Anbieter sind demgegenüber naturgemäß weniger zögerlich, wenn es um die Realisierung neuer digitaler (Geschäfts-)Modelle geht. Daher erstaunt es nicht, dass gerade auf dem sog. „zweiten Gesundheitsmarkt" die Digitalisierung derzeit den größeren Fortschritt erlebt.

> Der **erste Gesundheitsmarkt** wird dominiert von Organen der gemeinsamen Selbstverwaltung und stützt sich auf eine solidarische Finanzierung durch Kostenträger, z.B. gesetzliche Krankenkassen und private Krankenversicherungen. Der **zweite Gesundheitsmarkt** zeichnet sich hingegen durch einen stärkeren Fokus auf eigenfinanzierte Gesundheitsdienstleistungen aus und wird von privaten Anbietern dominiert [6: 191f.].

Egal ob Apple mit HealthKit, Microsoft mit Vitabook oder das Hasso-Plattner-Institut mit der Gesundheitscloud: All diese Anbieter präsentieren voller Zuversicht ihre Alternativangebote zur elektronischen Gesundheitskarte, die dem Einzelnen ebenfalls Funktionen wie eine persönliche Patientenakte oder einen persönlichen Medikationsplan eröffnen sollen. Die Zielsetzung dieser Anbieter ist ganz im Sinne der elektronischen Gesundheitskarte: mehr Patientensouveränität und -selbstbestimmung, der Patient als „Herr" seiner Daten, eine sicherere und bessere Behandlung dank vollständiger Datengrundlage usw. Und all dies soll nicht nur genauso sicher, sondern vor allem auch schneller als das Projekt Gesundheitskarte zu realisieren sein. Oder, um die Worte von Microsoft aufzugreifen:

„Die Politik plant seit fast 20 Jahren erfolglos die Einführung eines Notfalldatensatzes, den Online-Medikationsplan, das

Knieps F | Pfaff H (Hrsg.) "Digitale Arbeit - Digitale Gesundheit". BKK Gesundheitsreport 2017.
ISBN 978-3-95466-354-5, urheberrechtlich geschützt

e-Rezept, eine Gesundheitsakte und vieles mehr. All das bietet vitabook bereits jetzt." [7].

Ungeachtet all der möglicherweise innovativeren und auch schneller umsetzbaren Alternativen, die private Anbieter realisieren könnten, bleibt es aber zweifelhaft, ob das hohe Datenschutz- und Datensicherheitsniveau, wie es mit der elektronischen Gesundheitskarte verfolgt wird, bei einer Überantwortung der Digitalisierung des Gesundheitswesens an private Dienstleister gleichermaßen gewährleistet wäre. Die rechtlichen und technischen Schutzmechanismen, wie sie in § 291a SGB V vorgesehen sind, lassen sich bei einer Datenverarbeitung durch private Akteure nicht in vergleichbarer Weise umsetzen. Verwiesen sei hier beispielhaft auf das zentrale Zwei-Schlüssel-Prinzip mit der Kombination aus elektronischer Gesundheitskarte und elektronischem Heilberufsausweis, die einen besonderen Schutz vor Datenmissbrauch gewährleisten soll [8]. Und auch die Einwilligung als Erlaubnistatbestand für eine Verarbeitung von Gesundheitsdaten kann nur als Ausdruck einer freien Entscheidung eines Patienten verstanden und ihr mithin nur dann eine Legitimationswirkung zugeschrieben werden, wenn sie mit einem engen rechtlichen Korsett versehen ist, wie es bislang § 291a SGB V vorsieht: Insbesondere muss gewährleistet sein, dass die Einwilligung unter einer strengen Erforderlichkeitsmaxime steht und nicht als Einfallstor für eine denkbar weite Datenverarbeitung instrumentalisiert wird, wie es gerade im Bereich der privaten Datenverarbeitung regelmäßig der Fall ist [9]. Je mehr die Digitalisierung des Gesundheitswesens privatisiert wird, desto größer ist das Risiko, dass die Einwilligung der betroffenen Patienten in ein bloßes Kommerzialisierungsinstrument mündet. Auch im Gesundheitsbereich gibt es genügend Mittel und Wege, Versicherte und Patienten durch die Aussicht auf entsprechende Gegenleistungen zu einer großzügigen Preisgabe all ihrer sensitiven Gesundheitsdaten zu bewegen. Verwiesen sei hier nur auf erste Modelle im Bereich der Privatversicherung, „gute" Gesundheitsdaten zu Lebensstil und Fitness mit günstigeren Versicherungsprämien zu belohnen [10]. Und nicht zuletzt sei auf die teils gravierenden Datenschutzdefizite verwiesen, die die Angebote privater Anbieter auf dem Markt für digitale Gesundheit prägen, etwa bei sog. Wearables wie Fitness-Armbänden und Smart Watches samt zugehörigen Apps [11]. Gleichzeitig darf aber auch nicht vergessen werden, dass Patienten eine Modernisierung des Gesundheitswesens im Allgemeinen und insbesondere digitale Angebote zur eigenen Kontrolle des Gesundheitszustandes, zur Dokumentation des Behandlungsverlaufs und zur Prävention einfordern. Nicht ohne Grund können private Anbieter mit ihren Angeboten teils sehr erfolgreich sein [6: 192].

> Aus all den genannten Gründen darf die Digitalisierung des Gesundheitswesens jedenfalls dann, wenn man Datenschutz und Datensicherheit ernst nimmt, nicht allein privaten Akteuren auf dem zweiten Gesundheitsmarkt überlassen werden. Auch wenn greifbare Fortschritte wie beim Projekt elektronische Gesundheitskarte sehr lange auf sich warten lassen, müssen gesetzliche Krankenkassen und andere Akteure auf dem ersten Gesundheitsmarkt das Projekt „Digitalisierung" weiter vorantreiben.

Recht auf Nichtwissen und Big Data

Das stetige Mehr an Gesundheitsdaten, das mittels Digitalisierung zu einem Mehr an Wissen führen soll, nährt vor allem die Hoffnung auf ein Mehr an Gesundheit. Oder, um die Worte unserer Bundesforschungsministerin aufzugreifen: „Datenmengen müssen zusammengebracht und ausgewertet werden – dann können sie uns helfen, Krankheiten besser zu verstehen und zu behandeln". Das Ziel ist ein „lernendes, digital vernetztes Gesundheitssystem, in dem stets die richtige Person die richtige Information zur richtigen Zeit hat." [2] Für das Recht auf Nichtwissen scheint unter dieser Zukunftsvision von Big Data kaum noch Platz zu sein, zielt dieses Recht doch darauf ab, dass Informationen nicht an die „richtige Person" gelangen, sondern stattdessen überhaupt nicht zur Kenntnis genommen werden. Das Recht auf Nichtwissen zielt auf ein Weniger, nicht ein Mehr an Informationen. Es soll den Patienten gerade davor bewahren, alle möglichen Informationen über seinen Gesundheitszustand zu erlangen, auch wenn er ein derartiges Wissen gar nicht erhalten möchte. In den 90er-Jahren standen in diesem Zusammenhang u.a. heimliche HIV-Tests und ihre routinemäßige Durchführung bei Blutentnahmen im Zentrum der Debatte [12]. Nunmehr ist anerkannt, dass der Einzelnen zunächst einmal davor zu schützen ist, ohne seine Zustimmung in Kenntnis über seinen HIV-Status gesetzt zu werden [13].

Das Recht auf Nichtwissen wurzelt dabei im allgemeinen Persönlichkeitsrecht und berücksichtigt, dass die Kenntnis von bestimmten Informationen möglicherweise die Lebensplanung und Lebensführung einer Person ganz erheblich beeinträchtigt und deshalb das von Art. 2 Abs. 1 GG gewährleistete

Knieps F | Pfaff H (Hrsg.) "Digitale Arbeit - Digitale Gesundheit". BKK Gesundheitsreport 2017.
ISBN 978-3-95466-354-5, urheberrechtlich geschützt

Selbstbestimmungsrecht der betroffenen Person berührt ist [14: 2191]. Es präsentiert sich damit insgesamt als wissens- und damit fortschrittsfeindlich und vor allem in Zeiten einer zunehmenden Big-Data-Euphorie als zu rückwärtsgewandt.

Abgesehen von diesem grundsätzlichen Akzeptanzproblem sieht sich das Recht auf Nichtwissen gerade unter Big Data auch einem „strukturellen" Problem gegenüber. Um überhaupt sein Recht auf Nichtwissen ausüben zu können, bedarf der Einzelne zunächst einmal der Kenntnis dahingehend, welches Wissen denn zur Wahl steht [15: 667]. Eben dieses potenzielle Wissen ist aber unter Big Data überhaupt nicht mehr überschau- oder eingrenzbar. Die Philosophie von Big Data ist dadurch gekennzeichnet, dass Daten ohne Ziel und Zweck gesammelt und ausgewertet werden. Es ist an den Algorithmen, frei von jeder Ziel- und Zwecksetzung ergebnisoffen nach Verknüpfungsmustern zu suchen und nicht intendierte „Nebeninformationen" zu gewinnen, deren Art und Umfang von vornherein in keiner Weise absehbar sind [16: 92f.]. Damit bleibt aber die Frage offen, wie ein Recht auf Nichtwissen im Gesundheitsbereich überhaupt noch ausgeübt werden kann, wenn medizinisches Wissen derart unstrukturiert und jenseits der bislang üblichen Kausalitätsmuster gewonnen wird.

Umgekehrt ist das Recht auf Nichtwissen aber gerade in Zeiten von Big Data von besonderer Bedeutung [15: 668f.]. Allein schon die schiere Menge an Wissen, die durch Big Data geschaffen wird, bringt es mit sich, dass der Einzelne mit immer mehr Wissen konfrontiert wird, das möglicherweise mehr belastet als nützt. So produziert Big Data oftmals ein Wissen, das keine eindeutigen Aussagen, sondern lediglich Wahrscheinlichkeiten präsentiert. Wie aber soll eine Person etwa mit einer Wahrscheinlichkeitsprognose dergestalt umgehen, auf Grundlage einer Auswertung ihrer Daten aus sozialen Netzwerken sei mit einer 80%igen Wahrscheinlichkeit davon auszugehen, dass sie künftig einmal zu Drogen-, Tabak- oder Alkoholmissbrauch neigen werde? [17] Oder soll sich etwa eine Frau, der ein erhöhtes Brustkrebsrisiko prognostiziert wird, präventiv die Brust entfernen lassen? [18] Problematisch sind solcherlei Wahrscheinlichkeitsaussagen vor allem dann, wenn sich deren Qualität und Richtigkeit nur schwer oder gar nicht verifizieren lassen [19]. Und nicht zuletzt ist der schiere Wissenszuwachs infolge von Big Data auch deshalb problematisch, weil sich damit regelmäßig auch die Schere zwischen bloßem Wissen und möglichen Reaktionen auf diesen Wissenszuwachs weiter vergrößert. Das bloße Wissen um einen (mehr oder weniger wahrscheinlichen) schicksalhaften Verlauf von Leben und Gesundheit ohne die Möglichkeit, auf dieses Wissen reagieren und das prognostizierte Schicksal beeinflussen zu können, stellt für den Einzelnen eine ganz erhebliche Belastung und Beeinträchtigung seiner Persönlichkeit und Lebensführung dar.

All die genannten Aspekte sind nicht neu und nicht auf Big Data beschränkt, sondern haben sich als solche insbesondere auch schon mit den Fortschritten der Gendiagnostik gezeigt. Eben deshalb ist unter dem Gendiagnostikgesetz auch dem Recht auf Nichtwissen eine besondere Beachtung geschenkt und dieses Recht im Gendiagnostikgesetz entsprechend abgesichert worden.

§ 9 Abs. 2 Nr. 5 GenDG

Vor Einholung einer Einwilligung muss über das Recht auf Nichtwissen aufgeklärt werden.

§ 11 Abs. 4 GenDG

Das Ergebnis der genetischen Untersuchung darf der betroffenen Person nicht mitgeteilt werden, soweit die betroffene Person entschieden hat, dass das Ergebnis der genetischen Untersuchung zu vernichten ist oder sie ihre Einwilligung widerrufen hat.

Zu berücksichtigen ist in diesem Zusammenhang allerdings, dass es sich bei genetischen Daten um eine ganz bestimmte, eng eingegrenzte Wissenskategorie handelt, deren Nutzung detailliert reguliert werden kann. Vor allem auch der Umgang mit diesem Wissen kann unter einen strengen Arztvorbehalt gestellt werden. Eben darin unterscheidet sich das spezifisch gendiagnostische Wissen von dem allumfassenden Wissen, wie es durch Big Data allgemein produziert wird. Und eben deshalb wird es trotz aller Chancen, die Big Data mit sich bringt, eine besondere Herausforderung sein, ein Recht auf Nichtwissen auch in Zeiten von Big Data weiterhin als Schutzinstrumentarium für den einzelnen Betroffenen zu erhalten.

Ausblick: Digitalisierung, Big Data und Solidarprinzip

Nicht zuletzt ist der stetige Gewinn an Wissen bzw. der Verlust an Nichtwissen eine Bedrohung für das Solidarprinzip, wie es bislang in vielerlei Hinsicht den gesellschaftlichen Zusammenhalt prägt. Mit jedem Wissenszuwachs hinsichtlich der Eigenheiten und damit auch Ungleichheiten der einzelnen Individuen einer Gesellschaft sinkt auch die potenzielle

Knieps F | Pfaff H (Hrsg.) "Digitale Arbeit - Digitale Gesundheit". BKK Gesundheitsreport 2017.
ISBN 978-3-95466-354-5, urheberrechtlich geschützt

Bereitschaft, sich im Sinne einer Risikogemeinschaft solidarisch zu verhalten und unabhängig von der eigenen „Stärke“ die „Schwächen“ der Anderen mitzutragen [20: 194ff.]. Selbst im Bereich der Privatversicherung, bei der Beiträge schon immer auch risikobasiert bemessen worden sind, gibt es bislang einen Restschleier von Nichtwissen, der letztlich die Gewähr dafür bietet und vor allem Motivation dafür ist, dass sich unterschiedliche Risiken in einer Risikogemeinschaft zusammenfinden. Digitalisierung und Big Data werden demgegenüber einer weiteren Individualisierung massiven Vorschub leisten und letztlich den für jede Versichertengemeinschaft nötigen Schleier des Nichtwissens weiter lüften und damit für Versicherungsmodelle herkömmlicher Art immer weniger Raum lassen. Vor diesem Hintergrund spricht viel dafür, dass in Zeiten eines schier grenzenlosen Wissenszuwachses letztlich nur solche Versicherungssysteme zukunftsfest sind, die das Risikoprinzip von vornherein ausblenden und stattdessen auf ein Solidarprinzip setzen, welches überhaupt keiner Wissensgrundlage bedarf – egal was Digitalisierung und Big Data zukünftig an Wissen im positiven und im negativen Sinne schaffen werden.

Literatur

1. Pressemitteilung des BMWi. Zypries eröffnet Digital-Gipfel 2017: „Digital-Gipfel sendet starke Impulse für die digitale Vernetzung der Regionen, des Gesundheitswesens und der Wirtschaft“. URL: https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2017/20170613-zypries-eroeffnet-digital-gipfel-2017.html (Zugriff am: 02.07.2017)
2. Pressemitteilung 062/2017 des BMBF. Mit digitaler Gesundheit an die Spitze. URL: https://www.bmbf.de/de/mit-digitaler-gesundheit-an-die-spitze-4300.html (Zugriff am: 02.07.2017)
3. Stellungnahme des ULD zum Referentenentwurf für ein eHealth-Gesetz vom 11.2.2015. URL: https://www.datenschutzzentrum.de/artikel/874-ULD-Stellungnahme-zum-Referentenentwurf-fuer-ein-E-Health-Gesetz.html (Zugriff am: 02.07.2017)
4. Buchner B. Datenschutz und Datensicherheit in der digitalisierten Medizin. MedR 2016; 660
5. Ludwig K. Gesundheitskarte sorgt für neue Probleme. SZ-online vom 14.06.2017. URL: http://www.sueddeutsche.de/wirtschaft/krankenversicherung-gesundheitskarte-sorgt-fuer-neue-probleme-1.3544753 (Zugriff am: 02.07.2017)
6. Meister S., Becker S., Leppert F., Drop L. Digital Health, Mobile Health und Co. – Wertschöpfung durch Digitalisierung und Datenverarbeitung. In: Pfannstiel/Da-Cruz/Mehlich. Digitale Transformation von Dienstleistungen im Gesundheitswesen I. Wiesbaden 2017, S. 185
7. vitabook GmbH. URL: https://www.vitabook.de/ (Zugriff am: 02.07.2017)
8. Heldt-Andreas K. In: Bergmann/Pauge/Steinmeyer. Gesamtes Medizinrecht. 2. Aufl. 2014. § 291a SGB V Rn. 6ff.
9. Kühling J. BeckOK-Datenschutzrecht. 20. Ed. § 4a BDSG Rn. 62ff.
10. Generali Vitality GmbH. URL: https://www.generali-vitality erleben.de/ (Zugriff am: 02.07.2017)
11. Pressemitteilung vom 26.04.2017 der Verbraucherzentrale NRW. Wearables und Fitness-Apps: Daten außer Kontrolle. URL: http://www.verbraucherzentrale.nrw/wearables-und-fitness-apps–daten-ausser-kontrolle (Zugriff am: 02.07.2017)
12. Der Spiegel vom 29.11.1993, Zweifler auf der Zinne. URL: http://www.spiegel.de/spiegel/print/d-13682546.html (Zugriff am: 02.07.2017)
13. LG Köln. NJW 1995; 1621
14. BGH. NJW 2014; 2190
15. Duttge G. Das Recht auf Nichtwissen in einer informationell vernetzten Gesundheitsversorgung. MedR 2016; 664
16. Ladeur K.H. Wissenserzeugung im Sozialrecht und der Aufstieg von „Big Data“. In: Buchner/Ladeur. Wissensgenerierung und -verarbeitung im Gesundheits- und Sozialrecht. Tübingen 2016, S. 89
17. Studie der Conell University. Social Media-based Substance Use Prediction. URL: https://arxiv.org/abs/1705.05633 (Zugriff am: 02.07.2017)
18. Lossau, N. Wann ist präventive Brustentfernung sinnvoll? Welt-online vom 30.03.2017. URL: https://www.welt.de/gesundheit/article163269488/Wann-ist-praeventive-Brustentfernung-sinnvoll.html (Zugriff am: 02.07.2017)
19. Hoeren T. Big Data und Datenqualität – ein Blick auf die DS-GVO. ZD 2016; 459
20. Buchner B. Informationelle Selbstbestimmung. Tübingen 2006

Prof. Dr. Benedikt Buchner, LL.M. (UCLA)

Professor für Bürgerliches Recht an der Universität Bremen; Direktor des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR) der Universität Bremen.

Studium der Rechtswissenschaften in Augsburg, München und Los Angeles; 1999 bis 2005 wissenschaftlicher Assistent an der Ludwig-Maximilians-Universität München; 2005 Habilitation an der Juristischen Fakultät der Universität München mit einer Arbeit zum Thema „Informationelle Selbstbestimmung im Privatrecht“ (Bayerischer Habilitationsförderpreis; Wissenschaftspreis 2005 der Deutschen Stiftung für Recht und Informatik); Vorsitz Ethikkommission und Vorstandsmitglied DSRI; zahlreiche Publikationen zum Gesundheits- und Datenschutzrecht.

Knieps F | Pfaff H (Hrsg.) "Digitale Arbeit - Digitale Gesundheit". BKK Gesundheitsreport 2017.
ISBN 978-3-95466-354-5, urheberrechtlich geschützt