Gerrit Hornung/Manuela Sixt

Cyborgs im Gesundheitswesen

Die rechtlichen Herausforderungen der technischen Erhaltung und Optimierung körperlicher Funktionen („IT-Enhancement")

Ausgehend von der historischen Motivation, die Funktionen des eigenen Körpers zu erhalten, wenn nicht gar zu verbessern (I.) beschreibt der Beitrag zunächst eine Auswahl technischer Innovationen, die ein IT-Enhancement körperlicher Funktionen ermöglichen und zugleich ein erhöhtes Risikopotential darstellen (II.). Im Schwerpunkt werden zum einen der Fächer aufgeworfener Fragen auf grundrechtlicher sowie einfachgesetzlicher Ebene präsentiert (III.) und zum anderen die Fragen des Datenschutzes und der Datensicherheit analysiert (IV.). Schließlich zeigt der Ausblick (V.) die Bereiche auf, in denen disruptive Veränderungen zu erwarten sind.

I. Hintergründe und Abgrenzungen

Dass Menschen ihren Körper (in einem sehr allgemeinen Sinn) verbessern, ist keine neue Entwicklung. Schon in der Antike wurden bestimmte Ideale des äußeren Erscheinungsbilds und der körperlichen Leistungsfähigkeit propagiert.[1] Der Mythos von Daidalos und Ikaros zeugt nicht nur vom ewigen Traum des Menschen, sich in die Lüfte zu schwingen, sondern auch von der Phantasie, den eigenen Körper um künstliche Bestandteile zu erweitern. Mit der beginnenden Moderne verbinden sich diese Leitbilder mit der allgemeinen Technisierung des menschlichen Lebens. Zumindest in fiktionalen Darstellungen erstreckt sich der Einsatz neuer Technologien bald nicht nur auf die Umgebung des menschlichen Körpers, sondern auch auf diesen selbst.[2]

Viele dieser Vorstellungen von hybriden, organisch-technischen Wesen sind nach wie vor Science Fiction und werden dies auf absehbare Zeit auch bleiben.[3] Andere umfassen relativ konkrete technische Visionen, die inzwischen teilweise umgesetzt sind oder in naher Zukunft umsetzbar sein werden. Während die ersten tatsächlich verfügbaren technischen Hilfsmittel zumeist mechanischer Art waren, lässt sich seit einigen Jahren ein deutlicher Trend zum Einsatz von Informationstechnologie beobachten.

Ab welchem Grad an Technikeinsatz man Menschen, deren Körperfunktionen durch solche Hilfsmittel wiederhergestellt oder erweitert werden, als „Cyborgs" bezeichnet, ist im Wesentlichen eine definitorische Frage. Bemerkenswert ist jedenfalls, dass dieser Begriff – der sich aus den Wörtern cybernetic und organism zusammensetzt[4] – vielfach in einem positiven Sinn verwendet wird. Betroffene, die aufgrund medizinischer Notwendigkeit oder technischer Begeisterung Prothesen, Körperimplantate oder andere elaborierte Hilfsmittel verwenden,[5] bezeichnen sich selbst als Cyborgs und organisieren Veranstaltungen zum Austausch über technische Innovationen und Erfahrungen.[6] Während im Bereich der fiktionalen Charaktere viele abstoßende Beispiele wie die Borg aus der Science Fiction-Serie „Star Trek" zu finden sind,[7] entspricht ein solches neutrales oder sogar positiv konnotiertes Verständnis sogar dem der Erfinder des Begriffs. Dieser wurde erstmals im Jahre 1960 durch *Clynes* und *Kline* im Titel eines Aufsatzes zur technisch unterstützten Anpassungsfähigkeit des Menschen an die Lebensbedingungen im Weltraum verwendet.[8]

Im Weiteren soll es weniger um die grundsätzlichen Utopien und Dystopien gehen, die sich mit dem Begriff des Cyborgs verbinden, sondern um konkrere Fragen der „Verbesserung" des menschlichen Körpers. Diese kann sich zum einen auf eine Wiederherstellung oder Aufrechterhaltung menschlicher Fähigkeiten beziehen, die aus medizinischer Sicht indiziert ist. Zum anderen finden sich auch erste Beispiele für nicht-indizierte Anwendungen. Diese zielen darauf, die geistige und körperliche Leistungsfähigkeit des menschlichen Körpers über das „Natürliche" hinaus zu steigern.

Einzelne Instrumente zu einer derartigen Verbesserung werden häufig als „Enhancement" bezeichnet. In der wissenschaftlichen Diskussion wird dieser Begriff überwiegend auf die Gruppe nicht medizinisch indizierter Eingriffe beschränkt.[9] Aus rechtlicher Sicht ist allerdings

▷ Prof. Dr. Gerrit Hornung, LL.M. (Edinburgh), ist Professor für Öffentliches Recht, IT-Recht und Umweltrecht an der Universität Kassel und Mitglied des Direktoriums des Wissenschaftlichen Zentrums für Informationstechnik-Gestaltung (ITeG). Manuela Sixt ist Stipendiatin im DFG-Graduiertenkollegs „Privatheit" der Universität Passau. Der Text geht auf einen Vortrag des Erstautors auf der Tagung des Instituts für Europäische Gesundheitspolitik & Sozialrecht (ineges) am 24.3.2015 in Frankfurt zurück. Eine erweiterte Version wird im Tagungsband erscheinen.

1 *Pröglhöf/Mixday-Schima* in Hergovich (Hrsg.), Psychologie der Schönheit. Physische Attraktivität aus wissenschaftlicher Sicht, 2002, 104 ff.; *Wiesing* in Gordijn/Chadwick (Hrsg.), Medical Enhancement and Posthumanity, 2009, 9 ff.; s. zum Streben nach Selbstverbesserung in Antike und Neuzeit *Runkel*, Enhancement und Identität, 2010, 14 ff.; *Glockentöger/Bittner/Fangerau*, Jahrbuch für Wissenschaft und Ethik 2012, 71, 72 ff.; s. ferner die Beiträge in *Coenen/Gammel/Heil/Woyke* (Hrsg.), Die Debatte über „Human Enhancement", 2010.

2 S. die Zusammenstellung unter *https://en.wikipedia.org/wiki/Cyborgs_in_fiction*.

3 Zum Verhältnis von technofuturistischen Visionen und Science-Fiction-Literatur s. im hiesigen Zusammenhang *Gammel* in Coenen/Gammel/Heil/Woyke (Fn. 1.), 209 ff.

4 Er bezeichnet also ein hybrides Wesen, dessen organische Bestandteile durch „kybernetische" Elemente ergänzt oder erweitert werden, s. näher *Heilinger/Müller*, Jahrbuch für Wissenschaft und Ethik 2007, 23.; s.a. ebd., 21 ff. zu einzelnen Wesensmerkmalen; ferner *Clarke*, IEEE Technology and Society 30, 3 (2011), 49 ff.

5 Nach einer aktuellen Umfrage können sich 11 % der Bevölkerung „sehr gut" und 40 % „gut" vorstellen, sich Implantate zur Steigerung geistiger Fähigkeiten einpflanzen zu lassen, s. BMBF, Zukunftsmonitor 2015.

6 S. z.B. *http://borgfest.com/*: „a festival and expo to celebrate and support people interested in human augmentation, enhancement, body modification, and wearable technology". Verbindungen ergeben sich dabei auch zur „quantified self"-Bewegung, der es darum geht, durch Self-Tracking-Lösungen möglichst viele Daten über den eigenen Körper und das eigene Verhalten zu erheben und diese mit anderen auszutauschen.

7 Dabei handelt es sich um eine totalitäre, in der Art eines kollektiv agierenden Schwarms organisierte Gesellschaft aus Cyborgs, die andere Völker rücksichtslos assimiliert. Berühmt ist der (teilweise variierte) Ausspruch beim Kontakt mit diesen: „We are the borg. You will be assimilated. Resistance is futile".

8 *Clynes/Kline*, Cyborgs and space, Astronautics 1960, 26; frühe Beschreibungen auch bei *Rorvik*, As Man Becomes Machine: The Evolution of the Cyborg, 1971.

9 *Beck*, MedR 2006, 95; *Merkel*, ZStW 2009, 919, 929 f.; *Lindner*, MedR 2010, 463 f.; *Ruf*, Enhancements, 2014, 98 ff.; kritisch zur Unterscheidbarkeit *Groß* in Wienke/Eberbach/Kramer/Janke (Hrsg.), Die Verbesserung des Menschen, 2009, 85 ff.; Ausarbeitung einer Unterscheidung

gerade die Abgrenzung zwischen indizierten und nicht indizierten Eingriffen besonders relevant.[10] Im Weiteren werden deshalb beide Fallgruppen behandelt. Ohnehin ist die Unterscheidung in Grenzbereichen schwierig, weil sie vom Begriff der Krankheit abhängt, der sowohl aus medizinischer als auch aus rechtlicher Sicht nicht unumstritten ist.

Innerhalb der verschiedenen Möglichkeiten der Verbesserung des menschlichen Körpers nimmt der Bereich der Informationstechnologie („IT-Enhancement") eine besondere Stellung ein. In ihm verbinden sich zwei Modernitätsdiskurse. Zum einen schließt IT-Enhancement an die allgemeinere Diskussion um das Enhancement – insbesondere durch den Einsatz von Psychopharmaka (Neuro-Enhancement) – an und stellt viele dort diskutierte Probleme[11] unter einem neuen Blickwinkel. Zum anderen nimmt die Diskussion Grundfragen der Informationsgesellschaft auf, nämlich die Bedeutung technischer Hilfsmittel für das menschliche Leben, die damit verbundenen Veränderungen für das menschliche Selbstbild sowie die Möglichkeiten und Grenzen des Innovationsfolgenmanagements. Weitere Bezüge lassen sich zum Einsatz von Robotik im Gesundheitswesen[12] und zur Transplantationsmedizin[13] herstellen.

II. IT-Enhancement: Cyborgs ante portas?

In den letzten Jahren hat sich die Entwicklung technischer Hilfsmittel zur Untersrützung von Körperfunktionen erheblich beschlennigt. Die innovativen Technologien versprechen erhebliche Chancen, verursachen aber auch Risiken, die im Bereich der Gesundheitsversorgung bisher unbekannt waren.

1. Technische Innovationen

Unter dem Begriff des IT-Enhancements lässt sich eine Vielzahl technischer Innovationen zusammenfassen.

a) Herzschrittmacher

Eine erste Gruppe bildet die Verbesserung von Implantaten, die seit vielen Jahren in der Medizin Verwendung finden.[14] Moderne Herzschrittmacher können sich im Einzelfall auf die körperliche Beanspruchung des Trägers einstellen und den Herzschlag entsprechend anpassen.[15] Hierzu benötigen sie allerdings mehr Daten über die Herzfunktionen als ihre Vorgänger und eine gesteigerte Datenverarbeitungskapazität. Die Daten werden nicht nur einmalig für die Auslösung von Impulsen verwendet, sondern auch dauerhaft im Gerät gespeichert. Bei der Wartung des Schrittmachers und der Kontrolle des Einsatzes kann der behandelnde Arzt sodann die Informationen über den Herzrhythmus auslesen und auf diesem Wege eine Langzeitkontrolle durchführen. Nenere Entwicklungen ermöglichen die Datenabfrage auch durch den Patienten selbst, so dass dieser die Informationen kontinuierlich oder bei Beschwerden an seinen Arzt übermitteln kann.

Der Datenzugriff und die Konfiguration der Geräte werden perspektivisch standardmäßig (auch) über das Internet erfolgen. Bei Herzschrittmachern gibt es hierzn im Rahmen der Telenachsorge beziehungsweise des Telemonitorings je nach Anbieter schon länger Möglichkeiten zur Serveranbindung per GSM/GPRS oder über die Standardtelefonleitung.[16] Die Netzanbindungen sind in den letzten Jahren erheblich weiterentwickelt worden und ermöglichen deutlich gesteigerte Datenübertragungsraten. Insbesondere Mobilfunkstandards wie HSPA und LTE ermöglichen einen Breitbandzugang in Echtzeit über große Entfernungen auch im medizinischen Bereich.[17] Diese Weiterentwicklung wird z.B. beim Telemonitoring und bei der Telenachsorge eine bessere Telepräsenz sowie ein drahtlos mobiles Home-Monitoring ermöglichen.[18]

b) Hirnschrittmacher

Die Steuerung des menschlichen Körpers durch technische Geräte beschränkt sich seit einigen Jahren nicht mehr auf das Herz. Im Rahmen der sog. tiefen Hirnstimulation (umgangssprachlich „Hirnschrittmacher" genannt) werden dem Patienten zunächst mithilfe eine stereotaktischen Operation Elektroden minimalinvasiv an einem bestimmten Punkt im Gehirn platziert, der zuvor durch eine magnetresonanz- und computertomografische Aufnahme des Gehirns bestimmt wird. In einer zweiten Operation wird dann der eigentliche Hirnschrittmacher unter die Brusthaut implantiert und mit den Elektroden verbunden.[19] Bisher werden die Geräte insbesondere bei motorischen Problemen eingesetzt, an denen etwa Parkinson-Patienten leiden. Es gibt jedoch erste Erkenntnisse über die Möglichkeit der Beeinflussung von Gemütszuständen (die bisher vor allem als Nebenwirkungen auftreten), zur Steigerung der Gedächtnisleistung und anderer kognitiver Fähigkeiten.[20]

zwischen Therapie und Enhancement bei *Hoffmann*, Jahrbuch für Wissenschaft und Ethik 2006, 201 ff., kritisch und für eine engere Abgrenzung *Synofzik*, Ethik Med 2006, 37 ff.

10 *Beck*, MedR 2006, 95, 96 ff.; *Eberbach* in Wienke/Eberbach/Kramer/Janke (Fn. 9), 16 ff.

11 *Chadwick* in Gordin/Chadwick (Fn. 1), 25 ff.; *Merkel*, ZStW 2009, 919 ff.; *Lindner*, MedR 2010, 463 ff.; *Kunz*, MedR 2010, 471 ff.; *Gärditz*, PharmR 2011, 46 ff.; medizinische Perspektiven bei *Förstl*, Der Nervenarzt 2009, 840 ff.; *Gründer/Bartsch*, Der Nervenarzt 2014, 1536 ff.; s. aus medizinethischer Sicht *Groß* in Wienke/Eberbach/Kramer/Janke (Fn. 9), 85 ff. sowie umfassend die Beiträge in *Schöne-Seifert/Talbot/Opolka/Ach* (Hrsg.), Neuro-Enhancement – Ethik vor neuen Herausforderungen, 2009; philosophische Implikationen für die Vorstellung des „guten Lebens" bei *Glockentöger/Bittner/Fangerau*, Jahrbuch für Wissenschaft und Ethik 2012, 71, 84 ff.

12 Im Folgenden wird eine grobe Unterscheidung zwischen Eingriffen in den Körper sowie dem Einsatz von Implantaten (IT-Enhancement) einerseits und dem Einsatz externer Hilfsmittel (Robotik andererseits vorgenommen. Die Grenzen werden perspektivisch allerdings verschwimmen, wenn beispielsweise Roboter durch neuronale Verbindungen dauerhaft mit dem menschlichen Körper verbunden werden; dazu noch unten 4.2.1.

13 Während die „normale" Übertragung menschlicher Organe eher nicht im Sinne eines Enhancements verstanden wird, werfen Xenotransplantationen und künstlich hergestellte Organe ähnliche ethische und rechtliche Probleme auf.

14 Der erste Schrittmacher wurde etwa schon im Jahre 1958 durch *Ake Senning* implantiert, s. *http://www.cardiovascmed.ch/docs/2011/2011-04/2011-04-016.PDF.*

15 S. zur Entwicklung *Fröhlig/Carlsson/Jung/Koglek/Lemke/Markewitz/Neuzner*, Herzschrittmacher- und Defibrillator-Therapie, 2. Aufl. 2013.

16 *Rybak* in Goss/Middeke/Mengden/Smetak (Hrsg.), Praktische Telemedizin in Kardiologie und Hypertensiologie, 2009, 60.

17 *Wellnhofer/Jehle* in Jehle/Czeschik/Freund/Wellnhofer (Hrsg.), Medizinische Informatik Kompakt, 2014, 448 f.

18 *Wellnhofer/Jehle*, (Fn. 17) 449.

19 S. zu den technischen Hintergründen z.B. die Beiträge in *Krauss/Volkmann* (Hrsg.), Tiefe Hirnstimulation, 2004; *Vesper/Slotty*, Der Nervenarzt 2014, 169 ff. m.w.N.; ethische Probleme werden diskutiert z.B. von *Groß* in Wienke/Eberbach/Kramer/Janke (Fn. 9), 88 ff. und in den Beiträgen in Deutscher Ethikrat (Hrsg.), Der steuerbare Mensch, 2009; aus rechtlicher Sicht *Katzenmeier/Schmitz-Luhn* in Kern/Lilie (Hrsg.), FS zum 70. Geburtstag von Gerfried *Fischer*, 2010, 115 ff. sowie umfassend *Prütting*, Rechtliche Aspekte der Tiefen Hirnstimulation, 2013.

20 Z.B. *Groß* in Wienke/Eberbach/Kramer/Janke (Fn. 9), 90 f. m.w.N.; *Synofzik*, Der Nervenarzt 2013, 1175 ff.; s.a. die Nachweise bei *Beck* in dies. (Hrsg.), Jenseits von Mensch und Maschine, 2012, 10 ff. Eine Untersuchung mit 65 Probanden ergab z.B. einen leicht positiven Effekt der

c) Okular- und Cochlea-Implantate

Auch der Bereich der Sinnesorgane scheint für IT-Implantate vielversprechend. Künstliche Augäpfel oder Retina-Implantate könnten in der Zukunft Blinden das Sehen ermöglichen; entsprechendes gilt für Implantate zur Verbesserung oder Wiederherstellung der Hörfähigkeit (vor allem Cochlea-Implantate).[21] Die technisch-medizinische Herausforderung dürfte insoweit insbesondere die Verbindung mit den entsprechenden Nerven zu sein. Ist dies gelungen, so wäre ein weiterer Bereich des Enhancements im engeren Sinne eröffnet, weil die Sensorik selbst technisch praktisch beliebig moduliert werden kann. Mit anderen Worten wäre es relativ unproblematisch möglich, mit künstlichen Augen Infrarotstrahlen oder mit künstlichen Ohren Ultraschallwellen zu erfassen und an die entsprechenden Nervenenden weiterzuleiten.[22]

d) Prothesen

Künstliche Gliedmaßen funktionieren schon heute in vielen Bereichen nicht nur rein physikalisch-mechanisch, sondern auch mit Informationstechnologie. Dies wird sich in Zukunft weiter verstärken, insbesondere im Bereich feinmotorischer Aktivitäten, also beispielsweise beim Greifen mit den Fingern. Im Unterschied zum Gehen, das mit rein mechanischen Unterschenkelprothesen gut bewerkstelligt werden kann, erfordern solche komplexen Vorgänge – wie auch immer geartete – Schnittstellen zum Nervensystem.[23]

e) Observations-Implantate

Die Datenerhebung über menschliche Körperzustände könnte sich in vielen Bereichen in der Zukunft in den Körper selbst verlagern. In der Nähe des Herzens angebrachte Implantate können kontinuierliche EKGs aufzeichnen, die an mobile Endgeräte des Patienten außerhalb des Körpers übertragen und dort weiter ausgewertet werden.[24] Die Überwachung und Nachsorge für Patienten mit solchen Implantaten kann aus der Ferne im Wege eines Telemonitorings erfolgen,[25] das auch bei Cochlea-Implantaten viele Verbesserungen ermöglichen würde.[26] Die Anbindung nach außen kann dabei entweder über hergebrachte drahtlose Nahfeldkommunikationstechnologien wie Bluetooth erfolgen, oder perspektivisch durch den Körper selbst. Erste Forschungen zu sog. „Smart Tatoos" versprechen, durch hauchdünne Implantate die menschliche Haut zum Ausgabegerät zu machen und etwa Daten über den Herzrhythmus, das Schlafverhalten oder Muskelaktivitäten anzuzeigen.[27]

f) Umfangreiche eHealth-Datenerfassung

In ihrer Gesamtheit könnten sich dauerhaft und temporär in den menschlichen Körper eingebrachte IT-Implantate, die beschriebenen Kommunikations- und Ausgabetechnologien, permanent mitgeführte Gesundheitsdatenspeicher wie Fitness-Armbänder und persönliche Endgeräte wie Smartphones zu einem „Wireless Body Area Network" verbinden. Ein solches Netzwerk enthielte dann eine Vielzahl von Daten über Fitness- und Gesundheitszustand, die Anzahl der täglich aufgenommenen Kalorien und der gemachten Schritte, den jeweiligen Aufenthaltsort, Daten über die Funktionstüchtigkeit von Organen, den Schlafrhythmus und vieles mehr.

2. Risiken für Technik und Mensch

Die datenschutzrechtlichen Implikationen der beschriebenen technischen Innovationen sind offensichtlich. Hinzu treten IT-sicherheitstechnische Probleme, die in naher Zukunft eine erhebliche Relevanz erhalten könnten.

a) Anfälligkeit von IT-Lösungen

Schon die Funktionsweise von Herzschrittmachern zeigt, dass entsprechende Vorkehrungen und Maßnahmen getroffen werden müssen. Die Geräte enthalten neben dem Mikroprozessor auch elektronische Datenspeicher (RAM, ROM), auf denen die Programminformationen und Diagnosedaten gespeichert werden. Eine Kommunikation mit externen Programmiergeräten zur Datenübertragung und Programmänderung wird durch die integrierte Telemetriefunktion ermöglicht.[28] Aufgrund der großen Datenmengen, die bei kardiologischen Untersuchungen entstehen, wird aus betriebswirtschaftlichen Gründen empfohlen, die Daten bei externen Dienstleistern zu speichern.[29] Dies bringt freilich neue Angriffs- und Missbrauchsmöglichkeiten mit sich. Mittels effektiver Verschlüsselung kann darauf hingearbeitet werden, dass nur berechtigte Personen (Leistungserbringer und je nach Situation die Patienten selbst) Zugriff auf die Daten haben.[30] Je mehr Abläufe telemedizinisch umgesetzt werden, umso wichtiger wird dabei der Einsatz von Ende-zu-Ende-Verschlüsselung.[31] Eine besondere Herausforderung stellt der Einsatz von Cloud-Diensten dar.[32] Wenn dieser mit immer längeren Speicherfristen einhergeht, entsteht die Gefahr der Kompromittierung der verwendeten Algorithmen. Die Speicherung ist deshalb nach Möglichkeit von vornherein zu begrenzen.[33]

b) Attraktivität des Datenpools

In Notsituationen werden behandelnde Ärzte in Zukunft direkt auf den Herzschrittmacher zugreifen, um sofort die Daten auslesen und bestmöglich behandeln zu können.[34] Durch technische Zugriffsmöglichkeit auf Implantate besteht jedoch immer die Gefahr eines unautorisierten Zugriffs oder eines Hackerangriffs. Schon im

Tiefen Hirnstimulation auf die Fahrtüchtigkeit von Parkinson-Patienten, s. *Buhmann* u.a., Neurology 2014, 32 ff. Insgesamt besteht hier offenbar noch erheblicher Forschungsbedarf.

21 S. z.B. *www.heise.de/-1920784.html*; aus medizinischer Sicht s. den Überblick bei *Carlson/Driscoll/Gifford/McMenomey*, Otolaryngologic clinics of North America 2012, 221 ff.; s.a. *Ruf* (Fn. 9), 29; *McGee* in Gordijn/Chadwick (Fn. 1), 207 ff.

22 *Eberbach* in Wienke/Eberbach/Kramer/Janke (Fn. 9), 8.

23 Zu den entsprechenden Forschungen im Bereich der Neuroprothetik s. *Stieglitz*, Bundesgesundheitsbl 2010, 783 ff.

24 S. die Beispiele bei *Theißen*, Risiken informations- und kommunikationstechnischer (IKT-)Implantate im Hinblick auf Datenschutz und Datensicherheit, 2009, 25.

25 S. die Empfehlungen der AGs „Rhythmologie" und „Telemonitoring" der Deutschen Gesellschaft für Kardiologie – Herz- und Kreislaufforschung e.V. (DGK), Der Kardiologe 2013, 181 ff.

26 S. *Krüger-Brand*, DÄ 2013, A-2014 (*www.aerzteblatt.de/archiv/148399*).

27 S. *http://www.dailydot.com/technology/tattoos-wearables/*.

28 *Kogolek* in Fröhlig/Carlsson/Jung/Koglek/Lemke/Markewitz/Neuzner (Fn. 15), 220.

29 *Schütze/Kamler* in Goss/Middeke/Mengden/Smetak (Fn. 16), 25.

30 *Schütze/Kamler* in Goss/Middeke/Mengden/Smetak (Fn. 16), 26.

31 *Wellnhofer/Jehle*, (Fn. 17), 452.

32 Zum Einsatz von Cloud Computing im Gesundheitswesen s. *Hornung/Sädtler*, DuD 2013, 148.

33 *Wellnhofer/Jehle*, (Fn. 17), 452.

34 *Talbot*, Die Herzschlag-Verschlüsselung, *http://www.heise.de/-197213.html*.

Jahre 2008 wiesen erste Untersuchungen auf die Möglichkeiten von IT-gestützten Angriffen auf Herzschrittmacher und Defibrillatoren hin.[35] Im Jahre 2012 stellte der Wissenschaftsdienst des US-Kongresses einen erheblichen Verbesserungsbedarf fest, um Sicherheitsmängel von IT-Implantaten zu vermeiden, insbesondere wenn diese einen direkten Einfluss auf vitale Körperfunktionen haben (Herz- und Hirnschrittmacher, Insulinpumpen etc.).[36] Auf einer wissenschaftlichen Konferenz im selben Jahr demonstrierte ein Sachverständiger mögliche Angriffe auf ungeschützte Körperimplantate. Über eine externe, drahtlose Datenverbindung manipulierte er eine Insulinpumpe so, dass diese eine sehr hohe Hormonmenge ausschüttete, die im Falle des realen Einsatzes unmittelbar zur Ohnmacht und körperlichen Schädigung des Trägers führen würde. Drahtlos steuerbare Defibrillatoren und Herzschrittmacher wurden informationstechnisch so verändert, dass sie einen tödlichen 830-Volt-Impuls auslösten.

c) Zentrale Aspekte der IT-Sicherheit

Herzschrittmacher sollen nun vor Hackerangriffen besser geschützt werden. Neben klassischen IT-Sicherheitsmaßnahmen werden dabei auch innovative Methoden erforscht, die sicherstellen sollen, dass bestimmte Zugriffe nur aus der Nähe vorgenommen werden. Hierzu lässt sich heispielsweise die Erfassung von Herzschlagmustern einsetzen.[37] Zur Funkkommunikation mit medizinischen Implantaten wie Schrittmachern wird als Mobilfunk-Standard Medical Implantable Communication (MIC) genutzt, wodurch der kurze Übertragungsweg mit der Kontrolleinheit wie etwa einem Gerät oder Smartphone hergestellt wird.[38] Bei derartigen Telemonitoring-Anwendungen bestehen besondere Herausforderungen hinsichtlich der Übertragbarkeit und der Speicherkapazität großer Datenmengen. Fraglich bleibt zudem, ob tatsächlich eine ordnungsgemäße Behandlung des Patienten aus der Ferne erfolgen kann.[39] Für eine ordnungsgemäße Behandlung essentiell sind die Integrität der Informationen sowie eine eindeutige Zuordnung zum Urheber (Authentizität). Dies kann durch elektronische Signaturen und Zeitstempel erreicht werden.[40]

Ein Problem der Telemedizin stellt zudem die Tatsache da, dass als mobiles, drahtloses Gateway häufig eigene Endgeräte der Patienten wie Smartphones verwendet werden.[41] Schadsoftwareangriffe auf diese Geräte beeinträchtigen dann auch die Übertragungssicherheit der medizinischen Daten.[42] Werden die Daten nicht nur mittels Smartphone übermittelt, sondern auch auf diesen gespeichert, drohen im Falle von Diebstahl oder sonstigem Abhandenkommen die Kompromittierung der Daten oder sogar der Datenverlust, wenn keine Backups vorhanden sind. Soll das eigene Smartphone im Rahmen der Telemedizin zum Einsatz kommen, so hedarf es einer besseren Absicherung der Geräte.

Je nach Art des Implantats und technischer Funktionsfähigkeit kommen schlussendlich spezifische Risiken dazu. So könnte es zu unmittelbaren Verhaltensbeeinflussungen mittels der tiefen Hirnstimularion kommen, die in Tierversuchen hereits in den 50er Jahren des letzten Jahrhunderts demonstriert wurden.[43] Man mag darüber streiten, ob es für derartige Manipulationen ein realistisches Angreifermodell[44] gibt und wie hoch dementsprechend ihre Wahrscheinlichkeit im praktischen Einsatz ist. Mit Blick auf die massiven Gesundheitsrisiken der entsprechenden Angriffe wäre es aber jedenfalls nicht zu rechtfertigen, Körperimplantate nicht mit IT-Sicherheitsvorkehrungen auszustatten, die dem Stand der Technik entsprechen.

III. Gemeinsamkeiten und aufgeworfene Rechtsfragen

Aus medizinischer Sicht adressieren die technischen Innovationen des IT-Enhancements völlig unterschiedliche Krankheitshilder, Indikationen, medizinische Fachdisziplinen und Behandlungsformen. Dennoch lassen sich Gemeinsamkeiten und übergreifend Rechtsfragen formulieren.

1. Wunsch und medizinische Indikation

Die Gründe für die Einführung und Verwendung liegen typischerweise im Bereich der medizinischen Versorgung. Hier stellen sich allgemeine Fragen der medizinischen Sinnhaftigkeit, der Indikationen und Kontraindikationen sowie der Kostensteigerungen und Kosteneinsparungen insbesondere im Verhältnis zu alternativen Behandlungsmethoden wie der dauerhaften Medikamentengabe.[45] Nicht-indizierte Einsatzmöglichkeiten wie die Steigerung von Leistungsvermögen und Wohlbefinden treten zunächst als Nebenwirkungen auf oder sind Ausdruck spezifischer, anfänglich vielleicht sogar eher ungerichteter Forschungsinteressen. Betrachtet man die sich stetig beschleunigende Verbreitung von Informationstechnologie und innovativen Anwendungen in allen menschlichen Lebensbereichen, so scheint allerdings die Prognose gerechtfertigt, dass der Bereich der IT-Implantate weitaus stärker als andere medizinische

35 *Halperin* u.a., 2008 IEEE Symposium on Security and Privacy, DOI 10.1109/SP.2008.31.

36 S. *United States Accountability Office*, Medical Devices. FDA Should Expand Its Consideration of Information Security for Certain Types of Devices, August 2012, *http://www.gao.gov/assets/650/647767.pdf*; zu vergleichbaren Risiken beim Einsatz von Telechirurgieroboterm s. *http://www.heise.de/tp/artikel/45/45090/1.html*.

37 S. *Talbot* (Fn. 34). Dabei wird mittels eines Prüfgeräts das Herzschlagmuster des Patienten gemessen. Zur selben Zeit misst auch das Implantat das Signal und übermittelt es drahtlos nach außen. Stimmen beide Signale überein, so ist sichergestellt, dass jemand auf das Implantat zugreift, der tatsächlich in Kontakt mit der Person steht.

38 *Wellnhofer/Jehle*, (Fn. 17), 459.

39 Im deutschen Recht existiert kein allgemeines Fernbehandlungsverbot. Verboten ist nach § 7 Abs. 4 MBO-Ä aber die ausschließliche Behandlung über Print- und Kommunikationsmedien, vgl. *Wellnhofer/Jehle*, (Fn. 17), 452 f.; näher *Scholz* in Spickhoff, Medizinrecht, 2. Aufl. 2014, § 7 MBO Rz. 14 ff. m.w.N.

40 S. im hiesigen Zusammenhang z.B. *Heydenreich/Jürgens/Trost*, Ophthalmologe 2009, 800, 803 f.

41 *Wellnhofer/Jehle*, (Fn. 17), 449.

42 S. *Wellnhofer/Jehle*, (Fn. 17), 454; allgemein BSI, Überblickspapier Smartphones, *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf?__blob=publicationFile*; zu den rechtlichen Rahmenbedingungen derartiger mobiler Gesundheitsanwendungen s. allgemein *Rübsamen*, MedR 2015, 485 ff.

43 S. zu den Studien u.a. von *José Delgado* („ferngesteuertes" Anheben von Gliedmaßen, Stoppen von Bewegungen etc.) *Horgan*, Scientific American 2005, 66 ff.

44 Dieses ist Ausgangspunkt für die Beurteilung der Erforderlichkeit technischer IT-Sicherheitsmaßnahmen, s. *Eckert*, IT-Sicherheit. Konzepte – Verfahren – Protokolle, 6. Aufl. 2014, 205, 207.

45 Die Gesamtkosten einer tiefen Hirnstimulation werden auf ca. 40.000 € geschätzt, s. die Nachweise bei *Prütting* (Fn. 19), 98. Die durchschnittlichen jährlichen Medikamentenkosten bei Parkinson-Patienten betrugen 2007 3.260 €, s. *Dodel/Spottke*, Nervenheilkunde 2007, 256 (258).

Innovationen zu einer nicht-indizierten Verwendung (Enhancement im engeren Sinne) tendieren wird.

Betroffene können sich also schon in naher Zukunft von IT-Implantaten nicht nur im medizinisch-indizierten Bereich eine Heilung oder Besserung erhoffen, sondern auch eine Verbesserung ihrer motorischen und kognitiven Leistungsfähigkeit ohne jegliche medizinische Indikation. Der medizinisch nicht-indizierte Einsatz von IT-Implantaten wirft deshalb die Frage auf, ob ein verfassungsunmittelbarer oder einfachgesetzlicher Anspruch des Einzelnen auf IT-Enhancement bestehen kann.[46]

2. Grundrechtliche Fragen

Grundrechtlich wirft das IT-Enhancement des Weiteren insbesondere Probleme für das Recht auf Leben und körperliche Unversehrtheit (Art. 2 Abs. 2 GG) und das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), bei weitreichenden Eingriffen auch für die Menschenwürde (Art. 1 Abs. 1 GG) auf.[47] Diese Grundrechte spielen – beispielsweise in Form des Selbstbestimmungsrechts des Patienten[48] – in jeder Behandlungssituation eine Rolle. Sie sind auch zu beachten, wenn es um die Frage geht, ob der Gesetzgeber aufgrund der beschriebenen Risiken oder wegen der Unsicherheit über die langfristigen (körperlichen und ethischen) Folgen IT-basierte Körperimplantate gänzlich verbieten kann. Ein allgemeines Verbot freiwillig durchgeführter, medizinisch erforderlicher Eingriffe wäre mit Blick auf das Grundrecht des Art. 2 Abs. 2 GG und die sozialstaatlichen Pflichten des Gesetzgebers im Bereich der Gesundheitsversorgung[49] nicht zu rechtfertigen. Deutlich komplexer ist die Frage, ob der Gesetzgeber das IT-Enhancements im engeren Sinne, also den nicht indizierten Bereich, regeln oder sogar verbieten könnte.[50]

Neben den klassischen Grundrechtsfragen der Behandlung sind es die Beteiligten im Gesundheitswesen seit vielen Jahren gewöhnt, dass ihre Tätigkeit das Recht auf informationelle Selbstbestimmung als besondere Ausprägung des allgemeinen Persönlichkeitsrechts betrifft.[51] Dies betrifft insbesondere die Pflicht zur Patientendokumentation, die eine standesrechtliche Berufspflicht (Berufsordnungen analog § 10 MBO-Ä) und Teil des Behandlungsvertrags ist (herkömmlich als vertragliche Nebenpflicht zum Arztvertrag konstruiert,[52] seit dem Jahre 2013 in § 630f BGB spezifisch geregelt). Durch den Einsatz leistungskräftiger und vernetzter informationstechnischer Systeme vervielfachen sich die Probleme der informationellen Selbstbestimmung. Außerdem treten zwei weitere Grundrechte hinzu, nämlich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (ebenfalls eine Ausprägung des allgemeinen Persönlichkeitsrechts)[53] und das Fernmeldegeheimnis (Art. 10 GG). Die damit verbundenen Auslegung- und Konkurrenzfragen sind bisher noch nicht einmal andiskutiert.[54]

3. Einfachgesetzliches Handling der Datenprofile

Auch auf der einfachgesetzlichen Ebene werden vielfältige Rechtsprobleme aufgeworfen. Das betrifft insbesondere den Bereich des Sozialrechts, in dem sich Fragen des Versorgungsauftrags der Gesetzlichen Krankenversicherung, aber auch des spezifischen Sozialdatenschutzes stellen. Je größer und aussagekräftiger die gewonnenen Datenmengen sind, desto größer wird das Interesse an den aus ihnen gewinnbaren Persönlichkeitsprofilen sein. Deren Nutzung kann im unmittelbaren Interesse des Patienten liegen, wenn Ärzte ihm individualisierte Präventionsmaßnahmen empfehlen. Wenn allerdings private Krankenversicherungen ihr Risiko erheblich genauer kalkulieren, Lebensversicherungen oder Banken an der persönlichen Lebenserwartung interessiert sind oder Arbeitgeber die statistische Wahrscheinlichkeit einer Berufsunfähigkeit berechnen, so sind die Risiken für die Betroffenen mit Händen zu greifen.[55]

Die Rechtsfragen beschränken sich indes nicht auf das Datenschutzrecht, sondern umfassen auch Standesrecht und vielfältige Fragen des Zivil- und Strafrechts.[56] Wenn der menschliche Körper auf komplexe Art und Weise mit technischen Artefakten interagiert, können Dritte zu Schaden kommen. Dies führt zu komplexen Haftungsproblemen. Zum einen können sich Gemengelagen aus Individual- und Produkthaftungsrecht ergeben, wenn ein Betroffener eine Prothese oder einen angeschlossenen Roboter steuert und es zu Fehlfunktionen kommt.[57] Noch komplizierter sind Fälle, in denen umgekehrt der menschliche Körper auf Impulse der Technik reagiert, wenn beispielsweise mittels der tiefen Hirnstimulation einzelne Aktionen ausgelöst oder als Nebenwirkung gefahrgeneigte Gemütszustände (Aggressivität, Kleptoma-

46 Näher hierzu *Hornung/Sixt*, Tagungsband, i.E. Verfassungsrechtlich wird man dies – jenseits von Fällen gleichheitswidriger Verweigerung -kaum bejahen können, weil schon für medizinisch indizierte Eingriffe enge Grenzen bestehen, s. BVerfGE 115, 25; dazu z.B. *Kingreen*, NJW 2006, 877 ff.; *Padé*, NZS 2007, 352 ff.

47 Zu den Fragen von Berufs- und Forschungsfreiheit s. in Bezug auf das Enhancement *Ruf* (Fn. 9), 184 ff., 301 ff.

48 Dieses wird seit BVerfG v. 22.9.1993 – 2 BvR 1732/93, BVerfGE 89, 120 (130) überwiegend in Art. 2 Abs. 2 GG verortet, s. *Zuck* in Quaas/Zuck Medizinrecht, 3. Aufl. 2014, § 2 Rz. 36; ebenso schon das Sondervotum in BVerfG v. 25.7.1979 – 2 BvR 878/74, BVerfGE 52, 131 (174 f.), wo die Senatsmehrheit noch auf Art. 2 Abs. 1 GG abstellt.

49 Dazu *Di Fabio* in Maunz/Dürig, GG, Art. 2 II 1 Rz. 94; *Zuck* in Quaas/Zuck (Fn. 48), § 2 Rz. 23 ff.

50 Ausführlich hierzu insbesondere aus verfassungsrechtlicher Sicht: *Hornung/Sixt*, Tagungsband.

51 Durch das BVerfG im Volkszählungsurteil (BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1) anerkannt; s. monographisch z.B. die Darstellungen und Nachweise aus öffentlich-rechtlicher Sicht bei *Albers*, Informationelle Selbstbestimmung, 2005; aus zivilrechtlicher Sicht bei *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006; zur Innovationsgeschichte s. *Hornung*, Grundrechtsinnovationen, 2015, 266 ff.

52 BGHZ 72, 132 (137); 85, 327 (329) in Abkehr von der vorherigen Rspr., die in ihr lediglich eine Gedächtnisstütze sah, s. BGH, VersR 1963, 168 f.; zur Neuregelung z.B. *Katzenmeier*, BGH v. 4.7.2013 – V ZB 151/12, NJW 2013, 1714 ff.

53 BVerfG v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = CR 2008, 306; zum Innovationsverlauf und der bisher eingeschränkten Rezeption s. *Hornung* (Fn. 51), 277 ff.

54 S. noch unten 4.2.1.

55 Erste Entwicklungen in diese Richtung sind Versicherungsmodelle, die Rabatte gegen die Übermittlung umfassender Profildaten gewähren. Dies plant etwa die Generali ab 2016, s. *www.heise.de/-2750276.html*.

56 S. den allgemeinen Überblick für das Enhancement bei *Eberbach* in Wienke/Eberbach/Kramer/Janke (Fn. 9), 19 ff.; zur Vertragstypologie s. *Kern/Richter*, ebd., 135 ff.; zur zivilrechtlichen Haftung *Ruf* (Fn. 9), 127 ff.; zur Strafbarkeit der Leistungserbringer im Falle von Selbst- und Fremdschädigungen durch die Patienten *Prütting* (Fn. 19), 112 ff.; zum Standesrecht ebd., 138 ff.

57 Hinzu treten eher klassische produkthaftungsrechtliche Fragen, die unlängst sogar den EuGH beschäftigt haben, s. EuGH v. 5.3.2015 – Rs. C-503/13, Rs. C-504/13, CR 2015, 716 = NJW 2015, 1163 (fehlerhafte Herzschrittmacher und implantierbare Cardioverte Defibrillatoren); dazu bereits *Backmann/Wagner*, MPR 2008, 29; zur Haftung für IT-sicherheitstechnische Risiken *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007; *Gruber*, KJ 2013, 356.

nie, Veränderungen des Sexualtriebs)[58] auftreten. Aus strafrechtlicher Sicht stellen sich hier Fragen von Schuldunfähigkeit und actio libera in causa.[59] Konfiguriert der Arzt den Schrittmacher, kann medizinrechtlich außerdem die Nachbetreuungspflicht mit dem Selbstbestimmungsrecht des Patienten in Konflikt kommen.[60]

Je nach Lebensbereich kommen spezifische Fragestellungen hinzu. Dies betrifft beispielsweise das Prüfungsrecht.[61] Offenbar nimmt der Konsum von Aufputschmittelkonsum zur Prüfungsvorbereitung zu.[62] So wird z.B. Ritalin von Gesunden konsumiert, um ihre Konzentrationsfähigkeit zu steigern. Schon bei dieser Form des Neuro-Enhancements, noch mehr jedoch bei leistungssteigernden IT-Implantaten,[63] wird sich das Problem der Chancengleichheit unter Prüflingen stellen – bis hin zu der Frage, ob die Prüfungsleistung unter Einfluss leistungssteigernder Substanzen überhaupt noch als eigene gewertet werden kann. Mit der fortschreitenden Technisierung der Kriegsführung könnten auch bei Soldaten Körperimplantate zur Steigerung der Gefechtsfähigkeit eingesetzt werden. Hierbei würde sich dann das Problem stellen, ob dienstrechtlich sogar eine Pflicht zum IT-Enhancement bestehen könnte.[64]

IV. Rechtsfragen von Datenschutz und Datensicherheit

Wichtige, für die medizinische Heilbehandlung neue rechtliche Besonderheiten ergeben sich durch den Einsatz von Informationstechnologie direkt im menschlichen Körper. Derzeit werden die technischen, sozialen und rechtlichen Probleme von Datenschutz und IT-Sicherheit vor allem für die vernetzten Strukturen und Anwendungen des Internets diskutiert. Perspektivisch könnte es dazu kommen, dass alle diese Probleme direkte, auch physische Auswirkungen auf die Identität und Integrität der Menschen haben.

1. Datenschutz

a) Besondere Risikolagen

Der Einsatz von Informationstechnologie ist seit vielen Jahren integraler Bestandteil des Gesundheitswesens. Dies betrifft im Bereich der technisierten Medizin die Anamnese und Heilbehandlung selbst, insbesondere aber die begleitenden und nachgelagerten Datenflüsse. Je umfangreicher die Pflicht zur Dokumentation des Behandlungsgeschehens wird[65] und je mehr die Leistungserbringer im Rahmen von Überweisungen oder Konsiliarbehandlungen diese Dokumentationen austauschen müssen, desto wichtiger wird der Einsatz der Datenverarbeitungssysteme für den Alltag der Beteiligten. Mit der Einführung der elektronischen Gesundheitskarte und der sie umgebenden Telematik-Infrastruktur[66] versucht der Gesetzgeber seit einigen Jahren, die Datenflüsse unter Wahrung der informationellen und sonstigen Selbstbestimmung der Patienten zu ermöglichen und zu regeln. Das in der Endphase der Gesetzgebung befindliche E-Health-Gesetz[67] setzt diesen Weg fort, adressiert Fragen von IT-Implantaten jedoch nicht.

Gesundheitsinformationen gehören zu den sensibelsten personenbezogenen Daten. Es handelt sich um besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG), die erhöhten datenschutzrechtlichen Anforderungen unterliegen. Einwilligungen müssen sich explizit auf diese Daten beziehen (§ 4a Abs. 3 BDSG), vielfach ist eine Vorabkontrolle durchzuführen (§ 4d Abs. 5 Satz 2 Nr. 1 BDSG) und es gelten höhere Anforderungen an die Erhebung und Verwendung (§ 13 Abs. 2, § 14 Abs. 5 und Abs. 6, § 16 Abs. 1 Nr. 2 Satz 2, § 28 Abs. 6 bis 9, § 29 Abs. 5, § 30 Abs. 5, § 30a Abs. 1 Satz 2 und § 42a Satz 1 Nr. 1 BDSG). Die besondere Schutzbedürftigkeit kommt auch in mehreren Alternativen von § 203 Abs. 1 StGB zum Ausdruck.

Im Fall von IT-Implantaten treten weitere Faktoren hinzu. Üblicherweise setzt die Erhebung von Gesundheitsdaten eine externe Beobachtung eines Menschen, eine Äußerung seinerseits oder eine Erhebung bei Dritten voraus. Dagegen wird im Fall von Implantaten direkt auf den menschlichen Körper zugegriffen. Dies hat insbesondere bei Neurodaten eine besondere Qualität, weil es eine entsprechende Verbindung zwischen dem datenschutzrechtlich Betroffenen (§ 3 Abs. 1 BDSG) und seinen personenbezogenen Daten in dieser Form ansonsten nicht gibt.[68] Ob und in welchem Umfang Informationen aus dem Inneren des Menschen nach außen kommuniziert werden, ist bisher eine höchstpersönliche Entscheidung des Einzelnen. Durch die unmittelbare Erhebung aus dem Körper (besonders aus dem Gehirn) wird ihm die Chance zur Selbstdarstellung, einschließlich die zur Lüge genommen. Schweigen und Unwahrheit können jedoch in bestimmten Situationen ethisch legitim[69] und rechtlich zulässig[70] sein. Diese Wertungen könnten perspektivisch in Gefahr geraten.

Die dauerhafte, unmittelbare Verbindung mit der Person führt überdies wie andere persistente Identifizierungsmerkmale zu datenschutzrechtlichen Risiken des Trackings und der Bildung von Persönlichkeitsprofilen.[71]

58 Derartige Nebenwirkungen sind zumindest in einigen Fällen beobachtet worden, s. *Friedrich* in Manzeschke/Zichy (Hrsg.), Therapie und Person, 55 f.; *Brukamp*, ebd., 140; *Ruf* (Fn. 9), 31; *Witt*, Ethik Med 2013, 5, 6 f.; s.a. ebd. zu den Auswirkungen auf die personale Identität der Patienten.

59 S. *Beck* in Spranger (Hrsg.), Aktuelle Herausforderungen der Life Science, 2010, 113 f.

60 *Katzenmeier/Schmitz-Luhn* (Fn. 19), 122 f.

61 S. für Psychopharmaka *Gärditz*, PharmR 2011, 46, 51 f.; für die tiefe Hirnstimulation *Prütting* (Fn. 19), 224 ff.

62 *Galert/Bublitz/Heuser/Merkel/Repantis/Schöne-Seifert/Talbot*, Gehirn&Geist 2009, 1; *Glockentöger/Bittner/Fangerau*, Jahrbuch für Wissenschaft und Ethik 2012, 71 ff.

63 Hier mag es ggf. möglich sein, diese während der Prüfung auszuschalten oder so zu konfigurieren, dass lediglich ein „normales" Leistungsniveau erreicht wird. Ob dies technisch umsetzbar ist, ist derzeit aber völlig offen.

64 Zu einer Pflicht zum IT-Enhancement und einer möglichen Schutzpflicht des Gesetzgebers s. *Hornung/Sixt*, Tagungsband.

65 Zur rechtlichen Verortung s.o. 3.

66 Dazu z.B. *Hornung*, Die digitale Identität, 2005, v.a. 207 ff., 246 ff., 362 ff.; *ders.* in Anzinger/Hamacher/Katzenbeisser (Hrsg.), Schutz genetischer, medizinischer und sozialer Daten als multidisziplinäre Aufgabe, 2013, 51 ff.

67 Gesetzentwurf der Bundesregierung für Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen, BT-Drucks. 18/5293.

68 Zu den datenschutzrechtlichen Implikationen s. *Hallinan/Schütz/Friedewald/de Hert*, Surveillance & Society 2014, 55 ff.

69 *Kants* Versuch, für die Lüge das Gegenteil nachzuweisen („Über ein vermeintes Recht aus Menschenliebe zu lügen", Akademie-Ausgabe Band VIII, 423 ff.) wird ganz überwiegend und zu Recht zurückgewiesen.

70 Es gibt keine allgemeine Rechtspflicht zur Kommunikation und auch kein allgemeines Lügeverbot. In bestimmten Situationen besteht umgekehrt ein Recht zu Schweigen (bekanntestes Beispiel: nemo tenetur se ipsum accusare) oder sogar zur Lüge (etwa bei unzulässigen Fragen des Arbeitgebers im Bewerbungsgespräch) s. den Überblick bei *Armbrüster* in MünchKomm/BGB, § 123 Rz. 41 ff. m.w.N.).

71 Dazu im hiesigen Kontext *Theißen* (Fn. 24), 59 ff.

Wenn der Körper selbst als mobiles Endgerät fungiert, gerät er überdies in die Reichweite der Vorratsspeicherung von Telekommunikations-Verkehrsdaten. Diese derzeit wieder neu diskutierte Maßnahme zielt zwar auf herkömmliche Endgeräte. Da sie jedoch an die Datenübermittlung mittels Telekommunikation anknüpft, besteht durch die Entwicklung zum Ubiquitous Computing die Gefahr, dass die Speicherpflicht ohne weitere Entscheidung des Gesetzgebers in neue Lebensbereiche „hineinwächst".[72]

Besondere Risikolagen entstehen schließlich durch das Aufkommen neuer Akteure. Durch die Analyse großer Datenmengen (Big Data) werden Erkenntnisse über statistische Zusammenhänge und künftige Entwicklungen möglich, die Aussagen übet individuelle Risiken und Krankheitsverläufe zulassen. Erkennbar ist ein allgemeiner Trend zur Nutzung derartiger Erkenntnisse, beispielsweise im Bereich der polizeilichen Datenverarbeitung („predictive policing", etwa zur Entdeckung und Vorhersage von Schwerpunkten bei Wohnungseinbrüchen).[73] Die analoge Entwicklung einer „predictive medicine" verspricht Vorteile im Bereich der Vorsorge und Früherkennung, führt aber zugleich zu Risiken für diejenigen Betroffenen, denen mit einer hohen Wahrscheinlichkeit künftige Krankheiten vorhergesagt werden.

b) Einfachgesetzliche Schutzinstrumente

Wenn die entsprechenden Daten nicht anonymisiert oder pseudonymisiert werden (beispielsweise im Rahmen von Forschungsvorhaben), greifen die allgemeinen Regelungen des Datenschutzes im Gesundheitswesen.[74] Zunächst ist die verantwortliche Stelle (§ 3 Abs. 7 BDSG) zu bestimmen. Dies ist nicht der Betroffene selbst, auch wenn er die entsprechenden Implantate in seinem Körper mit sich führt und gegebenenfalls sogar teilweise bedient. Vielmehr wird regelmäßig der behandelnde Leistungserbringer im Rahmen einer dauerhaften Administration des jeweiligen Systems verantwortlich im Sinne des Datenschutzrechts sein. Durch die zunehmende Vernetzung kommen allerdings weitere Akteure hinzu. Dies betrifft insbesondere die Hersteller der entsprechenden Systeme, die im Rahmen von Wartungsverträgen, Notfall-Hotlines und anderen Angeboten viel stärker als bei bisherigen Medizinprodukten ins Spiel kommen werden. Soweit im Rahmen derartiger Dienstleistungen personenbezogene Daten anfallen, stellt sich die Frage einer gemeinsamen datenschutzrechtlichen Verantwortung mit den Leistungserbringern. Diese kann in Teilen vertraglich ausgestaltet werden, so dass auch eine Auftragsdatenverarbeitung nach § 11 BDSG in Betracht kommt.[75]

Rechtliche Grundlage für die entsprechenden Datenverarbeitungsvorgänge sind der Behandlungsvertrag (§ 28 BDSG) und die informierte Einwilligung des Betroffenen (§ 4 Abs. 1 und § 4a BDSG). Bei der Einwilligung ergeben sich dabei keine Unterschiede zwischen dem indizierten und dem nicht-indizierten IT-Enhancement,[76] wohl aber hinsichtlich § 28 BDSG. Dieser enthält erhöhte Anforderungen an die Verarbeitung von Gesundheitsdaten in § 28 Abs. 6 und Abs. 7 BDSG. § 28 Abs. 7 BDSG kann nicht-indizierte Eingriffe nicht legitimieren, weil es nicht um einen Zweck der Gesundheitsvorsorge, medizinischen Diagnostik, Gesundheitsversorgung oder Behandlung oder Verwaltung von Gesundheitsdiensten geht. Da regelmäßig auch § 28 Abs. 6 BDSG nicht eingreifen wird, ist im Ergebnis stets die Einwilligung erforderlich.

Eine zusätzliche Einschränkung ergibt sich für die Gesetzlichen Krankenkassen. Das Bundessozialgericht begreift die datenschutzrecbtlichen Normen des SGB V als abschließend nnd nicht durch Einwilligungen erweiterbar.[77] Die Krankenkassen werden deshalb auch die durch IT-Implantate generierten Daten nut auf der Basis gesetzlicher Ermächtigungsgrundlagen erheben und verwenden dürfen.

Die geltenden datenschutzrechtlichen Bestimmungen sind Ausdruck einer Reihe allgemeiner Schutzinstrumente, die auch für das IT-Enhancement gelten: Transparenz, Erforderlichkeit der Datenverarbeitung, Zweckbindung der erhobenen Daten, Pflicht zur technisch-organisatorischen Datensicherheit, Betroffenenrechte (insbesondere das Recht auf Auskunft).[78] Diese müssen risikoadäquat umgesetzt werden, das heißt unter Berücksichtigung der besonderen Sensibilität der Daten und der Einflüsse und Interessen der genannten weiteren Akteure.

Auf einfachgesetzlicher Ebene werden überdies datenschutzrechtliche Regelungen relevant werden, die bisher im Gesundheitswesen keine oder nur eine untergeordnete Rolle gespielt haben. So ist die Bestimmung zu „mobilen personenbezogenen Speicher- und Verarbeitungsmedien" (§ 6c BDSG) durch den Gesetzgeber zwar für personalisierte Chipkarten eingeführt worden, jedoch so allgemein formuliert, dass sie auch implantierte Mikrochips mit entsprechenden Speicher-und Verarbeitungskapazitäten umfasst.[79] Damit werden insbesondere Informationspflichten hinsichtlich der Funktionsweise des Implantats, der Betroffenenrechte und der bei Verlust oder Zerstörung zu treffenden Maßnahmen ausgelöst (§ 6c Abs. 1 BDSG), eine Pflicht der verantwortlichen Stelle zur unentgeltlichen Bereitstellung der für die Wahrnehmung des Auskunftsrechts erforderlichen Geräte und Einrichtungen statuiert (§ 6c Abs. 2 BDSG) und die Erkennbarkeit von Kommunikationsvorgängen vorgegeben, die auf dem Implantat eine Datenverarbeitung auslösen (§ 6c Abs. 3 BDSG).[80]

72 S. dazu *Hornung* in Hempel/Krasmann/Bröckling (Hrsg.), Sichtbarkeitsregime, Leviathan Sonderheft 25/2010, 245, v.a. 254.

73 In der letzten Zeit haben mehrere Landespolizeibehörden entsprechende Softwaresysteme angeschafft, s. *http://www.zeit.de/digital/datenschutz/2015-03/predictive-policing-software-polizei-precobs;* näher *Gluba*, Kriminalistik 2014, 347 ff.; aus US-Perspektive *Ferguson*, Emory Law Journal 2012, 259 ff. Nach einer Studie des LKA Niedersachsen ist der praktische Nutzen bisher noch nicht empirisch feststellbar, s. *https://netzpolitik.org/wp-upload/LKA_NRW_Predictive_Policing.pdf.*

74 S. dazu z.B. die Beiträge in *Kingreen/Kühling* (Hrsg.), Gesundheitsdatenschutzrecht, 2015.

75 S. zu den damit verbundenen Fragen des Outsourcings im Gesundheitswesen *Jandt/Roßnagel/Wilke*, NZS 2011, 641; *Paul/Gendelev*, ZD 2012, 315; *Menzel*, RDV 2013, 59.

76 S. zur datenschutzrechtlichen Einwilligung ausführlich *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013.

77 BSGE 102, 134; s. z.B. *Brisch/Laue*, AG Berlin-Mitte v. 23.10.2008 – 16 C 123/08, CR 2009, 265 ff.; *Kühling/Seidel*, GesR 2010, 231 ff.; *Leisner*, NZS 2010, 129 ff.; *Schneider*, VSSR 2009, 381 ff.

78 S. näher z.B. *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 70 ff.; *Simitis* in ders. (Hrsg.), BDSG, 8. Aufl. 2014, Einl. Rz. 30 ff.; *Trute* in Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 2.5 Rz. 32 ff., jeweils m.w.N.

79 Es ist derzeit unklar, ob die Norm nach Abschluss der europäischen Reform (dazu statt vieler *Hornung* in Scholz/Funk (Hrsg.), DGRI Jahrbuch 2012, 2013, 1 ff. m.w.N.) weitergelten wird. Eine wahrscheinliche Variante ist, dass dies zumindest im Rahmen von Öffnungsklauseln für nationale Regelungen im Gesundheits- und Sozialdatenschutzrecht möglich sein wird (s. derzeit Art. 81 und Art. 82a der Entwürfe von Parlament und Rat).

80 S. näher zu den Anforderungen *Hornung* (Fn. 66), 253 ff.; *ders.*, DuD 2004, 15 ff.

c) Notwendigkeit neuer Regelungen?

In Umsetzung seiner verfassungsrechtlich begründeten Schutzpflicht ist der Gesetzgeber aufgefordert, in Abhängigkeit vom konkreten Schutzbedarf die Persönlichkeitsrechte der Grundrechtsträger durch besondere gesetzliche Vorgaben zu schützen. Bisher erscheinen die technischen Funktionsweisen der verschiedenen Körperimplantate zu heterogen und die mit ihnen verbundenen persönlichkeitsrechtlichen Risiken noch zu wenig konturiert, um spezifische, auf die konkrete technische Funktionsweise bezogene datenschutzrechtliche Bestimmungen vorzugeben. Dies könnte sich jedoch in absehbarer Zeit ändern.

Rechtspolitisch könnte sich ein entsprechender Handlungsbedarf insbesondere aus einem Vergleich mit den sehr detaillierten Regelungen zur elektronischen Gesundheitskarte und zur Telematik-Infrastruktur ergeben.[81] Aus ihnen wird deutlich, dass die besonderen Risikolagen der Datenverarbeitung im Gesundheitswesen eine relativ hohe Regulierungsdichte erfordern. Unter dem Blickwinkel des Rechts auf informationelle Selbstbestimmung könnten IT-gestützte Körperimplantate perspektivisch mindestens ebenso große Risiken bergen wie die Datenerhebung, -verarbeitung und -nutzung medizinischer Informationen auf oder mittels der elektronischen Gesundheitskarte. Wenn der Gesetzgeber es dort für erforderlich gehalten hat, detaillierte Zugriffsregeln, technische Schutzmaßnahmen, Instrumente gegen den Datenmissbrauch und sogar besondere Straf- und Ordnungswidrigkeitentatbestände vorzusehen,[82] so spricht zumindest mittelfristig einiges für analoge Regelungen zum IT-Enhancement. Hierfür wird der deutsche Gesetzgeber voraussichtlich auch nach Abschluss der aktuellen europäischen Reform regelungsbefugt sein, weil diese Öffnungsklauseln für das nationale Gesundheitsdatenschutzrecht enthalten soll.[83]

2. IT-Sicherheit

Datenschutz und IT-Sicherheit sind eng miteinander verbunden, aber nicht identisch.[84] Die Überwindung von IT-Sicherheitsmaßnahmen[85] kann dazu dienen, widerrechtlich auf personenbezogene Daten zuzugreifen. Sie kann aber auch ohne einen solchen Zugriff die Manipulation eines IT-Systems bezwecken und dadurch den Nutzer – hier also den Träger eines IT-gestützten Körperimplantats – schädigen.

a) Grundrechtliche Konkurrenzsituationen

Am Beispiel der Eingriffe in die IT-Sicherheit lässt sich besonders plastisch demonstrieren, welche neuen Grundrechtsfragen das IT-Enhancement aufwirft. Wird von außen gegen den Willen des Trägers auf die Implantate zugegriffen, so gehen unterschiedliche Formen des grundrechtlichen Integritätsschutzes eine völlig neuartige Verbindung ein: Betroffen sind die Integrität des Körpers, die menschliche Persönlichkeit und das informationstechnische System – eine Situation, in der die zunächst etwas reißerisch anmutende Frage des Schutzes eines „Cyborgs" aus grundrechtssystematischer Sicht tatsächlich Sinn ergeben könnte.[86]

aa) Unberechtigter Zugriff auf Implantat

Dies soll am Beispiel eines rechtswidrigen externen Zugriffs auf einen Hirnschrittmacher nebst der Veränderung der auf ihm gespeicherten Daten und Steuerhefehle verdeutlicht werden.[87] Da diese Daten personenbezogen sind, handelt es sich um einen Eingriff in das Recht auf informationelle Selbstbestimmung. Überdies wird es sich – zumindest in Zukunft – bei den entsprechenden Schrittmachern um informationstechnische Systeme handeln, die „allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten".[88] Dies eröffnet den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[89] Das BVerfG hat herausgearbeitet, dass eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht, soweit der Betroffene das informationstechnische System als „eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt".[90] Dies muss erst recht gelten, wenn das System dauerhaft mit dem menschlichen Gehirn verbunden ist. Dass die tiefe Hirnstimulation Einfluss auf das menschliche Verhalten nimmt und man deshalb etwas spitzfindig einwenden könnte, dass hier nicht der Betroffene das System, sondern umgekehrt das System den Betroffenen „nutzt", spricht nicht gegen, sondern gerade für die Eröffnung des Schutzbereiches und einen besonders schweren Eingriff.

bb) Betroffene Grundrechte

Durch die Datenveränderung wird des Weiteren regelmäßig ein Eingriff in die körperliche Unversehrtheit vorliegen. Dies ist spätestens dann der Fall, wenn der Schrittmacher durch eine Manipulation in veränderter Art und Weise auf den Körper einwirkt.[91] Im Fall der Implantierung permanenter, mit neuronalen Strukturen verbundener IT-Systeme spricht überdies viel dafür, diese auch rechtlich als Teil des Körpers zu verstehen. Dies nimmt die überwiegende Meinung für fest verbundene Implantate wie Herzschrittmacher an, auch wenn diese operativ entfernt werden können.[92] Freilich führen sol-

81 S. Fn. 66.
82 Zu den Schutzinstrumenten s. insoweit *Hornung* (Fn. 66), 228 ff.
83 S. Fn. 79.
84 S. zum Verhältnis allgemein *Ernestus* in Simitis (Fn. 78), § 9 Rz. 2 f. m.w.N.; *Heibey* in Roßnagel (Fn. 78), Kap. 4.5.
85 S.o. 2.2.
86 Zu den Problemen des graduellen Übergangs zwischen Mensch und „Mensch-Maschine-Hybrid" s. *Heilinger/Müller*, Jahrbuch für Wissenschaft und Ethik 2007, 21 (24 ff.).
87 Die Frage der unmittelbaren Anwendung der folgenden Grundrechte (beim Zugriff durch staatliche Stellen) und der etwaigen mittelbaren Drittwirkung (beim Zugriff durch Private) bleiben im Folgenden außer Betracht. Demonstriert werden soll lediglich die Problematik der Grundrechtskonkurrenzen.
88 So die Schutzbereichsbeschreibung in BVerfG v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = CR 2008, 306 (314).
89 Ebenso wie im Fall der sog. Online-Durchsuchung liegt in dem externen Zugriff demgegenüber kein Eingriff in Art. 10 GG, weil der Eingriff zwar mittels Telekommunikation erfolgt, aber nicht auf Inhalt oder Umstände derselben zielt. Anders wäre es bei Eingriffen in die Datenübermittlung zwischen Steuergerät und Implantat zu beurteilen.
90 BVerfG v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 (315) = CR 2008, 306.
91 S. allgemein für das Neuro-Enhancement *Lindner*, MedR 2010, 463 (467.).
92 S. aus zivilrechtlicher Sicht *Stresemann* in MünchKomm/BGB, § 90 Rz. 28; *Fritzsche* in BeckOK/BGB, § 90 Rz. 31; aus strafrechtlicher Sicht *Eschelbach* in BeckOK/StGB, § 223 Rz. 15; differenzierend mit Blick auf den eintretenden Wandel zwischen Sache und Nicht-Sache *Eser/Bosch* in Schönke/Schröder, StGB, 29. Aufl. 2014, § 242 Rz. 20 f.; *Schmitz* in MünchKomm/StGB, § 242 Rz. 29.

che Überlegungen perspektivisch zu komplizierten Abgrenzungsproblemen, weil die Grenzen des Körpers fließend werden. Wenn Körperimplantate durch drahtlose Datenverbindungen mit externen Komponenten interagieren oder das Gehirn durch neuronale Schnittstellen ganze IT-Systeme steuert, so stellt sich die Frage, ob nicht zumindest im Fall der Unterstützung essenzieller Körperfunktionen auch derartige externe technische Artefakte im Rechtssinn Teil des menschlichen Körpers werden können und dementsprechend grund-, zivil- und strafrechtlich geschützt werden müssen.

Spätestens dann, wenn die Veränderung der Steuerungswirkung nicht nur nachrangige Körperfunktionen, sondern die Persönlichkeit betrifft (Gemütszustände, Verhaltensweisen etc.), ist daneben das allgemeine Persönlichkeitsrecht, in Extremfällen auch die Menschenwürde betroffen.[93]

Im Ergebnis sind bei externen Zugriffen auf IT-Implantate also mindestens vier Grundrechte anwendbar, die auf je spezifische Weise Facetten der physischen und psychischen menschlichen Persönlichkeit schützen. Wie diese Situation auf der Konkurrenzebene aufzulösen ist, ist bislang völlig offen. Hinsichtlich des Zusammenspiels zwischen dem Recht auf informationelle Selbstbestimmung und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme liegt dies hauptsächlich daran, dass das Verhältnis der beiden Grundrechte[94] insgesamt unklar ist.[95] Da das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme strengere Anforderungen an die Rechtfertigung von Eingriffen aufstellt, wird es – unabhängig von der dogmatischen Konstruktion – im Ergebnis jedenfalls die größere Rolle spielen. Im Übrigen ließe sich nach der Zielrichtung des Eingriffs differenzieren. Richtet dieser sich maßgeblich auf das Implantat als IT-System (also die in ihm gespeicherten Daten und seine Funktionen), wäre das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vorrangig. Geht es demgegenüber vorrangig um die Dimension der persönlichen Selbstbesrimmung und Lebenssphäre, liegt das allgemeine Persönlichkeitsrecht näher. Maßnahmen, die hauptsächlich physisch auf IT-Implantate wirken oder unmittelbarere Auswirkungen auf andere Körperteile haben, ließen sich dann nach dem Recht auf körperliche Unversehrtheit beurteilen. Vielfach wird freilich eine solche eindeutige Zuordnung kaum möglich sein.

b) Einfachgesetzliche Schutzinstrumente

Auch in Bezug auf die Probleme der Manipulation von Systemen des IT-Enhancements trifft den Gesetzgeber mit Blick auf die erläuterten Gefahren für die Grundrechte eine Schutzpflicht. Nach dem Urteil des BVerfG zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten umfasst der gesetzgeberische, grundrechtlich begründete Gestaltungsauftrag auch konkrete Regelungen zur IT-Sicherheit.[96]

Insoweit bieten sich insbesondere Instrumente zur Gefahrenvorsorge an. Dies sind allgemeine Fragen des Medizinprodukterechts, also der Vorabprüfung von Implantaten und Operationstechniken. Hier bestehen gesetzliche Anforderungen, die sich teilweise spezifisch auf „aktive implantierbare Medizinprodukte" beziehen (§ 7 Abs. 1, § 9 Abs. 1, § 12 Abs. 2, § 13 Abs. 1, § 22a Abs. 1 und § 23 MPG).

Implantate, die allein zu nicht-indizierten Zwecken des Enhancements vertrieben werden, fallen nicht in den Anwendungsbereich des Gesetzes (§ 2 Abs. 1 i.V.m. § 3 Nr. 1 MPG).[97] Für die datenschutzrechtlichen Anforderungen spielt dies freilich keine Rolle, da nach § 2 Abs. 4 MPG die Rechtsvorschriften über Geheimhaltung und Datenschutz unberührt bleiben und somit in jedem Fall anwendbar sind. Folglich sind IT-Sicherheitsmaßnahmen gem. § 9 BDSG[98] und der entsprechenden Anlage schon heute rechtlich verpflichtend. Allerdings fehlt es hier sowohl an spezifischen gesetzlichen Vorgaben als auch an technischen Standards.[99] Vielen Verantwortlichen im Medizinproduktebereich dürften diese Anforderungen deshalb nicht bekannt sein.

Überdies stellt sich die Frage, wer konkret die verantwortlichen Stellen oder Auftragsdatenverarbeiter sind, die die Pflichten aus § 9 BDSG treffen.[100] Dies werden nur in Ausnahmefällen die Hersteller nach § 3 Nr. 15 MPG sein, wenn sie beispielsweise als Dienstleister für Leistungserbringer entsprechende Systeme betreiben. Im Übrigen nimmt das geltende Datenschutzrecht die Entwickler und Hersteller von IT-Systemen allgemein viel zu wenig in die Pflicht.[101]

Nicht nur für IT-Implantate, sondern allgemein für vernetzte Medizinprodukte wären bereichsspezifische Pflichten zur Einhaltung von IT-Sicherheitsmaßnahmen deshalb sinnvoll.[102] Dasselbe gilt für das reine Enhancement. Dabei sind Anforderungen zu formulieren, die die besonderen Auswirkungen auf den Körper berücksichtigen. Aufgrund der erweiterten Erhebungs- und Verarbeitungskapazitäten dürfen entrsprechende Tests nicht nur die medizinische Wirksamkeit und die Vermeidung von Nebenwirkungen umfassen. Erforderlich sind ebenso Standards für die IT-Sicherheit (Zugriffsschutz, Verschlüsselung, Protokollierung etc.) und ihre effektive Prüfung.

Beides darf sich nicht auf die einmalige Zulassung und Kontrolle im Moment der Implantierung beschränken. Vielmehr wird in vielen Fällen schon aus Gründen der Erhaltung und Verbesserung der Funktionalität eine Wartung erforderlich sein, die auch etwaige Updates umfasst. Dies betrifft auch und gerade IT-Sicherheitsmaßnahmen. Regelungen entbalten insofern Normen über die Instandhaltung von Medizinprodukten (vor allem

93 Insbesondere bei Eingriffen in das Gehirn, s. *Lindner*, MedR 2010, 463 (466 f.); *Hilgendorf* in Joerden/Hilgendorf/Thiele (Hrsg.), Menschenwürde und Medizin, 2013, 867 ff.

94 Angesichts der klaren Schutzbereichsabgrenzung und eigenständigen Schrankendogmatik ist es gerechtfertigt, von selbständigen Grundrechten zu sprechen, s. *Hornung* (Fn. 51), 380 ff.

95 Zur Kritik an der Rechtsprechung des BVerfG s. insoweit z.B. *Britz*, DÖV 2008, 411 (412); *Volkmann*, DVBl. 2008, 590 (591 f.); *Böckenförde*, JZ 2008, 925 (927 f.); s.a. die Verteidigung zu diesem Punkt bei *Hoffmann-Riem*, JZ 2009, 1009 (1015 ff.).

96 BVerfGE 125, 260 (325 ff.); speziell zu dieser Frage s. *Hornung/Schnabel*, DVBl. 2010, 824 (829).

97 S. *Prütting* (Fn. 19), 207 ff.

98 Beziehungsweise (insbesondere im Krankenhausbereich) den entsprechenden landesrechtlichen Regelungen.

99 S. allgemein für vernetzte Medizinprodukte *Spyra*, MPR 2015, 15 (v.a. 18 ff.).

100 *Spyra*, MPR 2015, 15, 20, der für eine „Datenschutz-Compliance" des Medizinprodukte-Herstellers plädiert; zu den Problemen, die das Fehlen entsprechender Standards in der Praxis produziert, s. ebd., 21 ff.

101 Dazu *Hornung*, ZD 2011, 51 (52 ff.).

102 Das soeben verabschiede IT-Sicherheitsgesetz des Bundes vom 17.7.2015 (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, BGBl. I, 1324) erfasst zwar auch den Gesundheitssektor, aber nur hinsichtlich Kritischer Infrastrukturen (§ 2 Abs. 10 BSIG), nicht in Bezug auf einzelne Medizinprodukte.

§ 3 MPBetreibV) sowie § 33 Abs. 1 Satz 4 SGB V. Danach umfasst der Anspruch der Versicherten auf Versorgung mit Hilfsmitteln auch die notwendige Änderung, Instandsetzung und Ersatzbeschaffung von Hilfsmitteln, die Ausbildung in ihrem Gebrauch und, soweit zum Schutz der Versicherten vor unvertretbaren gesundheitlichen Risiken erforderlich, die nach dem Stand der Technik zur Erhaltung der Funktionsfähigkeit und der technischen Sicherheit notwendigen Wartungen und technischen Kontrollen. Diese allgemeinen Bestimmungen bedürfen mit Blick auf das IT-Enhancements der Konkretisierung und Fortentwicklung.

3. Vorläufige Bewertung der Regulierungsbedürftigkeit

Insgesamt ist erkennbar, dass der Einsatz von IT-Implantaten Regulierungsfragen aufwirft. Einige dieser Probleme sind bereits erkennbar, andere noch zu undeutlich für belastbare Aussagen. Da im Übrigen vielfach allgemeine Regelungen anwendbar sind, sind diese auf ihre Angemessenheit zu überprüfen und gegebenenfalls zu spezifizieren.

Im Bereich des Datenschutzrechts bestehen die Herausforderungen vor allem in der neuartigen Form der Datenerhebung und den Informationsflüssen zu Leistungserbringern und neuen Dienstleistern. Beides könnten in den größeren Kontext des Telemonitorings von Patienten (und gesunden, an Enhancement interessierten Betroffenen) gestellt und reguliert werden, indem rechtliche Zugriffsregeln aufgestellt und technisch abgesichert, Profilbildungen verhindert, Löschungspflichten definiert sowie Instrumente gegen den Datenmissbrauch implementiert werden.

Einige Fragen werden durch das Medizinprodukterecht abgedeckt, bedürfen aber einer Spezifizierung für IT-Implantate. Überdies ist näher zu analysieren, ob es dauerhaft angemessen ist, reine Enhancement-Systeme allein dem allgemeinen Produkthaftungs- und Datenschutzrecht zu überlassen. Vorgaben für die Erprobung technischer Implantate und ihre Evaluierung könnten sich auch auf die IT-Sicherheit erstrecken und in transparenten Verfahren (Datenschutzaudits)[103] Klarheit für die Betroffenen und die anwendenden Leistungserbringer erzeugen.

Von besonderer Bedeutung ist schließlich die Transparenz für die Betroffenen. Hier bieten die allgemeinen Aufklärungs- und Informationspflichten bereits einen relativ guten Schutz. Allerdings könnte beispielsweise die spezifische Informationspflicht für Implantate in § 10 MPBetreibV ausgebaut und auf reine Enhancement-Produkte erweitert werden.

V. Ausblick

Perspektivisch werden insbesondere die mit den Implantaten verbundenen weitreichenden Datenflüsse neue Rechtsfragen verursachen. Diese Übermittlungen werden zum einen innerhalb, zum anderen zunehmend auch außerhalb des hergebrachten Behandlungskontextes stattfinden.

Im ersten Bereich handelt es sich eher um graduelle Verschiebungen. Die behandelnden Leistungserbringer werden zunehmend Daten aus den Implantaten zur Kontrolle und Verbesserung der Behandlung erheben und diese im Rahmen der Konsiliarbehandlung und Überweisung an andere Leistungserbringer weitergeben. Auch Datenerhebungen zu Forschungszwecken kommen im Gesundheitswesen seit vielen Jahrzehnten standardmäßig vor. Mithilfe von IT-Implantaten werden aber neue Erhebungsmethoden möglich, die der Forschung aus ethischen Gründen bislang verschlossen waren. Dies betrifft insbesondere Erhebungen direkt aus dem menschlichen Gehirn.[104]

Neue Probleme stellen sich demgegenüber im zweiten Bereich, weil hier neu Akteure auftreten: neben den Krankenversicherungen[105] insbesondere die Hersteller der entsprechenden Implantate und Verfahren sowie die Krankenversicherungen. Bisher haben Medizinproduktehersteller typischerweise keinen direkten Kontakt zu den Patienten und erheben von diesen keine personenbezogenen Daten. Etwaige Verkaufs- und Marketingaktivitäten konzentrieren sich deshalb auf die Leistungserbringer. IT-gestützte Körperimplantate werden es in ihrer Vernetzung den Herstellern jedoch viel stärker als heute ermöglichen, direkt und unter völliger oder teilweiser Umgehung der behandelnden Leistungserbringer mit dem Patienten zu kommunizieren. Wie in anderen wirtschaftlichen Bereichen werden die Interessen der Hersteller dabei vielfältig sein und etwa die eigene Produktverbesserung, Standardberatungen und Notdienste, das Anbieten kostenpflichtiger Premium-Dienste (etwa über individuelle Gesundheitsleistungen)[106] oder die allgemeine Kundenbindung umfassen.

Auch eher praktische Probleme können im Ergebnis zu diesen fundamentalen Verschiebungen beitragen. Je komplexer die verwendeten technischen Systeme sind, desto wichtiger werden Fragen der Benutzbarkeit (Usability) und der technischen Kompetenz der Beteiligten. Dies betrifft die Patienten, die sich die technischen Fertigkeiten zur Bedienung der Geräte im Alltag aneignen müssen. Veränderungen ergeben sich aber auch für die Leistungserbringer. Es genügt für sie nicht mehr, die chirurgischen Fähigkeiten für den Eingriff mitzubringen. Insbesondere sensible Anwendungen wie die tiefe Hirnstimulation bedürfen einer exakten Konfiguration und Nachbetreuung, die außerhalb spezialisierter Krankenhausabteilung ein erhebliches Problem darstellen wird. Wenn die behandelnden Ärzte nicht über die entsprechenden Kompetenzen verfügen, werden sie selbst gezwungen, in Zweifelsfällen und bei technischen Problemen die Hersteller zu kontaktieren; dabei wird es in vielen Fällen erforderlich sein, Behandlungsinformationen an diese zu übermitteln. Wenn in dieser Situation letztlich die Akteure auf Herstellerseite die maßgeblichen Entscheidungen über die Konfiguration des IT-Systems und damit über den weiteren Verkauf der Behandlung fällen, würde dies die Verantwortlichkeiten erheblich beeinflussen.

103 Dazu grundlegend *Roßnagel*, Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung, 2000; mit Blick auf die europäische Reform *Hornung/Hartl*, ZD 2014, 219 ff.

104 S. *Engel/Moll/Fried/Ojemann*, Nature reviews Neuroscience 2005, 35 ff.; zu den Rechtsfragen s. *Prütting* (Fn. 19), 167 ff.

105 Die Datenflüsse zu den Gesetzlichen Krankenkassen sind im geltenden System des sozialrechtlichen Datenschutzes begrenzt und in den §§ 284 ff. SGB V rechtlich stark durchstrukturiert. Insbesondere im Rahmen der Tätigkeit des medizinischen Dienstes der Krankenkassen (MDK) nach §§ 275 ff. SGB V wird es aber auch insoweit zu neuen Datenübermittlungen kommen.

106 Zu diesen sog. „IGeL"-Leistungen s. aus rechtlicher Sicht z.B. *Clausen* in Terbille/Clausen/Schroeder-Printzen (Hrsg.), Münchner Anwaltshandbuch Medizinrecht, 2. Aufl. 2013, § 7 Rz. 301 ff.; *Schuldzinski*, VuR 2007, 428.

Dies könnte perspektivisch zu grundsätzlichen Veränderungen des Arzt-Patient-Verhältnisses führen, weil bisher der Arzt mit seinem überlegenen Wissen die Interessen seiner Patienten auch gegenüber anderen Akteuren im Gesundheitswesen wahrnimmt. Dies verschiebt sich, wenn nunmehr neue Akteure ins Spiel kommen und bisherige Informations- und Wissensmonopole aufgeweicht werden. Die Leistungserbringer verlieren also ein Stück weit ihre starke Position,[107] und es ist bisher unklar, welche konkreten Auswirkungen dies auf die Kommunikation mit den Patienten während des Behandlungsprozesses und den Heilungserfolgt insgesamt hat.

Die erweiterten Datenströme auch zu den Herstellern führen überdies zu der komplexen Frage, wem die durch Körperimplantate produzierten Daten eigentlich „gehören", wer also über sie verfügen und sie gegebenenfalls wirtschaftlich nutzen darf. Dieses Problem stellt sich auch in anderen Lebensbereichen wie dem vernetzten Automobil, in denen auf einmal neue Akteure mit innovativen Dienstleistungen ins Spiel kommen.[108] Das Problem der Verfügungsbefugnis stellt sich umso drängender, je mehr lokal (durch Implantate, Automobile, Endgeräte etc.) generierte Daten auf externen Server-Infrastrukturen des Cloud Computings gespeichert und weiterverarbeitet werden.

Viele dieser Fragen werden durch geltendes oder künftiges Datenschutzrecht determiniert werden. In vielen Fällen wird es auch im Interesse der Patienten sein, den Herstellern zur Verbesserung der Funktionalität, zur Wartung etc. den Zugriff auf ein IT-Implantat zu ermöglichen. Am Horizont droht indes die Gefahr, dass Ärzte wegen des unterlegeneu Wissens und der nicht oder nur unzureichend vorhandenen IT-Kompetenz zu ausführenden Stellen der Hersteller werden. Einer solcben Entwicklung ist mit Blick auf die besondere Bedeutung der Vertraulichkeitsbeziehung zwischen Arzt und Patient für den medizinischen Heilerfolg und die Funktionsfähigkeit des Gesundheitswesens insgesamt[109] vorzubeugen. Die Frage nach dem Cyborg bleibt insoweit immer die Frage nach dem Menschen.[110]

107 Dies unterscheidet die hier beschriebenen Entwicklungen von anderen Risiken für das Arzt-Patient-Verhältnis, wenn beispielsweise Ärzte ihr überlegenes Wissen nutzen, um zweifelhafte „IGeL"-Leistungen (s. Fn. 106) anzubieten. Zur verfassungsrechtlichen Perspektive aus Ärztesicht näher *Ruf* (Fn. 9), 301 ff.

108 Dazu *Hornung/Goeble*, CR 2015, 265 ff.; *Hornung*, DuD 2015, 359 ff.

109 S. BVerfGE 32, 370 (380); EGMR, Z ./. Finnland, Urteil v. 25.2.1997 (*http://www.echr.coe.int/Eng/Judgments.htm*), Abs. 95.

110 S. die Formulierung bei *Heilinger/Müller*, Jahrbuch für Wissenschaft und Ethik 2007, 21, v.a. 33 ff.