Telemedizin und Datenschutz

Wilfried Berg
Abdruck mit freundlicher Genehmigung, erschienen in „Medizinrecht", Springer, Heft 8/2004

1 Grundfragen zum Datenschutz und zum Recht auf informationelle Selbstbestimmung

1.1 Widersprüchlichkeit in der Bewertung der Privatsphäre

Am 15. Dezember 1983, also gewissermaßen am Vorabend des von George Orwell im Jahre 1948 beschriebenen Big-Brother-Jahres „1984" verkündete das Bundesverfassungsgericht sein Urteil zum Volkszählungsgesetz. Das Gericht erklärte die in dem Gesetz vorgesehenen Übermittlungsregelungen für nichtig und hob gleichzeitig das „Recht auf informationelle Selbstbestimmung" aus der Taufe. Mit dieser „grundrechtlichen Konkretisierung des allgemeinen Persönlichkeitsrechts" sollte den neuartigen Gefährdungen der menschlichen Persönlichkeit begegnet werden, die mit der Entwicklung automatischer Datenverarbeitung verbunden sind[1]. Dieses Urteil lag im Trend einer sich seit Beginn der 70iger Jahre des vorigen Jahrhunderts verstärkenden Bewegung, die das Schreckensbild des „gläsernen Menschen" und einer allwissenden, ungeteilten Staatsmacht an die Wand malte[2]. Walter Schmitt Glaeser hat dieser Bewegung eine „Übersensibilität mit zuweilen geradezu hysterischen Zügen" bescheinigt, wenn es um den Schutz der Privatsphäre im Verhältnis zum Staat ging; ähnlichem Misstrauen begegneten andere Institutionen, die man als „mächtig" und dementsprechend gefährlich einschätzte, wobei die Auswahl „recht willkürlich" getroffen wurde[3].

Schon damals konnte man aber eine auffallende Widersprüchlichkeit in der Bewertung der Privatsphäre feststellen. Wie Schmitt Glaeser schreibt, war in weiten Teilen des gesellschaftlichen Bereichs „ein geradezu grenzenloser Hang zu öffentlichen Schaustellungen intimster Gefühle und Lebensvorgänge" zu konstatieren[4], ein Drang zum Exhibitionismus, der bis heute immer neue und exzessivere Ausdrucksformen findet – von öffentlichen Telefonaten per Handy über Fernsehformate mit vorprogrammierten Nervenzusammenbrüchen bis hin zu Kannibalismus-Angeboten im Internet. Dementsprechend titelte die Marketing-Zeitschrift „Werben und Verkaufen" kürzlich: „Big Brother war gestern"[5] und zitiert den bayerischen Landesbeauftragten für den Datenschutz, Reinhard Vetter mit den Sätzen: „Das Gefahrenbewusstsein hat sich verringert – als abstraktes Thema interessiert das nur eine kleine Minderheit. Die meisten sagen, „von mir kann jeder alles wissen" und untermauern das durch das eigene Verhalten im Umgang mit ihren Daten".

Diese gesellschaftliche Entwicklung wird im hoheitlichen Bereich auf europäischer und staatlicher Ebene begleitet von einer „Öffnung der Aktenschränke" mit dem Ziel der Schaffung „gläserner Behörden" und der „Transparenz zum Anfassen". Geheimhaltung wird als „unzeitgemäß" verstanden und das Informationsfreiheitsgesetz von Nordrhein-Westfalen wird als ein „Schritt aus dem Entwicklungsrückstand Deutschlands" gefeiert[6]. Warnungen vor einer „Totalisierung der Öffentlichkeit, wie wir sie heute erleben" sind nur selten zu hören[7]. Der Funkchip unter der Haut wird nicht aufzuhalten sein. 20 Jahre nach den Geheimhaltungsexzessen fundamentalistischer Datenschützer, die insbesondere die historische, pädagogische und epidemiologische Forschung massiv behindert hatten – erinnert sei nur an die Kämpfe um ein Krebsregister[8] – scheint es jetzt zu einem Gegenschlag von Transparenzfanatikern zu kommen.

1.2 Der Staat als Adressat des Rechts auf informationelle Selbstbestimmung

Das vom Bundesverfassungsgericht aus den Grundrechten auf freie Entfaltung der Persönlichkeit (Art. 2 I GG) und auf Schutz der Menschenwürde (Art. 1 I GG) abgeleitete Recht auf informationelle Selbstbestimmung wird verstanden als die „Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden"[9]. Dieses Recht schützt generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten[10]. Adressat dieses Grundrechts ist also der Staat; eine unmittelbare Bindung Privater ist hier ebenso ausgeschlossen wie bei nahezu allen anderen Grundrechten – vom allgemeinen Gleichheitssatz bis zum Schutz der Ehe. Will der Staat private Daten vor der Erhebung und Verarbeitung durch Private schützen, muss er sich strikt an der Privatautonomie orientieren. Denn weil das Grundgesetz die Privatautonomie der Bürger um ihrer Selbstbestimmung und Selbstverantwortung willen garantiert, spricht „gleichsam eine verfassungsrechtliche Vermutung gegen gesetzliche Regulierungen"[11]. Der Umstand, dass direkt nur der Staat gezwungen ist, das Datenschutzgrundrecht zu respektieren, bestimmt auch über Art und Umfang der schützenswerten Daten. Der nur vom Staat ausgehenden Gefahr der Schaffung des „gläsernen Menschen" durch Erstellung umfassender Persönlichkeits- und Verhaltensprofile kann allein dadurch begegnet werden, dass sich der Schutz vor dem Staat auf alle Arten personenbezogener Daten erstreckt. Wegen der der Informationstechnologie eigenen

Autor: Wilfried Berg
Titel: Telemedizin und Datenschutz
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2005
Seite: 112-116

Verarbeitungs- und Verknüpfungsmöglichkeiten kann jedes, auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; „insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses“ Datum mehr“[12].

1.3 Grundsatz der Datenvermeidung und Datensparsamkeit

Aus alledem – aus den genannten verfassungsrechtlichen Vorgaben und zugleich in Umsetzung der EG-Datenschutzrichtlinie von 1995 – hat der (einfache) Gesetzgeber bei der Novellierung des Bundesdatenschutzgesetzes im Jahre 2001 die Konsequenz gezogen, einen Grundsatz der „Datenvermeidung und Datensparsamkeit“ (§ 3 a BDSG) aufzustellen[13]. Der juristische Laie könnte dies als Aufforderung zum Rückzug in die Steinzeit missverstehen. Aus neuerer arbeitsmedizinischer Sicht könnte man dem sogar einen therapeutischen Nutzen abgewinnen. So hat die Süddeutsche Zeitung bereits im Sommer des vergangenen Jahres eine „Sturmwarnung im Datenozean“ verbreitet: „Die digitale Informationsflut lähmt bei der Arbeit und macht krank – Rettung ist kaum in Sicht“[14]. Es gebe bereits eine krankhafte Sucht nach neuen „Infohappen“. Ein australischer Forscher spricht von „Infostress“, und in Harvard hat man ein „Pseudo-Aufmerksamkeitsdefizit-Syndrom“ entdeckt.

Nun, davor kann und soll der neue Datenvermeidungs- und Sparsamkeitsgrundsatz nicht schützen. Es geht vielmehr allein um möglichste Vermeidung der Erhebung, Verarbeitung und Nutzung **personenbezogener** Daten und ihre prinzipielle Ersetzung durch anonymisierte oder pseudonymisierte Daten[15]. Praktisch bedeutet dies, dass schon vor jeder Datenerhebung ebenso wie vor jedem Schritt der Verarbeitung und Nutzung geprüft werden muss, ob überhaupt personenbezogene Daten benötigt werden. Wird dies bejaht, ist weiter zu prüfen, welche dieser personenbezogenen Daten zur Erreichung des konkret angestrebten Zweckes tatsächlich erforderlich sind. „Mit der Aufhebung des Personenbezugs durch **Anonymisierung** oder **Pseudonymisierung** der Daten entfällt der Schutzbedarf, die datenschutzrechtlichen Regeln finden keine Anwendung“[16].

Im Unterschied zum Grundrecht auf informationelle Selbstbestimmung gelten Voraussetzungen und Rechtsfolgen der Datenvermeidung nicht nur für den Staat; ihre Regelung findet sich vielmehr im ersten Abschnitt des Bundesdatenschutzgesetzes über allgemeine und gemeinsame Bestimmungen, vor dem Abschnitt über Datenverarbeitung der öffentlichen Stellen (§§ 12 ff BDSG) und dem Abschnitt über Datenverarbeitung nicht-öffentlicher Stellen (§§ 27 ff BDSG).

2 Datenschutz im Gesundheitswesen

Ich komme nun zu Besonderheiten des Datenschutzes im Gesundheitswesen.

2.1 Verarbeitungsverbot Personen bezogener Daten über Gesundheit

Auszugehen ist dabei von dem **Grundsatz**, dass personenbezogene Daten über Gesundheit oder Sexualleben einem Verarbeitungsverbot unterliegen, das den Mitgliedstaaten durch die Datenschutzrichtlinie der EG vorgegeben worden ist[17]. Das Bundesdatenschutzgesetz hat sich bei der Umsetzung dieser Richtlinie von den Vorstellungen des Bundesverfassungsgerichts entfernt, wonach nicht so sehr die Art der Daten sondern ihre Verwendungsmöglichkeiten über ihre Sensibilität bestimmt, dass Daten also auch dann nicht belanglos sind, wenn sie keine intimen Vorgänge betreffen[18]. In § 3 IX BDSG hat das Bundesdatenschutzgesetz im Jahre 2001 vielmehr die neue Kategorie der „besonderen Arten personenbezogener Daten“ (sog. „sensitive Daten“) eingeführt. Das sind „Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“. In zahlreichen Einzelvorschriften werden dann Einschränkungen beim Umgang mit Daten davon abhängig gemacht, ob es um solche „besonderen Arten personenbezogener Daten“ geht, wie z. B. im Hinblick auf die Einwilligung (§ 4 a III BDSG), die Vorabkontrolle (§ 4 d V Nr. 1 BDSG), die Erhebung, Speicherung, Veränderung, Nutzung und Übermittlung durch öffentliche Stellen (§§ 13 II, 14 V, 16 I Nr. 2 Satz 2 BDSG) und das Erheben, Verarbeiten und Nutzen für eigene Geschäftszwecke, für Gesundheitszwecke etc. (§§ 28 VI - IX BDSG). Für die Marktforschung war es übrigens immer schon mit entscheidend, „welche Art von Angaben von dem Befragten gefordert wird: Gehalt, Gesundheit und Geschlechtsleben sind dabei unabhängig von der Datenverwendung immer noch Tabus, während sich unter „Freizeit, Fahrzeug, Ferien“ all jene Bereiche zusammenfassen lassen, die hohe Auskunftsbereitschaft versprechen“[19].

Um Missverständnisse zu vermeiden sei hier vorsichtshalber nochmals darauf hingewiesen, dass der Rechtsbegriff der „personenbezogenen Daten“ nicht impliziert, dass es sich um Informationen über die Privat- oder Intimsphäre handeln müsse. Entscheidend ist allein, dass Daten einer bestimmten Person zugeordnet werden können. Das Gegenstück zu den personenbezogenen Daten sind anonymisierte oder pseudonymisierte Daten, die – wie schon ausgeführt – aus dem Anwendungsbereich des Datenschutzrechts herausfallen[20].

2.2 Grundsätzliches Erfordernis der Einwilligung

Natürlich ist das Verarbeitungsverbot personenbezogener Gesundheitsdaten nicht das letzte Wort des Bundesdatenschutzgesetzes. Allerdings können Gesundheitsinformationen als eine der „besonderen Arten personenbezogener Daten“ im Sinne des § 3 IX BDSG nicht schon allein auf Grund eines Vertragsverhältnisses – z. B. des Behandlungsvertrages – erhoben und verarbeitet werden, wie dies sonst für nicht-öffentliche Stellen zur Erfüllung der eigenen Geschäftszwecke gilt, § 28 I Nr. BDSG. Vielmehr ist dies – von Notfällen abgesehen – prinzipiell nur dann zulässig, wenn der Patient unter ausdrücklichem Bezug auf die Gesundheitsdaten eingewilligt hat und zwar in schriftlicher Form, § 28 VI in Verbindung mit § 4 a I, III BDSG. Gemäß der Neufassung des § 126 III BGB kann die eigenhändige Namensunterschrift durch die elektronische Form ersetzt werden[21]. Eine wichtige Ausnahme von diesem datenschutzrechtlichen Erfordernis einer qualifizierten Einwilligung macht jedoch die – in anderem Zusammenhang bereits erwähnte – Bestimmung des § 28 VII 1 BDSG: Nach dem ausdrücklich in der Ge-

setzesbegründung geäußerten Willen des Gesetzgebers soll die bisher übliche stillschweigende Einwilligung dann ausreichen, wenn Gesundheitsdaten „zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich sind und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen“[22].

Diese Abkehr vom bisher ganz im Vordergrund stehenden Einwilligungserfordernis muss für das Gesundheitswesen begrüßt werden. Einwilligung hat nämlich prinzipiell nichts mit Datenschutz zu tun, sondern allenfalls mit Datenautonomie. Wer in die Weitergabe seiner Daten einwilligt, verzichtet ja gerade darauf, sein Geheimnis so umfassend wie bisher zu schützen. Einwilligung gefährdet also und schützt nicht. Wenn man gleichwohl bisher auf einem möglichst ausnahmslosen Einwilligungserfordernis bestand, dann lag das an der unreflektierten Übernahme der vom Bundesverfassungsgericht für das Verhältnis Bürger-Staat aufgestellten Regeln zum Schutz des Rechts auf informationelle Selbstbestimmung auch in das Patienten-Arzt-Verhältnis hinein. Dabei war man sich eigentlich immer schon darüber im Klaren, dass es in diesem Verhältnis wirkliche Datenautonomie des Patienten kaum, eine wirklich informierte Einwilligung („informed consent“) praktisch nie geben kann[23]. Das klassische Problem ist hier schon die Situation der Diagnose: Kein Patient und kein Arzt kann im Voraus wissen, welche Daten der Arzt durch eine Ultraschall-, Röntgen- oder Blutuntersuchung erheben wird – wie soll der Patient dann – informiert – in diese Erhebung einwilligen? Hier liegen fundamentale Unterschiede im Vergleich mit den Daten, die der Staat über Verhalten und Persönlichkeit seiner Bürger erheben und verarbeiten möchte. Ein weiteres Problem liegt darin, dass die ärztliche Dokumentation über den Besuch eines Patienten – also über dessen Daten – unabhängig davon erfolgen und erhalten bleiben muss, ob der Patient seine Einwilligung gegeben oder auch nur später mit Wirkung für die Zukunft widerrufen hat[24]. Diesen Unterschieden und Besonderheiten muss die Rechtsordnung Rechnung tragen, wenn sie verfassungsmäßigen und effektiven Datenschutz erreichen will.

2.3 Geheimhaltungspflichten

Das geschieht durch die Heranziehung der Geheimhaltungspflichten in der zitierten Bestimmung des § 28 VII BDSG. Ärzte unterliegen der strafrechtlich durch § 203 I Nr. 1 StGB sanktionierten Geheimhaltungspflicht, wenn ihnen in ihrer Eigenschaft als Arzt „ein fremdes Geheimnis anvertraut worden oder sonst bekannt geworden ist“. So wenig anheimelnd der strafrechtliche Hintergrund der ärztlichen Verschwiegenheitspflicht auch ist, so genau wird doch hier an das alles entscheidende Vertrauensverhältnis zwischen Arzt und Patient angeknüpft. Im Gesundheitsbereich geht es eben nicht um prinzipielle Verhinderung von Datenverarbeitung, um Eingriffe in die selbst bestimmte Persönlichkeitssphäre auszuschließen oder zu begrenzen. Datenautonomie ist zwar auch im Gesundheitsbereich schön und wichtig, aber ohne Gesundheit ist sie nicht mehr viel wert. Nicht einmal die Hoffnung auf postmortalen Schutz des allgemeinen Persönlichkeitsrechts bliebe dann[25]. Die Bedeutung des Vertrauens auf die Garantien der Vertraulichkeit der Behandlung von Informationen für die – im Patienten-Arzt-Verhältnis manchmal lebenswichtige – Richtigkeit und Vollständigkeit der Informationspreisgabe ist danach ganz enorm. Dazu hat das Volkszählungsurteil des Bundesverfassungsgerichts Ausführungen gemacht, die sich über den eigentlichen Anlaß der Anforderungen an die Mitwirkung der Bürger bei statistischen Erhebungen hinaus hierauf gut übertragen lassen: „Für die Funktionsfähigkeit der amtlichen Statistik ist ein möglichst hoher Grad an Genauigkeit und Wahrheitsgehalt der erhobenen Daten notwendig. Dieses Ziel kann nur erreicht werden, wenn bei dem auskunftspflichtigen Bürger das notwendige Vertrauen in die Abschottung seiner ... Daten geschaffen wird ... Eine Staatspraxis, die sich nicht um die Bildung eines solchen Vertrauens durch Offenlegung des Datenverarbeitungsprozesses und strikte Abschottung bemühte, würde auf längere Sicht zu schwindender Kooperationsbereitschaft führen, weil Mißtrauen entstünde“[26].

3 Umgang mit dem besonderen Gefährdungspotential der „Telemedizin“

„Telemedizin“ – so heißt es in den Einbecker Empfehlungen zu Rechtsfragen der Telemedizin von 1999 – „ermöglicht oder unterstützt in Überwindung räumlicher Entfernungen medizinische Dienstleistungen durch die kombinierte Anwendung von Telekommunikation und Informatik (Telematik)“. Es liegt in der Natur der Sache, daß durch das fehlende Erfordernis einer zeitlichen und räumlichen Koinzidenz der Handelnden die im klassischen Patienten-Arzt-Verhältnis gesicherte Abschottung der Patientendaten gelockert oder ganz aufgehoben wird oder werden kann. „Telemedizinische Anwendungen zeichnen sich insoweit durch ein besonderes Gefährdungspotential aus“[27]. Um die Heilungschancen nicht zu gefährden, muß indes alles getan werden, damit das essentielle Vertrauensverhältnis des Patienten gegenüber seinem Arzt gesichert bleibt. Besondere gesetzliche Regeln gibt es dazu bislang nicht, wenn man von der zum 01.07.2002 in Kraft getretenen novellierten Fassung der Röntgenverordnung absieht, die erstmals mit der Teleradiologie ein Teilgebiet der Telemedizin regelt[28]. Aber schon jetzt sind Sicherungsmechanismen vorhanden, deren überlegte und konsequente Nutzung die wesentlichen Ziele des Datenschutzes meines Erachtens durchaus erreichen kann.

3.1 Erforderlichkeit

Wie stets stellen sich datenschutzrechtliche Fragen auch bei telemedizinischen Anwendungen nur dann, wenn personenbezogene Daten bearbeitet werden. Hier dürfte die erst im Zug der Anpassung des Bundesdatenschutzgesetzes an die EG-Datenschutzrichtlinie aufgenommene und schon mehrfach erwähnte Bestimmung des § 28 VII BDSG eine zentrale Rolle spielen[29]. Danach bedarf die Erhebung von personenbezogenen Gesundheitsdaten dann keiner qualifizierten Einwilligung im Sinne des § 4 a I, III BDSG, wenn sie im wesentlichen für medizinische Zwecke erforderlich ist und wenn die Datenerheber Geheimhaltungspflichten nach § 203 StGB unterliegen. In diesen Fällen sind im Hinblick auf die für die Weitergabe

von Daten gebotene Einwilligung des Patienten lediglich die berufsrechtlichen Regeln einzuhalten, so daß die Einwilligung nicht schriftlich erteilt werden muß und durchaus auch stillschweigend erteilt werden kann[30]. Völlig zu Recht wird demgemäß gegenwärtig beim elektronischen Arztbrief oder in seltenen Fällen des Telekonsils „regelmäßig mit einer stillschweigenden Einwilligung des Patienten gearbeitet, der von dem Übermittlungsvorgang weiß oder mit ihm rechnet“[31].

Entscheidendes Augenmerk sollte aber seitens der Ärzte im Bereich telematischer Verfahren gerade nicht auf die Einwilligungsproblematik gerichtet werden, sondern auf die rechtlich vorrangige Frage, ob in diesen Fällen die Verarbeitung personenbezogener Daten überhaupt erforderlich ist, ob also keine anonymisierte oder pseudonymisierte Datenübermittlung ausreicht. Damit komme ich also auf den in § 3 a an prominenter Stelle in das Bundesdatenschutzgesetz eingeführten Grundsatz der Datenvermeidung und Datensparsamkeit zurück, der gerade in der Telemedizin größte Bedeutung haben muß[32]. So ist etwa im Rahmen eines Telekonsils oder bei der Inanspruchnahme von Telematik-Dienstleistern stets zu fragen, ob der Patientenbezug beibehalten werden muß oder ob die Daten nicht auch verschlüsselt übermittelt werden können[33]. Wenn dies möglich ist – z.B. in der Regel bei der Beurteilung eines Gewebeschnitts, eines Röntgenbildes oder eines EKGs – muß auf die Übermittlung personenbezogener Daten verzichtet werden. Überzeugend hat das OVG Rheinland-Pfalz vor einem Jahr in einem Rechtsstreit zur Teleradiologie festgestellt, daß es sich hier um ein „Hilfsmittel der Diagnose“ handelt, dessen Aussagekraft „nicht von dem Eindruck einer persönlichen Untersuchung des Patienten bestimmt wird. Der diagnostische Wert eines Computertomogramms hängt vielmehr von technischen Gegebenheiten (wie der Bildqualität), deren Beherrschung und der Erfahrung des befundenden Radiologen ab“[34]. Das Erfordernis der qualifizierten und formalisierten datenschutzrechtlichen Einwilligung entfällt mit der Verschlüsselung oder Anonymisierung. Selbstverständlich wird der Arzt dadurch nicht von den Bindungen an die berufs-, straf- und haftungsrechtlichen Geheimhaltungs- und Dokumentationspflichten befreit. – Auf die berufsrechtliche Problematik des sog. „Fernbehandlungsverbotes“ und auf die Auslegung des § 7 III Musterberufsordnung, die im Zentrum der zitierten Entscheidung des OVG Rheinland-Pfalz stand, kann hier nicht näher eingegangen werden[35].

3.2 Datenschutztechnik

Auch wenn es das Ziel der Datenverarbeitung in der medizinischen Praxis sein muß, den Anteil personenbezogener Daten so klein wie nur eben möglich zu halten und dadurch den Anwendungsbereich des Datenschutzrechts entsprechend zu verringern, wird auch in Zukunft der persönliche Patienten-Arzt-Kontakt ganz im Mittelpunkt stehen und stehen müssen. Das hier essentielle Vertrauensverhältnis ist weitestgehend davon abhängig, daß der Arzt alle technischen und organisatorischen Maßnahmen ergreift, um den Geheimnisschutz und den Schutz personenbezogener Daten sicher zu stellen. Das Bundesdatenschutzgesetz stellt hierzu in § 9 und in 8 Punkten einer Anlage Anforderungen an die Kontrollen des Zutritts, des Zugangs, des Zugriffs, der Weitergabe, der Eingabe, der Aufträge, der Verfügbarkeit und der Trennung der Daten. Dabei wird nicht die Einhaltung eines einheitlich-absoluten Schutzniveaus erwartet; vielmehr werden Schutzbedürftigkeit und Schutzaufwand in eine Verhältnismäßigkeitsbeziehung gesetzt[36]. Auf Einzelheiten der Problemstellungen – etwa bei elektronischen Rezepten – und der technischen Lösungsmöglichkeiten – etwa die kryptographischen Verschlüsselungsverfahren – kann hier nicht eingegangen werden. Gleiches gilt für die zum Teil schon in der Alltagspraxis erprobten datenschutzfreundlichen Technologien wie sie durch Heilberufsgesetze einiger Bundesländer für elektronische Arztausweise ermöglicht werden oder für die Einführung einer interoperablen elektronischen Health Professional Card (HPC)[37].

Festzuhalten bleibt, daß wirksamer Datenschutz selbstverständliche Basis aller gegenwärtigen und künftigen telemedizinischen Anwendungen sein muß. Datenschutz ist nur wirksam, wenn er die Technik, die die elektronische Datenverarbeitung hervorgebracht hat, dazu einsetzt, um die Gefahren dieser Technik wieder einzugrenzen. Es bedarf aller Anstrengungen zur technischen Innovation, um die wechselseitige Abschottung der Informationssysteme mit den Zielen des Persönlichkeits- und Geheimnisschutzes auszubauen und zu sichern[38]. Wenn sich das Datenschutzrecht in diese Richtung des Datenschutz-Technikrechts weiterentwickelt, dürfte es kein „Hemmschuh“ für telematische Anwendungen zum Wohle der Gesundheitsversorgung und Gesundheitsvorsorge mehr sein[39]. Ein in dieser Weise verstandener und praktizierter Datenschutz läßt Arzt und Patienten ohne neue Risiken teilhaben an den großen Chancen der Telemedizin.

Fußnoten

1 Vgl. BVerfGE 65, 1 (43 ff.); dazu Ernst Benda, Menschenwürde und Persönlichkeitsrecht, in: Benda/Maihofer/Vogel (Hrsg.), Handbuch des Verfassungsrechts, 2. Aufl. 1995, § 6 Rn. 34 ff.; Berg, Informationelle Selbstbestimmung und Forschungsfreiheit: Zum Spannungsverhältnis zwischen zwei in der Verfassung verankerten Rechten, in: Jehle (Hrsg.), Datenzugang und Datenschutz in der kriminologischen Forschung, 1987, S. 30 ff

2 Näher Berg, Datenschutz und Forschungsfreiheit, in: JöR NF 33 (1984), S. 68

3 Vgl. Schmitt Glaeser, Schutz der Privatsphäre, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts Bd. VI, 1989, § 129 Rn. 13

4 Vgl. Schmitt Glaeser, a.a.O. Rn. 12

5 Vgl. Rudolph Attlfellner, Werben und Verkaufen 26/2003, S. 22

6 Dazu mit zahlreichen weiteren Nachweisen Berg, Risikokommunikation als Bestandteil der Risikoanalyse (Risikobewertung - Risikomanagement - Risikokommunikation), ZLR 2003, 531. Siehe auch Kotzur, Verwaltung in der Kommunikationsgesellschaft - Eine Skizze zeitgemäßer Organisationsstrukturen, NWVBl. 2003, 298 ff, 302 ff.; ferner Nowak, Informations- und Dokumentationzugangsfreiheit in der EU, DVBl. 2004, 272 ff

7 Vgl. Depenheuer, Öffentlichkeit und Vertraulichkeit, Einführung, in: Depenheuer

(Hrsg.), Öffentlichkeit und Vertraulichkeit. Theorie und Praxis der politischen Kommunikation, 2001, S. 19

[8] Zu den Voraussetzungen einer funktionsfähigen Epidemiologie, Dierks/Nitz/Grau, Gesundheitstelematik und Recht, 2003, S. 20 f. mit weiteren Nachweisen Fn. 28. - Eine Zusammenstellung von datenschutzrechtlich motivierten Behinderungen der kriminologischen und sozialwissenschaftlichen Forschung findet sich in: Jehle (Hrsg.), Datenzugang und Datenschutz in der kriminologischen Forschung, 1987

[9] BVerfGE 65, 1 (41 f.)

[10] Vgl. BVerfGE 78, 77 (84); dazu Murswiek, in: Sachs (Hrsg.), Grundgesetz-Kommentar, 3. Aufl. 2003, Art. 2 Rn. 73. Typisches aktuelles Gefährdungspotential für die informationelle Selbstbestimmung bergen z.B. Methoden vorbeugender Rasterfahndungen; dazu Horn, DÖV 2003, 746 ff

[11] Vgl. Schmitt Glaeser, Fn. 3, Rn. 90. Siehe auch Murswiek, Fn. 10, Art. 2 Rn. 122: „Datenverarbeitung durch Private fällt in deren grundrechtlich geschützten Freiheitsbereich“

[12] BVerfGE 65, 1 (65); dazu Pieroth/Schlink, Grundrechte Staatsrecht II, 20. Aufl. 2004, Rn 377

[13] Dazu Bizer, in: Simitis (Hrsg.), Kommentar zum BDSG, 5. Aufl. 2003, § 3a Rn. 1, 22 ff.; Dierks/Nitz/Grau (Fn 8), S. 44 ff

[14] Vgl. Andreas Grote, Süddeutsche Zeitung Nr. 160, S. 35 vom 15.07.2003

[15] Zu den Forderungen nach Einsatz wirksamer Anonymisierungstechniken bereits Berg, Fn. 2, S. 82 ff. mit Nachweisen in Fn. 68 und S. 102

[16] Vgl. Dierks/Nitz/Grau, Fn. 8, S. 44

[17] Vgl. Dammann/Simitis, in: Simitis (Hrsg.), Fn. 13, § 3 Rn. 257 ff. bez. der „sensitiven“ Daten; ferner Dierks/Nitz/Grau, Fn 8, S. 57 f., 134 f. Eine eindruckvolle und höchst informative Vorstellung vom - vornehmlich europarechtlich bestimmten - Rechtsrahmen für eHealth-Anwendungen gibt Hanika, Bism@rck geht online, MedR 2003, 15 ff. und MedR 2004, 149 ff

[18] Vgl. BVerfGE 65, 1 (45). Diese Abkehr von der Differenzierung zwischen mehr oder minder „sensiblen“ Daten durch das Volkszählungsurteil des BVerfG wurde seinerzeit als Fortschritt im Datenschutzrecht gefeiert, vgl. Berg, Fn. 2, S. 82 mit Nachweisen in Fn. 66. Dammann/Simitis, Fn. 17, Rn. 260 stellen nach wie vor entscheidend auf den Verwendungszusammenhang ab

[19] Vgl. Attlfellner, Fn. 4, S. 25

[20] Vgl. Berg, Fn. 2, S. 82 f. Siehe auch oben im Text zu Fn. 15

[21] Vgl. Dierks/Nitz/Grau, Fn. 8, S. 46, 138, 140

[22] Näher dazu Dierks/Nitz/Grau, Fn. 8, S. 46 f., 138 ff. Simitis, Fn. 13, § 28 Rn. 325, 338 ff. läßt den Verzicht auf die Einwilligung nur in den vier vom Gesetz „ausschließlich und abschließend aufgeführten Fällen“ des § 28 VI Nr. 1-4 BDSG zu

[23] Dazu, daß Einwilligung einen Verzicht auf den grundrechtlichen Schutz vor Weitergabe der personenbezogenen Daten bedeutet Klaus Stern, Das Staatsrecht der Bundesrepublik Deutschland, Bd. III/2, 1994, S. 898 f. Hinweise auf schwerste Konflikte, die das Postulat der Einwilligung heraufbeschwören kann schon bei Berg, Fn. 2, S. 97 mit weiteren Nachweisen

[24] Siehe Dierks/Nitz/Grau, Fn. 8, S. 137

[25] Dazu BVerfGE 30, 173 (194 - „Mephisto“); BVerfG NJW 2001, 594 „Willy Brandt“. Es besteht kein Grundrechtsschutz des Verstorbenen aus Art. 2 I GG, „weil Träger dieses Grundrechts nur die lebende Person ist“. Siehe auch Pieroth/Schlink Fn. 12, Rn. 120

[26] Vgl. BVerfGE 65, 1 (50 f.) unter Bezugnahme auf die Begründung der Bundesregierung zum Entwurf des Volkszählungsgesetzes 1950

[27] Vgl. Dierks/Nitz/Grau, Fn. 8, S. 144; dort auch zu den Einbecker Empfehlungen, S. 127, abgedruckt S. 144 ff. Siehe ferner Hanika, Telemedizin - Handlungs- und Weiterentwicklungsbedarf, MedR 2001, 107 ff. - Umfassend zu den Möglichkeiten und Chancen der Telemedizin Jäckel (Hrsg.), Telemedizinführer Deutschland, 5. Aufl. 2004

[28] Dazu Walz/Loose, Teleradiologie nach RöV: Vorgaben und Möglichkeiten, in: Jäckel (Hrsg.), Fn. 27, S. 194 ff

[29] Siehe vor allem oben im Text zu Fn. 22

[30] Näher dazu Dierks/Nitz/Grau, Fn. 8, S. 46 ff. mit Hinweisen zur Abgrenzung der stillschweigenden Einwilligung von einer „mutmaßlichen“ Einwilligung in Fn. 113; ferner S. 138 ff

[31] Vgl. Dierks/Nitz/Grau, Fn. 8, S. 141. Zu den Einsatzmöglichkeiten von Telekonsil, Telekonferenz und Telmonitoring siehe die Beiträge in: Jäckel (Hrsg.), Fn. 27, S. 40 ff

[32] Siehe oben im Text zu Fn. 13 ff. mit weiteren Nachweisen

[33] Näher dazu Dierks/Nitz/Grau, Fn. 8, S. 44, 77, 103

[34] Vgl. OVG Rheinland-Pfalz, Entscheidung vom 21.01.2003 - 6 A 112.10/02. OVG, zitiert nach Dierks/Nitz/Grau, Fn. 8, S. 91 mit Fn. 297

[35] Dazu Dierks/Nitz/Grau, Fn. 8, S. 88 ff., 148 f., 159 f. (zum Werbeverbot)

[36] Zur herausragenden Rolle der Datensicherheit gerade im Gesundheitswesen Herbst/Wolthusen, Empfehlungen zur IT-Sicherheit von Praxis-Systemen, in: Jäckel (Hrsg.), Fn 27, S. 204 f. Siehe auch Debold/Reng, Generische Datenschutzmodelle für die medizinische Forschung, ebenda, S. 214 ff.; Dierks/Nitz/Grau, Fn. 8, S. 50 ff., 142 f., 144 ff. (zum datenschutztechnischen Regelungsbedarf), 189 (zu kryptographischen Verschlüsselungsverfahren)

[37] Ausführlich Goetz, Telematik im Gesundheitswesen - Herausforderungen für eine Modernisierung, in: Jäckel (Hrsg.), Fn. 27, S. 32 ff., 34

[38] Vgl. Berg, Informationelle Selbstbestimmung und Forschungsfreiheit: Zum Spannungsverhältnis zwischen zwei in der Verfassung verankerten Rechten, in: Jehle (Hrsg.), Fn. 7, S. 34 f.; ders., Vom Wettlauf zwischen Recht und Technik, JZ 1985, S. 404 f

[39] Zum notwendigen Abbau von Vorurteilen gegen IT-Sicherheit als „kompliziert, aufwändig, teuer, lästig“ Weinand, Ungeliebte IT-Sicherheit, in: Jäckel (Hrsg.), Fn. 27, S. 220 ff. Siehe auch Dierks/Nitz/Grau, Fn. 8, S. 134, die die „bestehenden Rechtsunsicherheiten im Datenschutz“ als „Hemmschuh in der Entwicklung telematischer Anwendungen“ bezeichnen.