Outsourcing von medizinischen Daten
-strafrechtlich betrachtet-

Inaugural-Dissertation
zur Erlangung der Würde eines
doctor iuris
der Juristischen Fakultät
der Bayerischen Julius-Maximilians-Universität
Würzburg

vorgelegt von
Christian Ehrmann
aus Hermannstadt
2008

Inhaltsverzeichnis

Gliederung

A. Einleitung

Sowohl im öffentlichen als auch im nicht-öffentlichen Bereich der Datenverarbeitung und Datenverwaltung im Gesundheitswesen gewinnt der Begriff „Outsourcing“ zunehmend an Bedeutung. Vor dem Hintergrund anwachsender Datenmengen und eines hohen Kostendrucks durch das Bereithalten aufwendiger IT-Infrastruktur wird vermehrt über Möglichkeiten der Kostenreduzierung nachgedacht. Insbesondere für Einrichtungen, die einen großen Datenbestand zu verwalten haben, ist die Möglichkeit des Outsourcings von Daten an externe, private IT-Dienstleistungsanbieter von Interesse[1].

Ein Ziel von Outsourcinggebern ist es, externe Kompetenz in einem speziellen und komplexen Bereich zu niedrigeren Kosten, insbesondere niedrigeren Lohnkosten, aber auch Sachkosten, zu erreichen. Private, hochspezialisierte IT-Dienstleistungsunternehmen erscheinen als Partner von Outsourcingprojekten als kostengünstigere Alternative oder Ergänzung zur eigenen Datenverwaltung und Datenwartung geeignet. Moderne Netzwerk- und IT- Infrastrukturen lassen es zu, auch große Datenmengen mit hoher Geschwindigkeit zu übermitteln. In Kombination mit der stetigen Zunahme externer Speicherkapazitäten und dezentraler Netzsysteme ergibt sich ein hohes Mobilitätspotential.

Dabei können sich sowohl für den Outsourcer als auch für das anbietende Unternehmen Vorteile ergeben. Für den Outsourcer bietet sich die Möglichkeit einer Kosteneinsparung, für das IT- Unternehmen erschließt sich ein zukunftsträchtiger und wachsender Markt. Zur Erreichung der erwähnten Vorteile, ist es für beide Partner äußerst bedeutsam, die rechtlichen Möglichkeiten, Voraussetzungen und Grenzen des Outsourcings vor dem geltenden Recht zu erfassen, um beabsichtigte Outsourcingprojekte hinsichtlich ihrer Risiken sowohl im rechtlichen als auch im wirtschaftlichen Sinne einordnen zu können. Im Rahmen dieser Arbeit sollen die strafrechtlichen Aspekte eines Outsourcings medizinischer Daten untersucht werden.

[1] Vgl. Süddeutsche Zeitung Nr. 242 vom 18. Oktober 2004, S. 24; Süddeutsche Zeitung Nr. 224 vom 1. Oktober 2004, S. 23.

I. Der Begriff „Outsourcing“

Der Begriff „Outsourcing“ ist kein feststehender, rechtstechnischer Begriff, sondern vielmehr phänomenologischer Natur. Ursprünglich aus der US-amerikanischen Wirtschaft stammend, leitet sich der Begriff von „outside resources using“ ab[2]. Damit wird das Benutzen von Sach- und Personalmitteln außerhalb des eigenen Wirkungsbereichs umschrieben. Erfasst werden durch diesen Sammelbegriff zum einen Auslagerungen von kompletten Funktionseinheiten an außenstehende Dritte zur selbständigen Bearbeitung[3]. Zum anderen kann darunter auch das Heranziehen externer Dritter zur Erfüllung interner Aufgaben oder die weisungsgebundene Übertragung bestimmter Aufgaben an Dritte unter Kontrolle durch den Übertragenden verstanden werden.

Speziell im Bereich der elektronischen Datenverarbeitung und der Informationstechnologie wird zum Teil zwischen Outsourcing und ASP (Application-Service-Providing) unterschieden, wobei als zentrales Unterscheidungskriterium der Grad der Individualisierung aus Anwendersicht herangezogen wird[4]. Andere sehen ASP als eine Form des Outsourcings an[5]. Hierzu ist anzumerken, dass beide Erscheinungsformen nicht trennscharf unterschieden werden können. Das Outsourcing ist ein wirtschaftliches Phänomen, das sich keinem herkömmlichen Vertragstyp zuordnen lässt. Typisch in diesem Bereich ist allein die Vielfalt der Gestaltungen und die Gemengelage der Leistungen. Vertragsrechtliche Beurteilungen können nur für den Einzelfall nach Bestimmung der konkreten Leistungsart und des Leistungsumfangs erfolgen[6]. Eine abstrakte Differenzierung zwischen einem Outsour-

---

[2] Näher zum Begriff Müthlein/Heck, Outsourcing und Datenschutz, S. 1; Hartig, in: Roßnagel, Handbuch Datenschutzrecht, S. 1000; Schneider, Handbuch des EDV-Rechts, S. 136; Heymann/Lensdorf, in: Redeker, Handbuch der IT-Verträge, 5.4 Rn. 1.

[3] Vielfach wird dafür im Bereich der Datenverarbeitung der Begriff Funktionsübertragung im Gegensatz zur Datenverarbeitung im Auftrag verwendet, vgl. Breidenbach, in: Bäumler/Breinlinger/Schrader, Datenschutz von A-Z, O 400, S. 1 f.; Schaffland/Wildfang, BDSG, § 11 Rn. 7; unklar, ob die Auftragsdatenverarbeitung auch zum Outsourcing zu zählen ist, Simitis, in: Simitis, Bundesdatenschutzgesetz, § 28 Rn. 136; vgl. auch Kessler, DuD 2004, S. 40 (41), der Auftragsdatenverarbeitung und Funktionsübertragung als Alternativen für das Outsourcing behandelt; zur ganzen Bandbreite möglicher Outsourcingprojekte vgl. auch Küchler, in: Bräutigam, IT-Outsourcing, S. 61 f.; Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 406; Bachmann, NZA 2002, S. 1131.

[4] Westerholt/Berger, CR 2002, S. 81 f.; vgl. auch Czychowski/Bröcker, MMR 2002, S. 82.

[5] So Glossner, in: Bräutigam IT-Outsourcing, S. 207 (insbesondere Fußnote 6); zweifelnd Söbbing, in: Söbbing, IT-Outsourcing, S. 105.

[6] Soweit ein ASP Vertrag auf die entgeltliche Überlassung von Standardsoftware gerichtet ist, nimmt der BGH mittlerweile an, dass Mietvertragsrecht anzuwenden ist, BGH vom 15.11.2006, Az.: XII ZR 120/04.

cing-Vertrag und einem ASP-Vertrag ist kaum aussagekräftig und damit wenig hilfreich. Vollends unerheblich ist eine solche Differenzierung für die strafrechtliche Beurteilung. Aufgrund der Vielzahl der erfassten Vorgänge muss zur (straf-) rechtlichen Beurteilung jeweils feststehen, welche Qualität dem konkreten Vorgang innerhalb der aufgezeigten Bandbreite möglicher Outsourcingformen zukommt.

Der Gegenstand des Outsourcings, der die unterschiedlichsten Sach- und Dienstleistungen betreffen kann, soll im Rahmen dieser Arbeit auf medizinische Daten und die Aufgabe ihrer Verwaltung und Verarbeitung beschränkt werden und betrifft somit einen klassischen Bereich des Outsourcings von Dienstleistungen in der Informationstechnologie[7]. Interne Outsourcingvorgänge, d.h. Outsourcing innerhalb rechtlich selbständiger Zuordnungseinheiten, sollen dabei außer Betracht bleiben[8].

II. Entwicklungen im Gesundheitswesen

Die Attraktivität möglicher Outsourcingprojekte medizinischer Daten wird durch die jüngste Reform im Gesundheitswesen begünstigt. Das System der Gesetzlichen Krankenversicherung ist im Wesentlichen beitragsfinanziert. Grundkonzept ist eine solidarische Umlagenfinanzierung. Die gesetzlichen Krankenkassen leisten aufgrund von Verträgen eine Gesamtvergütung an die Kassenärztlichen Vereinigungen, die diese dann nach bestimmten, durch die Selbstverwaltungskörperschaften entsprechend den gesetzlichen Vorgaben festgelegten Maßstäben an die jeweiligen Vertragsärzte verteilen. Maßgeblich für die Einnahmensituation und somit für das Verteilungsvolumen ist der Beitragssatz. Dabei machen Beiträge sozialversicherungspflichtiger Arbeitnehmer den größten Teil des Einnahmevolumens in der gesetzlichen Krankenversicherung aus.

Zur Bestimmung der Gesamtvergütung, der Verteilungsmaßstäbe sowie einzelner Leistungswerte muss ein erheblicher statistischer Aufwand betrieben werden. Hierbei wirken eine Vielzahl von gesetzlichen, untergesetzlichen und vertragli-

[7] Hartmann, Outsourcing in der Sozialverwaltung und Sozialdatenschutz, S. 14 f.
[8] Zur Differenzierung zwischen externem und internem Outsourcing vgl. Hartmann, Outsourcing in der Sozialverwaltung und Sozialdatenschutz, S. 18.

chen Regelungen unterschiedlichster Normgeber zusammen. Entsprechend dem aus dem Sozialstaatsprinzip abgeleiteten staatlichen Versorgungsauftrag[9], der Bevölkerung ausreichende und flächendeckende Gesundheitsleistungen bereitzustellen, ist die Leistungserbringung, Leistungsbeschreibung und Preisbildung stark durch staatliche Planung und Regelung gekennzeichnet. Zur Umsetzung der komplexen Regelungen ist auf institutioneller Ebene ein erheblicher administrativer Aufwand erforderlich. Ein Hauptziel etlicher Reformen der gesetzlichen Krankenversicherung war und ist es, die chronisch defizitäre Finanzsituation der gesetzlichen Krankenkassen zu verbessern und ständige Beitragssatzerhöhungen zu vermeiden.

Verantwortlich für die schlechte Finanzentwicklung sind unterschiedliche externe und interne Faktoren[10]. Genannt werden der demographische Faktor, die Arbeitslosenquote, die Zunahme der Leistungserbringer, insbesondere der Vertragsärzte, hohe Arzneimittelpreise, unnötige Arztbesuche, fehlende Vernetzung der Leistungserbringer, Kostenintensivität neuer, moderner Diagnose- und Behandlungsmöglichkeiten, Effizienzlücken in Diagnostik und Behandlung sowie fehlender Wettbewerb. Teilweise besteht ein Wechselspiel zwischen einzelnen Ursachen und dem Beitragssatz. Beispielhaft kann auf den Zusammenhang zwischen Lohnnebenkosten, Beitragssatz und Arbeitslosenquote verwiesen werden. Nahezu einhellig wird in der Wirtschaft darauf hingewiesen, dass ein Anstieg der Lohnnebenkosten, zu denen auch der Arbeitgeberanteil der Krankenversicherungsbeiträge zählt, mitursächlich für eine Erhöhung der Arbeitslosenquote sei. Eine höhere Arbeitslosenquote führt zu geringeren Beitragszahlungen. Bei einem Rückgang der Beitragszahlungen besteht die Gefahr der Erhöhung des Beitragssatzes durch die Krankenkassen. Dadurch erhält das System eine gefährliche Eigendynamik.

Durch die jüngste Gesundheitsreform, die am 01.01.2004 in Kraft getreten ist, ist versucht worden, einer weiteren Beitragssatzerhöhung entgegenzuwirken. Unverkennbar sind die Bemühungen, innerhalb der gesetzliche Krankenversicherung Wettbewerbselemente einzuführen und die gesetzliche Krankenversicherung der privaten Krankenversicherung anzunähern. Dies vor der zunehmenden Erkenntnis, dass ein vollumfänglicher Versicherungsschutz alten Zuschnitts angesichts sich

[9] Vgl. Henke/Berhanu/Mackenthun, Die Zukunft der Gemeinnützigkeit von Krankenhäusern, S. 5 f.; siehe auch SG Hamburg vom 13.11.2002, Az.: S 23 1386/01.
[10] Vgl. zur Übersicht, Waltermann, Sozialrecht, Rn. 134.

veränderndner Rahmenbedingungen mit dem bisherigen System nicht finanzierbar ist. Langfristig ist mit tiefgreifenden Umstellungen zu rechnen. Diskutiert wurde mittelfristig die Einführung einer so genannten „Bürgerversicherung“ oder einer einheitlichen Pauschale, sog. „Kopfpauschale“, positiver als „Gesundheitsprämie“ bezeichnet. Bei dem letztgenannten Modell wäre eine Entkopplung der Beitragssätze vom Faktor Lohn möglich[11]. Als Kompromiss beider Positionen zeichnet sich die Einführung eines „Gesundheitsfonds“ ab. Nach dem Gesetz zur Stärkung des Wettbewerbs in der Gesetzlichen Krankenversicherung (GKV-WSG) soll im Zuge der jüngsten Gesundheitsreform der Gesundheitsfond im Jahr 2009 eingeführt werden.

Eine weitere nicht zu vernachlässigende Ursache der Finanzschwierigkeiten sind hohe Verwaltungskosten bei Teilen der gesetzlichen Krankenkassen. Diese Ausgaben zu senken muss ebenfalls Ziel gesetzgeberischer Reformtätigkeit sein, gerade und auch im Interesse der Versicherten. Das GKV-Modernisierungsgesetz enthält mit Einführung der elektronischen Kommunikation und der Erweiterung der bisherigen Chipkarte zur elektronischen Gesundheitskarte Ansätze zu einer Kostensenkung in diesem Bereich[12].

Das Problem hoher Verwaltungskosten ist nicht auf die gesetzlichen Krankenkassen beschränkt. Auch bei anderen Einrichtungen, beispielsweise bei Krankenhäusern oder privaten Krankenversicherungsunternehmen, stellen Verwaltungskosten einen großen Teil der Ausgaben dar. Hinzu kommt, dass auch die kapitalgedeckte private Krankenversicherung, die jeden Einzelnen nach individueller Risikoeinschätzung versichern kann, nicht vor den demographischen Einflüssen, der Zunahme der Leistungserbringer sowie dem Fortschritt in der Medizin verschont bleibt.

Unabhängig von gesetzgeberischen Reformprojekten erscheint das „Datenoutsourcing“ als ein mögliches Instrumentarium zur Kostensenkung.

---

[11] Vgl. IDZ, Information, Nr. 1/2005 vom 17. März 2005 unter http://www.idz-koeln.de/m3-d.htm.

[12] Zur elektronischen Gesundheitskarte vgl. Bizer, DuD 2004, S. 243; Weichert, DuD 2004, S. 391; BSI, Chipkarten im Gesundheitswesen; Hornung, DuD 2004, S. 15, sowie umfassend Iwanski, Datenschutzrechtliche Probleme von Chipkarten; auf Herausforderungen an die ärztliche Schweigepflicht hinweisend Schirmer, in: Rossnagel, Handbuch des Datenschutzrechts, S. 1362; vgl. zur rechtspolitischen Entwicklung Schnorr/Wissing, ZRP 2001, S. 487.

III. Einsatzmöglichkeiten

Die Einsatzmöglichkeiten des Outsourcings von Datenverwaltung und Datenverarbeitung sind vielfältig. Im Bereich des Gesundheitswesens praktiziert man die Speicherung von Krankenhausdatenbeständen durch externe Speicherfirmen[13]. Dabei bedient sich der Outsourcer der Speicherfirma gleichsam als externes Speichermedium. Hierin erschöpft sich die Aufgabe des externen Anbieters. Neben Krankenhäusern kommen auch größere Praxisnetze im Rahmen der integrierten Versorgung und neu entstehende medizinische Versorgungszentren für diese Form des Outsourcings in Betracht. Aufgrund der geschaffenen Möglichkeit zur Bildung größerer Einheiten, unter deren Dach vielfältig spezialisierte Leistungen angeboten werden, ist, einhergehend mit dem Anstieg der pro Einheit zu verwaltenden Datenmengen, mit einer Ausweitung solcher Outsourcinglösungen zu rechnen.

Einen weitergehenden Schritt stellt das Bereitstellen externer Plattformen durch private Anbieter für die Umsetzung der elektronischen Gesundheitskarte dar. Hierbei sind neben der Frage der Einrichtung eines zentralen Datenpools[14] auch ständige Interaktionen zwischen Outsourcer und Anbieter sowie zwischen Patient und Anbieter technisch zu lösen[15]. Die Anforderungen im technischen und rechtlichen Bereich sind hier weitergehender als bei der reinen externen Speicherung. Bei rechtsfähigen, öffentlich-rechtlichen Institutionen ist die Gründung eines privatrechtlichen Unternehmens möglich, an das dann interne Funktionen fremd vergeben werden[16]. Denkbar ist aber auch die Kooperation mit anderen öffentlich-rechtlichen Einrichtungen oder mit Privaten in bestimmten Tätigkeitsbereichen[17]. In der medizinischen Forschung ist das Betreiben von Datenbanken mit medizinischen Daten durch nicht öffentliche Stellen von Interesse[18].

---

[13] Vgl. Weichert, MedR 2003, S. 678; http//www.datenschutzzentrum.de/material/themen/gesund/dslabor.htm; Braunschweig/Geis/-Tolksdorf/Hansen, MedR 2004, S. 353; Klöcker/Meister, Datenschutz im Krankenhaus, S. 74 ff.

[14] Dazu Vetter, DuD 2003, S. 39 ff.

[15] Vgl. auch Schirmer, in: Roßnagel, Handbuch des Datenschutzrechts, S. 1386 ff. sowie die Fundstellen unter Fußnote 12.

[16] Zur Gründung einer gemeinnützigen Labor GmbH durch einen öffentlich-rechtlichen Krankenhausträger vgl. Dessauer, MedR 1993, S. 379.

[17] Vgl. OVG Nordrhein-Westfalen, RDV 2006, S. 75 ff. zur Überlassung von beihilferechtlichen Daten an den Kreis sowie BGHZ 64, 232 ff. zur Kooperation zwischen gesetzlichen und privaten Krankenversicherungsunternehmen hinsichtlich einer Krankenhauszusatzversicherung.

[18] Vgl. Sokol, DuD 2001, S. 5 ff. und NJW 2002, S. 1767; Wellbrock, MedR 2003, S. 77; Schulz, DuD, S. 12 ff.

IV. Wirtschaftlicher Hintergrund

Die Entwicklung des Outsourcing ist vor dem Kontext historisch- wirtschaftlicher Entwicklung zu begreifen. War die Wirtschaft im ausgehenden 19. Jahrhundert und angehenden 20. Jahrhundert noch durch vergleichsweise geringe Konzentration, einen kleinen industriellen Sektor, geringen Automatisierungsgrad und einen großen landwirtschaftlichen Sektor geprägt, hat sich dies zum Anfang des 21. Jahrhunderts grundlegend geändert. Der Landwirtschaftssektor ist im Zuge der Industrialisierung zurückgedrängt worden. Gleichzeitig hat sich neben der Landwirtschaft und der Industrie ein dritter Sektor, der Dienstleistungssektor entwickelt. Heute nimmt der Dienstleistungssektor mehr als die Hälfte des Bruttoinlandproduktes ein.

Die Produktionsprozesse sind infolge des rasanten technischen Fortschritts zunehmend komplexer geworden, auch mit der Folge, dass aufgrund technischer Neuerungen Risiken entstanden sind, die rechtlich bewältigt werden mussten und müssen[19]. Die Zahl der Produktionsstufen, -formen und -abläufe hat sich stark erhöht. Es entstanden große Produktionseinheiten mit mehrfacher horizontaler und vertikaler Gliederung, in denen die Zuordnung von individueller Verantwortlichkeit zunehmend schwieriger geworden ist[20]. Das Prinzip arbeitsteiligen Vorgehens gewann stetig an Bedeutung. Gleiche Erscheinungen sind beim Absatz festzustellen[21].

Gleichzeitig nahmen internationale wirtschaftliche Verflechtungen zu. Das Schlagwort der „Globalisierung“[22] kennzeichnet eine Entwicklung dahingehend, dass Produktion, Dienstleistung, Absatz und Unternehmensstruktur zunehmend nicht mehr national begrenzt sind. Auslagerungen von Produktions- oder Dienst-

---

[19] Näher aus strafrechtlicher Sicht Hilgendorf, Strafrechtliche Produzentenhaftung in der „Risikogesellschaft“, S. 23 ff.

[20] Dies zeigt sich auch daran, dass § 831 BGB, der nicht auf die Risikotragung arbeitsteiligen Verhalten zugeschnitten ist, als unzureichend empfunden wird. So erfolgt im Bereich der deliktischen Produzentenhaftung überwiegend die Ansiedlung von Verkehrssicherungspflichten im Bereich des § 823 Abs. 1 BGB statt in § 831 BGB, vgl. dazu nur Belling/Eberl-Borges, in: Staudinger, BGB § 823 Rn. 5 und 10; operiert wird dabei im Rahmen des § 823 Abs. 1 BGB mit dem Begriff des „Organisationsverschuldens“, dazu Palandt, BGB, § 823 Rn. 206; auf neuere Entwicklungen im Bereich der Produktion und des Absatzes geht Kupjetz, Moderne Produktions- und Absatzformen, S. 1ff ein; den Aspekt des „Organisationsverschuldens“ im Krankenhausbereich thematisieren Zwiehoff, MedR 2004, S. 364 und Deutsch, NJW 2000, S. 1745.

[21] Dazu Kupjetz, Moderne Produktions- und Absatzformen, S. 1 ff.

[22] Vgl. im Zusammenhang mit dem Outsourcing Bizer, in: Simitis, BDSG, § 3a Rn.16.

leistungsabläufen ins Ausland oder auf externe Unternehmen sind häufig Ausdruck einer Strategie, global und mit hoher Mobilität zu agieren und Kostenvorteile, insbesondere im Lohnbereich, zu realisieren. Dies gilt umso mehr als hohe Produktivitätssteigerungen und Wachstumsraten, welche die hohen Kosten kompensieren könnten, nicht mehr zu erwarten sind. Hier gewinnt der Aspekt der Kostensenkung und Effizienzsteigerung durch Auslagerung vermehrt an Bedeutung.

Dabei kommt auch der Auslagerung von Abläufen innerhalb nationaler Grenzen erhebliches Gewicht zu. Verstärkt wird dieser Gesichtspunkt durch den Einsatz moderner Informationstechnologien. Das angebrochene Zeitalter der Digitalisierung und der Informationsgesellschaft ermöglicht in Verbindung mit steigender Vernetzung und raschen neuen Übertragungstechniken ein ungeahntes Maß an Informationszunahme und Mobilität von Daten. Das kostengünstige verwalten riesiger Informationsmengen und Datenaufkommen wird daher eine große Herausforderung der Zukunft in der Informationsgesellschaft[23] sein. Für Unternehmen und Einrichtungen kann diese Herausforderung einen neuralgischen Punkt darstellen[24].

Betriebswirtschaftlich rückt dabei das Outsourcing verstärkt in den Mittelpunkt des Interesses. Die Bestrebungen zum Outsourcing von Datenverwaltung und Datenwartung, aber auch von anderen Prozessen, sind betriebswirtschaftlich durch Flexibilitätssteigerungen, Senkung der Investitionskosten sowie der laufenden Kosten und Effizienzsteigerung motiviert. Diese betriebswirtschaftlichen Überlegungen gelten für das Outsourcing unterschiedlichster Aufgaben im privatwirtschaftlichen und im öffentlich-rechtlichen Bereich[25].

---

[23] Kennzeichnend ist der Einsatz sog. „data warehouse“ Lösungen, vgl. Sinz, Datenschutz und Datensicherheit in einem landesweiten Data-Warehouse-System für das Hochschulwesen, S. 1 ff und Wilmes, Die strategische Ressource „data warehouse“, S.1 ff. Im öffentlichen Bereich haben auf dem Weg zur Informationsgesellschaft die Länder Brandenburg, Nordrhein-Westfalen, Schleswig-Holstein sog. Informationsfreiheitsgesetze erlassen, ein Bundesgesetz ist zum 01.06.2006 in Kraft getreten; hinzuweisen ist auch auf die Diskussion zum E-Government, vgl. dazu die Meldung in der Süddeutschen Zeitung Nr. 165 vom 20. Juli 2004, S. 8.

[24] Man muss sich nur vor Augen halten, dass eine einzelne, dreidimensionale, computergestützte tomographische Aufnahme des menschlichen Körpers heute schon ein Datenvolumen im zweistelligen Gigabytebereich hat. Korrespondierend zu der großen Datenmenge ist die Auflösung solcher Aufnahmen so gut, dass die Gefahr besteht, die Person zu erkennen.

[25] Zum Bereich der Sozialverwaltung vgl. Hartmann, Outsourcing in der Sozialverwaltung und Sozialdatenschutz, S. 20; für den Bereich der Steuerverwaltung vgl. Topp, in: Rossnagel, Handbuch des Datenschutzrechts, S. 1683 f.; vgl. auch den Beitrag in der Süddeutschen Zeitung Nr. 165 vom 20. Juli 2004, S. 8; aus wirtschaftlicher Sicht für den öffentlich-rechtlichen Bereich vgl. Stößel, Outsourcing in der öffentlichen Verwaltung und Proeller, Auslagerung in der hoheitlichen Verwaltung S. 1 ff.

Im öffentlich-rechtlichen Sektor wird das Outsourcing an private Unternehmen von den Schlagwörtern „Liberalisierung staatlicher Monopole“, „Wettbewerbsorientierung“, „Dienstleistungsorientierung staatlichen Handelns“, „Privatisierung“ und „Public Private Partnership“ begleitet[26]. Beispielhaft seien die Liberalisierung des nationalen Strommarktes, die Privatisierungen im Telekommunikations- und Postbereich, die Zusammenarbeit der Bundesregierung mit dem Konsortium TollCollect zur Einführung eines einheitlichen LKW-Mauterfassungssystems[27] sowie die Modernisierung der IT-Technik der Bundeswehr genannt[28]. Aber auch bei Verwaltungsreformdiskussionen spielt das Thema Outsourcing zur Effizienzsteigerung eine Rolle.

Das Outsourcing von Daten im Besonderen im öffentlich-rechtlichen Bereich ist in den größeren Kontext der Reduzierung der Aufgabenerfüllung durch staatliche Einrichtungen sowie des Einzuges marktwirtschaftlicher Elemente zu stellen. Gerade das Einschalten Privater zur Aufgabenerfüllung, sei es in Kooperation mit privatrechtlichen Einrichtungen oder durch Privatisierung, ist eine Reaktion auf die Zunahme des staatlichen Leistungskatalogs, Kostensteigerungen in der öffentlichen Verwaltung und den Einbruch staatlicher Einnahmen. Die schwierige Haushaltslage im öffentlich-rechtlichen Bereich zwingt zu alternativen Handlungskonzepten unter Orientierung an marktwirtschaftlichen Kriterien sowie dazu, die alte Forderung nach einem „Weniger an Staat“ verstärkt anzugehen.

Ein „Weniger an Staat“ ist aber nicht zwangsläufig verbunden mit effizienteren und kostengünstigeren Lösungen. Tatsächlich sind auch erhebliche wirtschaftliche Risiken mit der Einschaltung Privater verbunden[29]. Ein besonders drastisches Risiko ist das Ausfall- und Insolvenzrisiko. Das Beispiel TollCollect zeigt mit den erfolgten Einnahmenausfälle aufgrund der Verzögerung der Einführung des Mauterfassungssystems wegen technischer Schwierigkeiten die Gefahren bei der Einschaltung Privater. Letztlich droht, dass den Ausfall oder die Insolvenz Priva-

[26] Vgl. Lensdorf/Steger, CR 2005, S. 161, die auf vergaberechtliche Aspekte bei Public-Private-Partnership eingehen; zur Zulässigkeit von Public Private Partnership bei der Einziehung öffentlicher Forderungen Abel/Karpenstein, RDV 2005, S. 15; zu privaten Sicherheitsdiensten Stober, ZRP 2001, S. 260 ff.

[27] Zum Fall TollCollect unter informationsrechtlichen Gesichtspunkten, Püschel, DuD 2004, S. 290.

[28] Vgl. Süddeutsche Zeitung Nr. 224 vom 27. September 2004, S. 8.

[29] Vgl. zu Gründen für und gegen das Outsourcing Hartmann, Outsourcing in der Sozialverwaltung und Sozialdatenschutz, S. 20.

ter, die in die Aufgabenerfüllung eingeschaltet worden sind, bei ungenügender vorsorgender Absicherung der öffentlichen Hand, der Steuerzahler zu tragen hat. Der wirtschaftliche Erfolg privater Akteure ist keinesfalls garantiert. Hinzu kommt die Gefahr, dass mit dem Outsourcing von Leistungen an Private der Preis für diese Leistungen leichter steigen kann und zudem die Gefahr der Abhängigkeit von bestimmten privaten Dienstleistungsunternehmen besteht. Die finanzielle (Folgen)-Verantwortung ist daher bei Outsourcingprojekten ein zu beachtender Faktor.

V. Auswirkungen

Outsourcing bedeutet arbeitsteiliges Vorgehen zwischen Outsourcer und anbietendem Dienstleister. In der Konsequenz besteht für Dritte, die durch diese Vorgehensweise nachteilig betroffen werden, oftmals die Schwierigkeit, einen einheitlich verantwortlichen Ansprechpartner zu finden. Die Frage der Verantwortlichkeit für rechtswidrige Handlungen Dritten gegenüber muss entschieden werden, um die zivilrechtlichen, öffentlich-rechtlichen oder strafrechtlichen Konsequenzen beurteilen zu können[30]. Dies ist generell ein Phänomen arbeitsteiligen Vorgehens. Es stellt sich beispielsweise auch im Rahmen der Produzentenhaftung sowie generell bei kooperativen Zusammenschlüssen mit der Konstellation eines Mehrpersonenverhältnisses.

Dabei ist zu prüfen, wie neue Erscheinungsformen vom bestehenden Recht erfasst werden oder inwiefern eine Anpassung erforderlich erscheint. Hier liegt ein Hauptproblem in einer sachgerechten Zurechnung der Verantwortlichkeit sowohl

[30] Normen, die die Risiken arbeitsteiligen Vorgehens zuordnen, sind beispielsweise §§ 31, 89, 278 BGB; vgl. zu weiteren Normen Belling/Eberl-Borges, in: Staudinger, BGB, § 831 Rn. 18 f. Eine weitere Möglichkeit besteht in der Zuordnung von Risikosphären und der Etablierung von Gefährdungstatbeständen unter Abkehr vom Verschuldensprinzip. Vielfach sind solche Gefährdungstatbestände als Reaktion auf das Versagen herkömmlicher rechtlicher Instrumentarien geschaffen worden. So ist § 84 AMG als Reaktion auf den berühmten Contergan Fall, LG Aachen JZ 1971, S. 511 ff, entstanden, vgl. Hilgendorf, Strafrechtliche Produzentenhaftung in der „Risikogesellschaft“, S. 12. Auch im Bereich der Produzentenhaftung ist durch das Produkthaftungsgesetz eine Gefährdungshaftung eingeführt worden. Eine weitere Möglichkeit besteht in der Einführung von Beweiserleichterung bis hin zur Beweislastumkehr, wie sie beispielsweise in der zivilrechtlichen Produzentenhaftung durch die Rechtsprechung vollzogen worden ist. Dabei hat die Rechtsprechung bei der deliktischen Produzentenhaftung § 823 Abs. 1 BGB derart modifiziert, dass er sich in diesem Bereich einer Gefährdungshaftung annähert, vgl. dazu Hilgendorf, Strafrechtliche Produzentenhaftung in der „Risikogesellschaft“, S. 83 ff. Aktuell ist im Gentechnikgesetz ein verschuldensunabhängiger Haftungstatbestand eingeführt worden.

unter dem Gesichtspunkt der Zulässigkeit arbeitsteiligen Vorgehens als auch unter dem Gesichtspunkt der strafrechtlichen und zivilrechtlichen Konsequenzen. Zu trennen ist die Zurechnung zivilrechtlicher, öffentlich-rechtlicher und strafrechtlicher Verantwortlichkeit. Erstere betrifft hauptsächlich die Feststellung einer materiellen Ausgleichspflicht unter den Beteiligten oder im Verhältnis zu Dritten[31]. Die Klärung öffentlich-rechtlicher Verantwortlichkeit geht einher mit der Frage der Zulässigkeit und Rechtmäßigkeit staatlichen Handelns[32]. Strafrechtliche Verantwortlichkeit ist für das Feststellen der Strafbarkeit einer Person von Bedeutung.

Entsprechend dem Ziel dieser Arbeit wird lediglich auf die strafrechtlichen Aspekte des Outsourcings von medizinischen Daten eingegangen. Ob ein geplantes Outsourcingprojekt gegen eine Strafrechtsnorm verstößt, hat neben der Strafbarkeitsfrage auch Bedeutung für das Zivilrecht, beispielsweise für die Wirksamkeit von zivilrechtlichen Verträgen[33], für wettbewerbsrechtliche Verstöße[34], im Bereich des Schadensersatzes und Schmerzensgeldes[35] oder für Unterlassungsansprüche[36]. Im Folgenden soll untersucht werden, inwiefern bei Outsourcingvorhaben von medizinischen Daten de lege lata die Gefahr der Verwirklichung eines Straftatbestandes besteht und ob de lege ferenda Änderungen angezeigt sind. Dabei soll im Zusammenhang mit Fragen des materiellen Strafrechts auch auf dazugehörige Probleme des formellen Strafrechts eingegangen werden.

---

[31] Hier ist die Begründung eines Schadensersatzanspruches von Interesse. Zu denken ist an vertragliche wie gesetzliche Ansprüche auf Schadensersatz im BGB oder in anderen Gesetzen, vgl. Bake, Datenschutz und Datensicherheit im Gesundheitswesen, S. 70 f.

[32] Zu diesem Aspekt vgl. Hartmann, Outsourcing in der Sozialverwaltung und Sozialdatenschutz S. 1 ff.

[33] Vgl. die Grundsatzentscheidung BGHZ 115, 123 zur Nichtigkeit des Vertrages über die Beauftragung einer privatärztlichen Verrechnungsstelle wegen Verstoßes gegen § 203 StGB; eingehend zu dieser Problematik Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 125 ff.

[34] Ein Verstoß gegen § 1 UWG wurde beispielsweise in dem Urteil des Oberlandesgerichts Düsseldorf angenommen, OLG Düsseldorf, CR 1997, S. 536 ff.; zur Bedeutung von Strafrechtsverstößen im Rahmen des § 823 Abs. 2 vgl. Palandt, BGB, § 823 Rn. 149.

[35] OLG München vom 18. Dezember 1997, Az.: 1 U 5625/95 und BGH vom 3. November 1998 Az.: VI ZR 47/98; vgl. auch Lilie, Medizinische Datenverarbeitung, Schweigepflicht und Persönlichkeitsrecht, S. 55.

[36] Vgl. dazu OLG Hamm vom 9. November 1994, Az.: 3 U 120/94.

B. Datenfluss zwischen den Beteiligten

I. Rechtlicher Rahmen

Mit dem Begriff „Outsourcing“ sind, wie dargelegt, unterschiedliche Sachverhalte verbunden. Vor dem Eingehen auf die Gefahr einer möglichen Straftatbestandsverwirklichung ist der rechtliche Rahmen für Outsourcingprojekte zu bestimmen.

1. Daten als Gegenstand des Outsourcings

Sind medizinische Daten Gegenstand des Outsourcings, ist zur rechtlichen Einordnung zu klären, was unter medizinischen Daten zu verstehen ist. Sprachlich leitet sich der Begriff „Medizin“ ursprünglich vom lateinischen Wort „medicina“ ab und bedeutet ärztliche (Heil-)Kunst. Heute ist darunter zum einen die Wissenschaft vom gesunden und kranken Menschen, von den Ursachen, den Wirkungen, der Vorbeugung und Heilung von Krankheiten zu verstehen. Zum anderen werden damit die Arzneimittel bezeichnet[37].

Der Begriff „Daten“ ist lateinischer Herkunft. Das Datum leitet sich von dare ab und ist mit dem Angegebenen oder dem Bezeichneten zu übersetzten. Die sprachliche Bedeutung zieht unmittelbar die Frage nach sich, was das Angegebene oder Bezeichnete ist, zielt also auf einen Inhalt. Daraus kann abgeleitet werden, dass Daten auf eine Nachricht bezogen sind, oder anders ausgedrückt, dass in den Daten eine verkörperte Information enthalten ist. Nach heutigem technischen Verständnis sind entsprechend einer Konvention in der deutschen Industrienorm DIN 44300 Nr. 19 unter Daten Zeichen zu verstehen, die zum Zweck der Verarbeitung Informationen aufgrund bekannter oder unterstellter Abmachungen darstellen[38]. Unter diesem Aspekt können unter medizinischen Daten all diejenigen dargestellten Informationen verstanden werden, die in Beziehung zu Gesundheit oder Krankheit stehen[39]. Diese Daten stammen primär aus der Beziehung zwischen Patient und unmittelbar Behandelnden, können aber auch von dritten Beteiligten aus dem Gesundheitswesen herrühren, sofern sie einen Krankheits- bzw. Gesund-

[37] Pschyrembel, Klinisches Wörterbuch, S. 1036.
[38] Podlech, Der Informationshaushalt der Krankenkassen, S. 20 (Fußnote 1).
[39] Ähnlich Seelos, Wörterbuch der medizinischen Informatik, S. 317; siehe auch Vahle, DuD 2001, S. 614.

heitsbezug aufweisen. Sie müssen sich nicht notwendig auf einen Patienten beziehen.

Andere Ansätze gehen von dem Bereich, in dem die Daten verarbeitet werden, aus. So ist in der medizinischen Informatik im Zusammenhang mit telematischen Anwendungen eine Einteilung der „medizinischen Daten“ in patientenbezogene Daten, medizinisches Wissen und Verwaltungsdaten üblich[40]. Patientenbezogene Daten beinhalten Informationen, die einem Individuum unmittelbar zugeordnet werden können. Medizinisches Wissen enthält Erkenntnisse der Medizin als Wissenschaft. Diese Daten sind in anonymer Form veröffentlicht[41]. Verwaltungsdaten sind Daten mit Bedeutung für die Überprüfung und Abrechnung medizinischer Leistungen. Eine andere Einteilung für die Verarbeitung von Daten in Informationssystemen im Gesundheitswesen geht von dem Überbegriff „Patientendaten“[42] aus. Die Patientendaten untergliedern sich in Identifikationsdaten, (Name, Geburtsdatum, Adresse, evtl. Krankenkassennummer, sowie krankenhausinterne Identifikatoren), administrative Daten (Versicherungsdaten, Bewegungsdaten, weitere fallbezogene Daten wie z.B. Wahlleistungen) und medizinische Daten (allgemeine anamnestische Daten, abrechnungsrelevante Diagnosen und Therapien, Befunde, Laborwerte und andere diagnostische und therapeutische Daten, besonders sensible Daten, wie z. B. psychiatrische Daten, bestimmte Befunde, genetische Daten)[43]. Als medizinische Daten werden bei dieser Einteilung nur solche Daten erfasst, die im Zusammenhang mit dem individuellen Gesundheitszustand eines Patienten stehen. Diese Einteilung erfolgt mit Blick auf die Sensibilität der Daten für den Persönlichkeitsbereich des Patienten.

Für die rechtliche Beurteilung sind diese Einteilungen nicht maßgeblich. Vielmehr ist für jedes medizinische Datum der Bezug zu einer den Umgang mit Daten regelnden Norm ausschlaggebend. Für eine Zuordnung zu einer Rechtsnorm ist die durch das Outsourcing betroffene Datenart und die Qualifikation der am Outsourcing Beteiligten determinierend. Im Rahmen einer strafrechtlichen Beurteilung ist zu fragen, ob es sich bei den zu prüfenden „medizinischen Daten“ um Daten handelt, die einem strafrechtlichen Geheimnisschutz unterliegen. Im Bereich des

[40] Lehmann/Mayer, Handbuch der medizinischen Informatik, S. 571 f.
[41] Zur problematischen Veröffentlichung von Patientenfotos in Fachzeitschriften vgl. Schlund, MedR 1990, 323.
[42] Allgemein zu dem Begriff Seelos, DuD 1993, S. 433 ff.
[43] Bake, Datenschutz und Datensicherheit, S. 77 f.

strafrechtlichen Schutzes des „Privatgeheimnisses“ nach § 203 StGB ist allein von Bedeutung, ob Daten betroffen sind, die dem Geheimnisbegriff des § 203 StGB unterfallen. Eine Legaldefinition des Geheimnisses besteht hier nicht.

Hinsichtlich strafrechtlicher Regelungen zum Schutz des Datengeheimnisses ist der Umgang mit personenbezogenen Daten von zentraler Bedeutung[44]. Damit ist für das Outsourcing medizinischer Daten relevant, ob durch das Outsourcing-vorhaben Daten betroffen sind, die einen Personenbezug aufweisen. Der Begriff „personenbezogene Daten“ wird im Bundesdatenschutzgesetz legaldefiniert. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. In § 3 Abs. 8 BDSG sind Gesundheitsdaten als besondere personenbezogene Daten erwähnt. In diesem Zusammenhang ist auch § 28 Abs. 7 BDSG zu erwähnen, der zusammen mit § 3 Abs. 8 BDSG das zentrale Gerüst des medizinischen Datenschutzes darstellt[45]. Diese Vorschriften setzen Vorgaben der EG Datenschutzrichtlinie 95/46/EG um, die in Art. 8 Abs. 1 und Abs. 3 Gesundheitsdaten als besondere personenbezogene Daten nennt.

Bezüglich des strafrechtlichen Sozialgeheimnisschutzes nach § 85 SGB X ist maßgeblicher gesetzlicher Anknüpfungspunkt der Begriff der „Sozialdaten“. § 67 SGB X definiert Sozialdaten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in § 35 SGB I des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden.

Unter den Datenarten sind Überschneidungen denkbar. Medizinische Daten können zugleich Sozialdaten im Sinne von § 35 SGB I[46], personenbezogene Daten im Sinne der Datenschutzregelungen und Daten, die dem Schutz nach § 203 StGB unterworfen sind, sein. Andererseits ist auch vorstellbar, dass medizinische Daten personenbezogene Daten sind, aber nicht „Geheimnisse“ i.S.v. § 203 StGB. Eine

[44] Vgl. § 46 BDSG; ähnliche Vorschriften finden sich in den meisten Landesdatenschutzgesetzten, z.B. Art. 37 Bayerisches Datenschutzgesetz.
[45] Schirmer, in: Rossnagel, Handbuch des Datenschutzrechts, S. 1363.
[46] Scholz, in: Kassler Kommentar Sozialversicherungsrecht, § 76 SGB X Rn. 4.

nähere Abgrenzung kann nur für den konkreten Einzelfall nach Auslegung der jeweiligen Regelung erfolgen.

2. Das Recht auf informationelle Selbstbestimmung

Outsourcingprojekte von medizinischen Daten implizieren ein Zugänglichmachen dieser Daten. Soweit solche Daten sensible Informationen, beispielsweise über den Gesundheitszustand einer Person, enthalten, besteht ein natürliches Interesse der Person am Schutz dieser Daten sowie daran, dass sie selbst darüber bestimmen kann, an wen diese Daten gelangen. Ausgangspunkt rechtlicher Überlegungen ist die Frage nach der Berechtigung zur Erhebung, Verarbeitung und Weitergabe von Daten, die sensible Informationen über Personen enthalten.

Hierzu hat das Bundesverfassungsgericht im so genannten „Volkszählungsurteil" grundsätzlich Stellung genommen[47]. Vor dem Hintergrund einer datenmäßigen Erfassung der Bevölkerung durch das Erhebungsprogramm des Volkszählungsgesetzes von 1983 hat das Bundesverfassungsgericht dem Einzelnen ein Recht auf informationelle Selbstbestimmung zuerkannt, welches sich als Teil des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ableitet.

Die Entwicklung des Rechts auf informationelle Selbstbestimmung im Volkszählungsurteil geht auf eine stetige Stärkung des allgemeinen Persönlichkeitsschutzes durch die Rechtsprechung zurück. Schon im Jahre 1954 griff der Bundesgerichtshof zur Herleitung eines allgemeinen Persönlichkeitsrechts auf Art. 1 und Art. 2 GG zurück[48]. Im weiteren Verlauf entwickelte das Bundesverfassungsgericht das allgemeine Persönlichkeitsrecht fort[49]. Differenziert wurde zwischen Individualsphäre, Privatsphäre und Intimsphäre[50]. Bezüglich der Intimsphäre besteht nach der Rechtsprechung und der h.L. ein absolutes Eingriffsverbot[51]. Hinsichtlich der anderen Sphären besteht eine, entsprechend der unterschiedlichen Schutzintensität

---

[47] BVerfGE 65, 1.
[48] BGHZ 13, 334 (338).
[49] Vgl. zur Entwicklung Lang, Das Recht auf informationelle Selbstbestimmung, S. 28 ff.; Simitis, NJW 1984, S. 398; Klöcker/Meister, Datenschutz im Krankenhaus, S. 10 ff.
[50] Näher zu dieser Unterscheidung BVerfGE 35, 35 (39 f.); Di Fabio, in: Maunz-Dürig, Grundgesetz, Art. 2 Rn. 158 ff.
[51] Zu diesem unantastbaren Kernbereich Schmitt-Glaeser, in: Isensee/Kirchhof, Handbuch des Staatsrechts, VI § 129, Rn. 35.

der Sphären, gestufte Möglichkeit der Einschränkung unter bestimmten Voraussetzungen[52]. Dem allgemeinen Persönlichkeitsrecht wurde daneben eine aktive und eine passive Schutzrichtung zugemessen[53]. Die passive Schutzrichtung erfasst die Abwehr des Einzelnen gegen Eingriffe von außen. Der einzelnen Person soll ein geschützter Rückzugsraum zustehen. Dieser Aspekt kann überzeugend durch die Sphärentheorie der Rechtsprechung und der Lehre erklärt werden[54]. Die aktive Schutzrichtung erfasst die Selbstdarstellung der einzelnen Person nach außen. Über diese Außendarstellung soll der Einzelne grundsätzlich selbst bestimmen dürfen[55].

Im Volkszählungsurteil nimmt das Bundesverfassungsgericht zu dem Recht auf informationelle Selbstbestimmung vor dem Hintergrund der Datenerhebung und automatisierten Datenverarbeitung ausführlich Stellung. Dem Urteil kommt für den Bereich des Informationsflusses als Weichenstellung grundsätzliche Bedeutung zu. Rechtsnormen des öffentlichen Rechts in diesem Bereich sind vor dem Hintergrund dieser Rechtsprechung zu betrachten und am Recht auf informationelle Selbstbestimmung zu messen.

Erkannt wurden die Gefahren des durch Computereinsatzes erleichterten Datenflusses[56]. Gefahren liegen darin, dass Unberechtigte auf nicht nachvollziehbarem und unkontrolliertem Weg Kenntnis von persönlichen Daten erlangen und diese beliebig austauschen, einsehen und manipulieren können[57]. Hinzu kommt die rasante Entwicklung des Internets sowie anderer dezentraler, technischer Kommunikationsnetze mit grenzüberschreitender Verbindung. Der Aufenthaltsort persönlicher Daten lässt sich dadurch nahezu beliebig verschieben. Der Einsatz zentraler, vergleichsweise abgrenzbarer elektronischer Datenverarbeitungsanlagen ist technisch überholt. Hierdurch entstehen für den Einzelnen kaum nachvollziehbare Missbrauchs- und Manipulationsmöglichkeiten[58]. Durch das Recht auf informati-

---

[52] Di Fabio, in: Maunz-Dürig, Grundgesetz, Art. 2 Rn. 172.
[53] Vgl. dazu Schmitt- Glaeser, in: Isensee/Kirchhof, Handbuch des Staatsrechts, VI, § 129 Rn. 19.
[54] Vgl. dazu Schmitt- Glaeser, in: Isensee/Kirchhof, Handbuch des Staatsrechts, VI, § 129 Rn. 15, der zutreffend darauf hinweist, dass der aktive Aspekt nicht überzeugend mit der Sphärentheorie erklärbar sei, weshalb die Sphärentheorie um das externe Element der Möglichkeit autonomer Selbstdarstellung ergänzt werden müsse.
[55] Vgl. dazu das „Lebach"-Urteil, BVerfGE 35, 202 (220).
[56] BVerfGE 65, 1 ff.
[57] Dreier, in: Dreier, Grundgesetz, Art. 2 Rn. 53; Di Fabio, in: Maunz-Dürig, Grundgesetz, Art. 2 Rn. 173.
[58] Vgl. dazu Süddeutsche Zeitung vom 29.07.2004, Nr. 165, S. 8.

onelle Selbstbestimmung wird dem Einzelnen gewährleistet, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Aufgrund der Gefahren des Einsatzes elektronischer Datenverarbeitung sind alle personenbezogenen Daten geschützt. Kein Datum kann als belanglos a priori aus dem Schutzbereich aussortiert werden[59].

Das Recht auf informationelle Selbstbestimmung gilt jedoch nicht schrankenlos. Einschränkungen sind im überwiegenden Allgemeininteresse und auf Grundlage einer verfassungsmäßigen, gesetzlichen Ermächtigung möglich[60]. Erforderlich ist ein Gesetz im materiellen Sinne. Ausreichend können auch Satzungen oder Verordnungen sein[61]. Allerdings haben die Regelungen den Grundsatz der Verhältnismäßigkeit zu beachten[62]. Schließlich muss auch der Eingriff in das Recht auf informationelle Selbstbestimmung auf Grundlage der Regelung geeignet, erforderlich und angemessen hinsichtlich des verfolgten Zweckes sein. Da der Zweck nur ein überwiegendes Allgemeininteresse sein kann, hat eine Abwägung zwischen der Maßnahme, die in das Recht auf informationelle Selbstbestimmung eingreift, und dem überwiegenden Allgemeininteresse zu erfolgen[63]. Zur Bestimmung des überwiegenden Allgemeininteresses ist auf den Zweck der Datenerhebung und Datenverarbeitung abzustellen.

Nur wenn dieser Zweck hinreichend bestimmt und klar in den Regelungen zur Datenerhebung und Datenverarbeitung gefasst ist, kann eine Verhältnismäßigkeitsprüfung sinnvoll und nachvollziehbar erfolgen und überprüft werden, dass Daten nicht außerhalb des Allgemeininteresses verwendet werden[64]. Das Bundesverfassungsgericht spricht in diesem Zusammenhang vom Gebot der „Normklarheit“, welches sich aus dem allgemeinen Rechtsstaatsgebot herleitet[65].

---

[59] Dreier, in: Dreier, Grundgesetz, Art. 2 Rn. 52; Schmitt-Glaeser, in: Isensee/Kirchhof, Handbuch des Staatsrechts, VI, § 129 Rn. 43.
[60] BVerfGE 65, 1 (45 f.), eine solche gesetzliche Grundlage fehlt nach Feststellung des BGH für die verdeckte „Online Durchsuchung“, vgl. BGH, Beschluss vom 31.01.2007, Az.: StB 18/06.
[61] Dammann, in: Simitis, BDSG, § 4 Rn. 9.
[62] Auf legislativer Ebene ist freilich dem Normgeber ein weiterer Gestaltungsspielraum zuzubilligen.
[63] Vgl. Dierks, Schweigepflicht und Datenschutz in Gesundheitswesen und medizinischer Forschung, S. 29 ff.
[64] Vgl. zu dem durch das BVerfG abgeleiteten Erfordernis bereichsspezifischer Regelungen BVerfG, vom 2. März 2006, 2 BvR 2099/04.
[65] Zu den Konsequenzen im Bereich der Telemedizin Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 202 ff.

Im Hinblick auf beide Grundsätze, Verhältnismäßigkeitsgrundsatz wie Gebot der Normklarheit, verlangt die Rechtsprechung des Bundesverfassungsgerichts, dass vorausschauend organisatorische und verfahrensrechtliche Sicherheitsvorkehrungen zu treffen sind[66]. Ziel dieser Vorkehrungen im Vorfeld ist die Schaffung von Transparenz, deren Verwirklichung auch das Gebot der Normklarheit bezweckt. Die Anforderungen variieren in der Qualität und Intensität und sind abhängig davon, ob eine Datenerhebung in anonymisierter Form oder in individualisierter bzw. individualisierbarer Form erfolgt. Lassen die erhobenen Daten keinen Rückschluss auf die Identität der Person zu, sind sie also anonym, dann reichen Zwecke die allgemein der Erfüllung öffentlicher Aufgaben dienen können, soweit Vorkehrungen getroffen sind, die Missbrauchsmöglichkeiten verhindern[67]. Werden individualisierte oder individualisierbare Daten erhoben und verwendet, sind strengere Anforderungen zu stellen. Hier sind Datenerhebung und Datenverarbeitung nur im Rahmen einer klar beschriebenen Einzelaufgabe möglich. Unzulässig sind Datensammlungen, die ein Persönlichkeitsprofil zeichnen können[68]. Werden beispielsweise zwangsweise DNA-Proben zur Ermittlung eines Täters durchgeführt, so dürfen neben der Übereinstimmung der verglichenen DNA- Muster weitergehende Informationen, die in der DNA- Sequenz enthalten sind, beispielsweise über Erbkrankheiten, nicht gesammelt werden[69].

Zur Umsetzung der strengen Zweckbindung und unter dem Aspekt der Verhältnismäßigkeit ist zu beachten, dass auch innerhalb von Organisationseinheiten der Zugang zu personenbezogenen Daten, die für bestimmte Einzelaufgaben verarbeitet werden, nur den mit diesen Aufgaben betrauten Personen ermöglicht werden darf. Dies ist von vornherein festzulegen und erfordert organisatorisch eine Trennung der Aufgabenbereiche. Hier gilt das so genannte „Gebot informationeller Gewaltenteilung“[70]. Hinzu treten verfahrensrechtliche Anforderungen wie beispielsweise Löschungs- und Akteneinsichtsrechte. Insbesondere das Gebot informationeller Gewaltenteilung birgt allerdings Probleme. In Konsequenz dieses Gebotes ist ein Datenzugang zwischen unterschiedlichen Aufgabenträgern und auch zwischen Organisationseinheiten einer Behörde zu verhindern, so dass jedes Amt

[66] Di Fabio, in: Maunz/Dürig, Grundgesetz, Art. 2 Rn. 185.
[67] Di Fabio, in: Maunz/Dürig, Grundgesetz, Art. 2 Rn. 177 und 185.
[68] Di Fabio, in: Maunz/Dürig, Grundgesetz, Art. 2 Rn. 184.
[69] BVerfG, NJW 2001, S. 879 (880).
[70] Vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 1 Rn. 22; Rasmussen, NZS 1998, S. 67.

innerhalb einer einheitlichen Behörde eine geschlossene, räumlich getrennte Datenverarbeitung haben muss[71].

Dies kann angesichts technischer Entwicklungen und der Forderung, die Verwaltung zu modernen Dienstleistungsanbietern umzubauen, als anpassungsbedürftig kritisiert werden, zumal die Bedrohung personenbezogener Daten im Privatbereich durch die Entwicklungen im Internet mittlerweile als ähnlich groß wie im staatlichen Bereich angesehen werden kann. Das Augenmerk ist auf eine angemessene Reaktion auf neue Gefährdungslagen zu richten. Sollen neue IT-Techniken auch auf hoheitlicher Seite bei der Aufgabenerfüllung nutzbar gemacht werden, ist an eine Konvergenz staatlichen und privaten Datenschutzes zu denken, da die Gefährdungslagen kaum noch in den Kategorien Staat- Privatbereich fassbar sind[72]. Zu fragen ist, ob durch technische Möglichkeiten eine Aufrechterhaltung oder gar Verbesserung des Schutzniveaus auch in präventiver Hinsicht erreichbar ist. Die Ausdehnung des Bundesdatenschutzgesetzes auf Private weist in diese Richtung. Dieser Aspekt ist bei der Auslegung von Rechtsnormen des öffentlichen Rechts, die dem Schutz oder der Ausgestaltung des Rechts auf informationelle Selbstbestimmung dienen und damit den Umgang mit personenbezogenen Daten betreffen, zu berücksichtigen.

Die dargestellten Anforderungen für Einschränkungen des Rechts auf informationelle Selbstbestimmung zugunsten öffentlicher Zwecke gelten im Verhältnis Staat- Bürger. Hier zeigt sich die klassische Funktion der Grundrechte als Abwehrrechte gegen den Staat. Daneben ist in Rechtsprechung und Wissenschaft aber allgemein anerkannt, dass Grundrechte auch im Privatrecht wirken[73]. Dies wird ganz überwiegend davon abgeleitet, dass Grundrechte eine objektive Wertentscheidung für das gesamte Recht beinhalten[74].

Gleichzeitig wird diese gestaltende und ordnende Wirkung der Grundrechte begrenzt. Diese Begrenzung folgt der zutreffenden Erkenntnis, dass eine Ausgestaltung und Konkretisierung des Rechts nicht durch Grundrechte erfolgen kann, son-

---

[71] Vgl. Bergmann/Möhrle/Herb, BDSG, § 3 Rn. 161.
[72] Di Fabio, in: Maunz/Dürig, Grundgesetz, Art. 2 Rn. 190.
[73] Jarass/Pieroth, Grundgesetz, Vorb. vor Art. 1 Rn. 58; Dreier, Grundgesetz, Vorb. vor Art. 1 Rn. 57 ff.
[74] BVerfGE 73, 261 (269); Stern, Staatsrecht, III/1, S. 1572.

dern grundsätzlich dem einfachen Gesetz vorbehalten sein muss[75]. Grundrechte sind für solch eine Aufgabe zu allgemein gehalten, im Übrigen auch nicht konzipiert. Andererseits ist den inhaltlichen Zielsetzungen der Grundrechte, insbesondere der Freiheitssicherung, mit Hinblick auf ihre Bedeutung und prominente Stellung in der Rechtsordnung bestmöglich Geltung zu verschaffen. Daher hat die Rechtsprechung versucht, eine Balance zwischen Grundrechten als Programmsätzen und Privatrechtsgestaltung durch Grundrechte zu finden.

Exemplarisch kann dies an folgender Formel des Bundesverfassungsgerichts dargestellt werden: „Der Richter hat kraft Verfassungsgebots zu prüfen, ob von der Anwendung zivilrechtlicher Vorschriften im Einzelfall Grundrechte berührt werden. Trifft dies zu, dann hat er diese Vorschriften im Lichte der Grundrechte auszulegen und anzuwenden“[76]. Ähnliche Formulierungen finden sich auch in anderen Entscheidungen[77]. In der Rechtswissenschaft aber auch in Teilen der Rechtsprechung ist dies treffend mit dem Begriff „Ausstrahlungswirkung“ zusammengefasst worden[78]. In den plastischen Worten des BVerfG zu dem aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG abgeleiteten allgemeinen Persönlichkeitsrecht entfaltet dieses „als objektive Norm seinen Rechtsgehalt auch im Privatrecht und strahlt in dieser Eigenschaft auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus.“

Verbreitet wird auch von „mittelbarer Drittwirkung“ der Grundrechte gesprochen[79]. Diese Bezeichnung ist indes unglücklich gewählt[80], suggeriert sie doch, dass es eines Vermittlers in der Wirkung bedarf. Zwar ist zuzugeben, dass häufig die Generalklauseln, insbesondere die §§ 242, 138, 133, 157 BGB, als Einfallstor für Grundrechte dienen. Diese gilt es grundrechtskonform auszulegen und anzu-

---

[75] Vgl. die Rechtsprechung zum Nachbarschutz und Bestandschutz im Baurecht, der grundsätzlich nicht mehr unmittelbar auf Art. 14 GG gestützt werden kann, sondern auf einfachgesetzliche Regelungen beschränkt ist, BVerwGE 67, 334 (337); BVerwG DVBl, 1974, S. 777 f; VG Berlin vom 04.06.2003, Az.: 19 A 98.03; Schoch, Nachbarschutz im öffentlichen Baurecht, Jura 2004, 317 ff.; Schmaltz, in: Schrödter, BauGB, § 35 Rn. 115 f.; Söfker, in: Ernst/Zinkahn/Bielenberg, BauGB, § 35 Rn. 184 ff.; Fischer, Juristische Anforderungen an das Bauen und den Brandschutz im Bestand, S. 9.

[76] BVerfGE 84, 192 (194 f.); BVerfG, vom 23.10.2006, Az.: 1 BvR 2027/02, Absatz-Nr. 28-30

[77] BVerfGE 103, 89 (100).

[78] Vgl. speziell zur Ausstrahlungswirkung des Rechts auf informationelle Selbstbestimmung, Maunz/Dürig, Grundgesetz, Art. 2 Rn. 139 f.

[79] Vgl. Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 119 f.

[80] Vgl. auch Badura, in: Merten/Papier, Handbuch der Grundrechte, I, § 20 Rn. 27, der in dem Abstellen auf die Rechtstermini „unmittelbare Drittwirkung“ oder „mittelbare Drittwirkung“ nur vordergründig die Frage der privatrechtsgestaltenden Wirkung von Grundrechten behandelt sieht.

wenden, soweit spezifische verfassungsrechtliche Problemstellungen berührt sind. Allerdings taucht das dahinter stehende Problem der Interpretation und Konkretisierung von Rechtsnormen auch außerhalb von Generalklauseln des Privatrechts auf. Auslegungsbedarf und Spielraum bei der Anwendung finden sich vielfach sowohl auf Tatbestandsseite als auch auf Rechtsfolgenseite von Rechtsnormen des Privatrechts. Generalklauseln, unbestimmte Rechtsbegriffe[81] und Rechtsfolgeermessen lassen sich nicht immer trennscharf unterscheiden[82]. Nur die Weite des Spielraums variiert. Es besteht hinsichtlich der Einwirkungsmöglichkeiten der Grundrechte lediglich ein gradueller Unterschied und kein qualitativer Unterschied, welcher eine grundsätzlich andere Wirkungsart der Grundrechte im öffentlichen Recht gegenüber dem Privatrecht legitimieren könnte.

Die Frage der Wirkungsbegrenzung der Grundrechte im einfachen Recht hindert nicht die Annahme einer direkten Wirkung der Grundrechte im Privatrecht. Dem sachlichen Unterschied zwischen Privatrecht und öffentlichem Recht kann auch bei der Annahme einer direkten Wirkung Rechnung getragen werden. Richtig ist zunächst, dass Unterschiede zwischen Privatrecht und öffentlichem Recht bestehen. Das Privatrecht mit seiner zentralen Kodifikation, dem BGB, geht nach der Konzeption seiner geistigen Väter von einem gleichberechtigten Gegenübertreten von Privatrechtssubjekten aus. Das Recht der Willenserklärung, maßgeblich beeinflusst durch Savigny, gründet auf der Überlegung des freien, eigenverantwortlichen Willensentschlusses[83]. Das Vertragsrecht ist geprägt durch den Begriff der „Privatautonomie“, der auch verfassungsrechtlich durch Art. 2 Abs. 1, 14 Abs. 1 GG garantiert wird. Im BGB fanden sich ursprünglich nur wenige Einschränkungen der Privatautonomie oder Schutzvorschriften für die Vertragsparteien. Innerhalb des BGB waren dies im Wesentlichen die §§ 242, 134 und 138 BGB. Erst im Laufe der Entwicklung fanden vermehrt Schutzvorschriften und Einschränkungen der Privatautonomie Eingang in das Privatrecht. Beispielhaft kann auf die Entwicklung des Verbraucherschutzes aber auch des Anlegerschutzes hingewiesen werden[84]. Dennoch ist das Prinzip der Privatautonomie prägend geblieben.

---

[81] Allgemein zum unbestimmten Rechtsbegriff vgl. aus neuerer Zeit Schoch, Jura 2004, S. 612 ff.
[82] Exemplarisch Maunz, in: Maunz/Dürig, Grundgesetz, Art. 72 Rn. 18.
[83] Vgl. Palandt, BGB, Einf. v. § 116 Rn. 2.
[84] Die Bedeutung des Verbraucherschutzes kann man anhand der so genannten „Heininger“ Entscheidung nachvollziehen vgl. EuGH, NJW 2002, S. 281; zu Verbraucherschutzvorschriften vgl. Palandt, BGB, Einleitung Rn. 10; zum Anlegerschutz vgl. das Prospekthaftungsgesetz und das Verfahren gegen die Telekom, Meldung der Süddeutschen Zeitung vom 23.11.2004 Nr. 264, S. 1, neben der zivilrechtlichen Seite hat das Verfahren auch einen strafrechtlichen Aspekt; zum straf-

Aufgrund dieser Unterschiede zwischen Privatrecht und öffentlichem Recht ist die Wirkung von Grundrechten im Privatrecht zutreffend enger zu begrenzen als die Wirkung im öffentlichen Recht. Wann eine Einwirkung der Grundrechte anzunehmen ist, kann nur im Einzelfall bestimmt werden. Anhaltspunkte können die Intensität des Grundrechtseingriffs, die Bedeutung des Grundrechts, bestehende strukturelle Macht- oder Informationsdefizite beim Betroffenen oder Regelungslücken mit Berührung zum betroffenen Grundrecht sein. Grundrechtlich oder einfachgesetzlich verbürgte Freiheiten funktionieren nur, wenn die Freiheiten einzelner Handlungssubjekte in bestimmten Situationen beschränkt werden, um die Freiheit im Gemeinwesen zu sichern. Leitend muss die Überlegung sein, ob eine Einwirkung auf das Privatrecht wegen fehlender oder ungenügender Regelungen des Privatrechts unerlässlich ist. Ist dies der Fall, gestalten Grundrechte das Privatrecht.

Dass zunächst ein Gericht angerufen werden muss, welches die Grundrechtsverletzung prüft, kann als eine Frage der gerichtlichen Rechtsfindung und Rechtsdurchsetzung verstanden werden und hindert nicht die dogmatische Auffassung einer direkten Wirkung der Grundrechte auch im Privatrecht. Denn es wäre, auch hinsichtlich der Funktion der Judikativen im System der Gewaltenteilung, schlecht nachvollziehbar, dass ein Privater solange nicht durch die Grundrechte verpflichtet ist, bis der Richter dies ausspricht. Unabhängig von der dogmatischen Ableitung der Grundrechtswirkung im Privatrecht bleibt die sachliche Frage zu entscheiden, ob eine Wirkung der Grundrechte im Privatrecht eintritt.

Für den Bereich der medizinischen Daten hat die Rechtsprechung eine Auswirkung des aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleiteten Rechts auf informationelle Selbstbestimmung auf die Privatrechtsbeziehung zweier Ärzte anlässlich einer Praxisübergabe angenommen[85]. In der neueren Diskussion stehen Gefahren im Zusammenhang mit der Möglichkeit einer Genomanalyse. Hier ist an nachteilige Konsequenzen für den Einzelnen bei unberechtigter Kenntniserlangung solcher für den Einzelnen höchst bedeutsamer und oft das Schicksal bestimmender Daten zu denken. Gleichzeitig besteht die Gefahr, dass eine Verpflichtung zur Erstellung von Genomanalysen gefordert wird. Diese Versuchung

---

rechtlichen Anlegerschutz nach § 400 Abs. 1 AktG im Urteil des LG München vom 08.04.2004 vgl. Kiethe, NStZ 2004, S. 73.

[85] BGHZ 116, 268 (273).

stellt sich insbesondere in der Krankenversicherungswirtschaft[86]. Hier sind private Abreden in Allgemeinen Versicherungsbedingungen, sofern gesetzliche Regelungen in Umsetzung staatlicher Schutzpflichten fehlen, unmittelbar am Recht auf informationelle Selbstbestimmung in seiner negativen Ausprägung als Recht auf Nichtwissen zu messen[87].

3. Einfachgesetzliche Regelungen

Neben der grundrechtlichen Verwirklichung des Schutzes persönlicher Daten, hat der Gesetzgeber einfachgesetzliche Regelungen zum Schutz personenbezogener Daten erlassen[88]. Sie dienen in diesem Bereich der Freiheitssicherung des Einzelnen vor dem Hintergrund des verfassungsrechtlichen Auftrags des Freiheitsschutzes im Gemeinwesen. Zu beachten sind neben nationalen Rechtsnormen auch europarechtliche Regelungen.

Allgemeine Regelungen zur Wahrung des Datengeheimnisses mit Bedeutung für den Umgang mit medizinischen Daten enthalten das Bundesdatenschutzgesetz, sowie die Datenschutzgesetze der Länder. Im Bereich des Gesundheitswesens bestehen sektorspezifische Regelungen in den Krankenhausgesetzen der Länder mit entsprechenden Verordnungen oder in weiteren speziellen Regelungen zum Gesundheitsdatenschutz, beispielsweise in dem Gesundheitsdatenschutzgesetz in Nordrhein-Westfalen. Im kirchlichen Bereich existiert ein eigenständiger Datenschutz. Zu nennen sind insbesondere das Kirchengesetz über den Datenschutz in der Evangelischen Kirche Deutschlands, DSG-EKD, für die Katholische Kirche die Anordnung über den kirchlichen Datenschutz, KDO mit entsprechender Durchführungsverordnung, KDO-DVO. Im Bereich des Arbeitnehmerdatenschutzes finden sich Regelungen im Betriebsverfassungsgesetz, BetrVG, sowie in den Personalvertretungsgesetzen. Auf europarechtlicher Ebene sind die allgemeine EG-Datenschutzrichtlinie vom 24.10.1995, Richtlinie 95/46/EG und die Datenschutzrichtlinie für elektronische Kommunikation, Richtlinie 2002/58/EG v. 12.07.2002 von Bedeutung. Die allgemeine EG-Datenschutzrichtlinie enthält nä-

[86] Zu der Absicht eines gesetzlichen Verbotes, das den freiwilligen Selbstverzicht der Versicherungswirtschaft ablösen soll vgl. die Meldung in der Süddeutschen Zeitung vom 19. November 2004, Nr. 269, S. 20.
[87] Di Fabio, in: Maunz/Dürig, Grundgesetz, Art. 2 Rn. 192.
[88] Vgl. zum Überblick die Gesetzesnachweise bei Schaffland/Wildfang, BDSG.

here Anforderungen zum Umgang mit medizinischen Daten. Eine Umsetzung erfolgte durch die Reform des BDSG im Jahr 2001. Dem Schutz des Kommunikationsgeheimnisses, (Post- und Fernmeldegeheimnis) dienen Art. 10 GG, § 206 StGB sowie einfachgesetzliche bereichsspezifische Regelungen zur Umsetzung von Art. 10 GG.

Das Privatgeheimnis wird im Gesundheitsbereich strafrechtlich durch § 203 StGB, berufsrechtlich durch die Musterberufsordnung der Ärzte sowie durch die Berufsordnungen der jeweiligen Landesärztekammern geschützt. Erreicht wird der strafrechtliche Schutz durch das Statuieren von Schweigepflichten. Um Umgehungen zu verhindern wird die Schweigepflicht durch Schweigerechte- bzw. Aussageverweigerungsrechte im Prozess, §§ 53, 53a StPO, und Beschlagnahmeverbote, § 97 StPO, gesichert. Dem Schutz des Sozialgeheimnisses dienen vor allem Regelungen aus dem Sozialgesetzbuch, hier insbesondere Vorschriften aus dem ersten und zehnten Buch. Schließlich finden sich verstreut im Bundes-, Landes- und Europarecht sowie in internationalen Vereinbarungen weitere Vorschriften, die das Recht auf informationelle Selbstbestimmung näher konkretisieren[89].

II. Der Informationsfluss zum Outsourcer

Bevor ein Outsourcing medizinischer Daten erfolgen kann, müssen die Daten zum Outsourcer gelangen. Vor der Betrachtung des Outsourcings medizinischer Daten sind daher die rechtlichen Grundlagen des Informationsflusses zum Outsourcer kurz darzustellen. Die Daten müssen vor einem Einschalten Dritter zunächst zum Outsourcer gelangen. Dies betrifft Fragen der Erhebung und Übermittlung von medizinischen Daten. Sofern solche Daten einen Personenbezug aufweisen ist vor dem Hintergrund des Rechts auf informationelle Selbstbestimmung eine hinreichende gesetzliche Grundlage erforderlich.

Im Bereich der Gesetzlichen Krankenversicherung regelt das SGB V den Zugang zu Leistungen der Krankenversicherung. Gemäß § 15 SGB V erhält der Versi-

[89] Vgl. die Zusammenstellung datenschutzrelevanter Regelungen bei Geis/Helfrich, Datenschutzrecht; Eingehend zu den Rechtsgrundlagen des Datenschutzes im medizinischen Bereich Mand, MedR 2003, S. 393 und Schirmer, in: Roßnagel, Handbuch des Datenschutzrechts, S. 1362 ff.; vgl. auch die Nachweise bei Hanika, MedR 2004, S. 149 ff.

cherte als Nachweis der Berechtigung zur Inanspruchnahme von Leistungen eine Krankenversicherungskarte. Diese enthält die in § 291 SGB V genannten Daten, die sowohl der Krankenkasse als auch dem behandelnden Arzt bzw. dem Krankenhaus zugänglich werden. Die Versicherungskarte stellt die „Eintrittskarte" in das System der Gesetzlichen Krankenversicherung dar. Neben diesen Daten dürfen die Krankenkassen nach Maßgabe von § 284 SGB V Daten erheben. In § 285 SGB V ist die Datenerhebung durch die Kassenärztlichen Vereinigungen geregelt.

Eine weitergehende Datenerhebung kann im Zuge der Behandlung des Patienten erfolgen. Der Arzt ist verpflichtet im Rahmen des Behandlungsvertrages eine umfassende Dokumentation der behandlungsrelevanten Daten zu führen. Diese Dokumentationspflicht, der auf Patientenseite ein privatrechtlicher Anspruch auf umfassende Dokumentation gegenübersteht, ist nach h.M. eine Nebenpflicht des Behandlungsvertrages und Ausfluss des Rechts auf informationelle Selbstbestimmung[90]. Einfachgesetzliche Regelungen, welche eine Dokumentationspflicht statuieren, finden sich in der Musterberufsordnung für Ärzte und den entsprechenden Berufsordnungen der Landesärztekammern[91]. Entsprechend der Dokumentationspflicht besteht aus dem Behandlungsvertrag in Verbindung mit anderen Rechtsnormen die Möglichkeit, medizinische Daten zu erheben und zu speichern[92].

Für die anschließende Übermittlung personenbezogener medizinischer Daten innerhalb anderer Leistungserbringer oder Leistungsträger im System der gesetzlichen Krankenversicherung finden sich zahlreiche Rechtsgrundlagen[93]. Von zentraler Bedeutung sind die Regelungen in § 67 SGB X i.V.m. §§ 294- 303 SGB V. Daneben bestehen für Übermittlungen an Einrichtungen außerhalb des Systems der gesetzlichen Krankenversicherung besondere Regelungen in den §§ 67 ff. SGB X sowie gesetzliche Anzeige- und Mitteilungspflichten[94].

---

[90] Zur Dokumentationspflicht BGH NJW 1989, S. 764; Schirmer, in: Roßnagel, Handbuch des Datenschutzrechts, S. 1367.

[91] Zum allgemeinen Anspruch des Patienten auf Akteneinsicht vgl. Maunz/Dürig, Grundgesetz, Art. 2 Rn. 139; Bake, Datenschutz und Datensicherheit, S. 23, 67 f.

[92] Vgl. die Übersicht bei Bake, Datenschutz und Datensicherheit, S. 28.

[93] Vgl. Bake, Datenschutz und Datensicherheit, S. 41 ff.; von zentraler Bedeutung sind die §§ 284 – 301 SGB V.

[94] Beispielsweise in den Meldegesetzen der Länder, im Infektionsschutzgesetz, im Personenstandsgesetz; § 11 Abs. 4 Bestattungsgesetz, § 138 StGB; vgl. auch von Lewinski, MedR 2004, S. 96 ff.

Im Bereich der Privaten Krankenversicherung ist für die Erhebung medizinischer, personenbezogener Daten der Versicherungsvertrag mit den Allgemeinen Versicherungsbedingungen i.V.m. dem Versicherungsvertragsgesetz maßgeblich, soweit es um die Erhebung durch private Krankenversicherungsunternehmen geht. Der Behandlungsvertrag ist die Grundlage, soweit es um die Erhebung durch Ärzte oder Krankenhäuser geht.

III. Rechtsgrundlagen für das Outsourcing

Sind personenbezogene, medizinische Daten einer Einrichtung zugeflossen, stellt sich die Frage, ob für das Outsourcing der vorhandenen medizinischen Daten eine ausdrückliche gesetzliche Regelung besteht, die für Outsourcingzwecke auch eine Weitergabe medizinischer Daten an private Dritte ermöglicht.

Eine bundeseinheitliche Regelung für den Bankenbereich ist mit § 25a KWG geschaffen worden[95]. Eine vergleichbare bundeseinheitliche Regelung des Outsourcings medizinischer Daten fehlt im Bereich des Gesundheits- und Sozialwesens. Auch auf landesrechtlicher Ebene existieren keine spezifischen Outsourcingregelungen für das Gesundheitswesen[96]. Innerhalb unterschiedlicher Regelungsgebiete finden sich aber sowohl im Bundesrecht als auch im Landesrecht verstreut Vorschriften, die in Ausgestaltung des Rechts auf informationelle Selbstbestimmung als Rechtsgrundlage für das Outsourcing von medizinischen Daten herangezogen werden können.

So ermöglichen die Landesdatenschutzgesetze, das Bundesdatenschutzgesetz und § 80 SGB X über das Institut der Auftragsdatenverwaltung die Möglichkeit, unter bestimmten Voraussetzungen personenbezogene Daten im Auftrag durch andere private Stellen zu erheben, verarbeiten oder zu nutzen[97]. Im Bundesdatenschutzgesetz sieht § 28 BDSG die Möglichkeit der Übermittlung von personenbezogenen Daten an Dritte unter engen Voraussetzungen vor. Entsprechende Regelungen

[95] Dazu ausführlich aus strafrechtlicher Sicht Otto, wistra 1999, S. 205; vgl. auch Eul, in: Roßnagel, Handbuch des Datenschutzrechts, S. 1090; Hoeren, DuD 2002, S. 736; Steding/Mayer, BB 2001, S. 1693.
[96] Vgl. Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 191 ff.
[97] Vgl. § 11 BDSG, durch den das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten im Auftrag geregelt ist; ähnliche Regelungen finden sich in den Landesdatenschutzgesetzen, z.B. Art. 6 BayDSG.

finden sich auch in den allgemeinen oder sektorspezifischen Datenschutzgesetzen der Länder. Im Strafrecht kann in § 203 Abs. 2 S. 1 Nr. 2 StGB die Grundlage gesehen werden, Daten durch Dritte verarbeiten zu lassen.

Im Übrigen kann das Outsourcing medizinischer Daten aufgrund vertraglicher Regelung erfolgen. Der Vertragsfreiheit sind vor dem Hintergrund des Rechts auf informationelle Selbstbestimmung Grenzen gesetzt[98]. Zu beachten sind zwingende gesetzliche Vorgaben. Regelungen des Datenschutzes, die teilweise als mögliche Grundlage zum Outsourcing herangezogen werden, wirken zugleich durch ihre Anforderungen an den Datenschutz begrenzend. Daneben sind weitere Regelungen als Anforderungen für den elektronischen Datenverkehr mittelbar auch für das Outsourcing von medizinischen Daten relevant[99]. Weitergehende Anforderungen stellen die oben erwähnten Regelungen zum Schutz besonderer Geheimnisse, insbesondere der strafrechtliche Schutz der Privatgeheimnisse in § 203 StGB.

IV. Beteiligte

Eine Entscheidung für das Outsourcing medizinischer Daten kommt für verschiedene Einrichtungen in Betracht. Zu denken ist dabei gleichermaßen an Leistungsträger wie Leistungserbringer im System der Gesetzlichen Krankenversicherung und der Privaten Krankenversicherung. Der Outsourcinggeber kann dabei sowohl in der Rechtsform des Privatrechts als auch in einer öffentlich-rechtlichen Rechtsform organisiert sein. Als Rechtsträger kommen weiterhin natürliche und juristische Personen in Betracht. Allein diese Einordnung des Outsourcinggebers kann Bedeutung für die rechtliche Beurteilung eines Outsourcingprojekts haben. Neben dem Outsourcinggeber ist der Outsourcingnehmer an dem Outsourcingvorhaben beteiligt. Dieser kann zwar auch öffentlich-rechtlich organisiert sein, ist aber in der Regel ein privates IT-Dienstleistungsunternehmen.

Die rechtlichen Beziehungen zwischen den Beteiligten im Bereich des Outsourcings medizinischer Daten sind regelmäßig durch einen privatrechtlichen Vertrag geregelt. Das Institut der Beleihung ist zwar bei öffentlich-rechtlichen Outsourcinggebern denkbar, spielt aber im Bereich des Outsourcings von Datenverarbeitung und Datenverwaltung kaum eine Rolle. Sofern personenbezogene Daten

[98] Vgl. insbesondere §§ 134, 138, 242 BGB.
[99] Beispielhaft zu nennen sind das Signaturgesetz und die Signaturverordnung.

durch das Outsourcing betroffen sind, ist die Person als Betroffener mittelbar Beteiligter.

In der folgenden Darstellung beschränkt sich die Untersuchung auf Ärzte und Krankenversicherungen als potentielle Outsourcinggeber sowie auf private externe IT- Dienstleistungserbringer als Outsourcingnehmer bei Inanspruchnahme personeller Dienstleistungen durch den Outsourcer.

C. Outsourcing und Privatgeheimnisschutz nach § 203 StGB

Für die strafrechtliche Beurteilung des Outsourcings medizinischer Daten ist unabhängig von der Rechtsform der Beteiligten von zentralem Interesse, ob das Vorhaben mit der Regelung zum Schutz von Privatgeheimnissen nach § 203 StGB kollidiert. In § 203 StGB wird für einen bestimmten Personenkreis das unbefugte Offenbaren von fremden Geheimnissen unter Strafe gestellt. Seiner Systematik nach erfasst der erste Absatz des § 203 StGB Angehörige bestimmter Berufsgruppen oder privater Einrichtungen, während § 203 Abs. 2 StGB an Amtsträger oder ihnen ähnliche, dem öffentlichen Bereich zugeordnete Personen anknüpft. In § 203 Abs. 3 StGB werden bestimmte Personen den Schweigepflichtigen nach § 203 Abs. 1 StGB gleichgestellt.

I. Outsourcing ohne Zustimmung des Betroffenen

Eine Strafbarkeit würde im Ergebnis entfallen, wenn eine wirksame Zustimmung seitens eines Zustimmungsberechtigten vorläge. Das Problem einer solchen auf den ersten Blick einfachen Lösung liegt darin, dass die Zustimmung jederzeit widerruflich ist. Eine vertragliche Ausgestaltung als unwiderrufliche Zustimmung dürfte vor dem Hintergrund des grundrechtlich geschützten Rechts auf informationelle Selbstbestimmung nach § 138 BGB sittenwidrig und damit nichtig sein. Weiterhin wird es, jedenfalls wenn eine Vielzahl von Personen durch das Outsourcing betroffen ist, wahrscheinlich sein, dass nicht jede Person ihre Zustim-

mung erteilen wird[100]. Es bestehen also erhebliche Unwägbarkeiten, so dass das Interesse eines potentiellen Outsourcinggebers dahin gehen wird, dass sein Outsourcingvorhaben auch ohne eine Zustimmung möglich wird, ohne dass nachteilige rechtliche, vorliegend strafrechtliche, Konsequenzen drohen. Nur wenn dies nicht möglich sein sollte, wird der Outsourcinggeber eine Zustimmungseinholung in die Überlegungen miteinbeziehen. Im Folgenden werden zunächst die Outsourcingmöglichkeiten ohne Zustimmung untersucht.

II. Rechtsgut und Deliktsart

Die Bedeutung der Strafdrohung in § 203 StGB erklärt sich aus dem Bedürfnis nach dem Schutz von Daten, die dem persönlichen Lebensbereich zuzuordnen sind. In Vertrauensbeziehungen des Einzelnen zu anderen privaten Personen in bestimmten Funktionen, aber auch in der Beziehung des Einzelnen gegenüber dem Staat, hat der Gesetzgeber einen strafrechtlichen Schutz als ultima ratio neben dem zivilrechtlichen Selbstschutz für erforderlich gehalten. Dabei ist für den Zugang zum Verständnis des Normzwecks des § 203 StGB die Bestimmung des geschützten Rechtsgutes sowie der Deliktsart erforderlich. Die Frage nach dem Rechtsgut ist umstritten[101]. Mit unterschiedlichen Nuancen bewegen sich die Ansichten zwischen dem Verständnis des Rechtsgutes als Kollektivrechtsgut oder Individualrechtsgut, wobei verschiedene vermittelnde Positionen vertreten werden[102].

Ein Ansatz will primär Allgemeininteressen durch § 203 StGB geschützt wissen[103]. Dabei wird das Rechtsgut kollektiv definiert als allgemeines Vertrauen in die Verschwiegenheit Angehöriger bestimmter Berufe bzw. der Träger bestimmter Funktionen. Für die Orientierung an Berufsbildern spricht die große gesellschaftliche Bedeutung, die traditionell manchen Berufen wie insbesondere dem Beruf des Arztes oder des Rechtsanwaltes zukommt. Solche Berufsbilder blicken auf eine lange Historie, in der stets hohe Anforderungen an die Integrität der Be-

[100] Dazu das Beispiel „deCode“ bei Schulz, DuD 2001, S. 13 mit Fußnote 13; für das Kreditwesen Hoeren, DuD 2002, S. 737: „außerhalb jeder Praktikabilität“.
[101] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 14 ff.; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 2 ff.
[102] Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 2, 3 ff.
[103] Lenckner, in: Schönke/Schröder, StGB, § 3 Rn. 3; Würthwein, Innerorganisatorische Schweigepflicht, S. 20 ff.

rufsausübenden gestellt worden sind, zurück. Dementsprechend statuierten berufsständische Normen schon früh besondere Schweigepflichten. Auch enthielten frühere Strafvorschriften dem Gesetzeswortlaut nach Formulierungen, die auf das anvertraute Geheimnis abstellten[104]. Schließlich kann auch in der heutigen Fassung des § 203 StGB eine Orientierung an Berufsbildern in § 203 Abs. 1 StGB erkannt werden. Die Beschränkung auf bestimmte Berufe sei der sozialen Funktion dieser Berufe geschuldet[105].

Die Ansicht, dass durch § 203 StGB nur oder primär Allgemeininteressen geschützt werden, überzeugt nicht. Der Wortlaut der Vorschrift weist nicht auf ein vorrangig kollektives Rechtsgutverständnis hin. So spricht das Gesetz bei dem Geheimniserlangen davon, dass ein fremdes Geheimnis dem Geheimnisträger „anvertraut oder sonst bekannt geworden ist". Danach ist es nicht maßgeblich, ob das Geheimnis planmäßig innerhalb einer Vertrauensbeziehung erfahren wird oder zufällig zu dem Geheimnisträger gelangt. In beiden Fällen erachtet das Gesetz das fremde Geheimnis für gleich schützenswert. Dies legt es nahe, dass das Gesetz das Geheimnis um des Individuums willen schützt, also der Individualrechtsschutz im Vordergrund steht.

Gegen einen Schutz von Allgemeininteressen spricht auch, dass die in § 203 Abs. 1 StGB aufgeführten Berufe eine inhomogene Gruppe[106] darstellen und zudem auch Angehörige privater Unternehmen aus der Versicherungswirtschaft aufgenommen worden sind, die sich kaum einer einheitlichen Berufsgruppe zuordnen lassen und nichts mit den freien Berufen gemein haben. Andererseits sind Heilberufe, die zur Führung der Berufsbezeichnung einer staatlich geregelten Ausbildung nicht bedürfen, wie beispielsweise der Heilpraktiker, nicht in § 203 Abs. 1 StGB aufgeführt, obwohl in der Sache Geheimnisse gleicher Qualität betroffen sein können. Dass manche Berufe nicht aufgenommen worden sind, spricht aber nicht, wie teilweise vertreten wird[107], gegen den Individualrechtsschutz. Die Beurteilung, wem gegenüber persönliche schutzwürdige Geheimnisse als ultima ratio eines strafrechtlichen Schutzes bedürfen, obliegt zutreffend dem Gesetzgeber[108].

---

[104] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 14.
[105] So insbesondere Schlund, JR 1977, S. 265 ff.
[106] Rechtspolitisch umstritten ist insbesondere § 203 Abs. 1 Nr. 5 StGB; zur Kritik an der Aufnahme von Tierärzten vgl. Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 7.
[107] Vgl. Würthwein, Innerorganisatorische Schweigepflicht, S. 21.
[108] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 14, 16.

Dabei hat er einen weiten gesetzgeberischen Ermessensspielraum, in welchen Bereichen auch unter Berücksichtigung gesellschaftlicher Veränderungen nur ein strafrechtlicher Schutz ausreichend ist. Ausgangspunkt gesetzgeberischer Beurteilung ist dabei der persönliche Bereich des Einzelnen, dessen Integrität zu achten ist.

Dieser Blickwinkel ist auch im Hinblick auf den grundrechtlichen Schutz des persönlichen Bereichs durch das allgemeine Persönlichkeitsrecht nach Art.1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG, aus dem sich das Recht auf informationelle Selbstbestimmung ableitet, angezeigt. Grundkonsens ist, dass der persönliche Bereich zu schützen ist. Der persönliche Bereich ist keine feststehende, statische Größe, sondern kann erst in der Interaktion des Einzelnen mit gesellschaftlichen und staatlichen Institutionen bestimmt werden. Ein Individuum ohne Interaktion mit der Umgebung ist nicht denkbar. Der Einzelne ist, wenn der persönliche Bereich betroffen ist, bei dieser Interaktion sowohl Subjekt als auch Objekt. Subjekt ist er in dem Sinne, dass er entscheiden kann, den persönlichen Bereich offen zu legen und über Teile des persönlichen Bereichs zu disponieren. Objekt ist er in dem Sinne, dass auf den persönlichen Bereich des Einzelnen durch Dritte zugegriffen wird, ohne dass eine tatsächliche oder rechtliche Dispositionsbefugnis besteht. Die Objektivität schränkt die Subjektivität der Interaktion ein. Insofern besteht zwischen beiden Polen ein Spannungsverhältnis, dessen sachgerechte Auflösung bei gesetzliche Regelungen, auch strafrechtlichen, beachtet werden muss.

Das grundrechtlich abgeleitete Recht auf informationelle Selbstbestimmung muss dabei aber nicht zwingend identisch mit dem strafrechtlich geschützten Rechtsgut des § 203 StGB sein. Denn es obliegt primär dem Strafrechtsgesetzgeber unter Ausfüllung seines Gestaltungsspielraums durch einfaches Gesetz festzulegen, in welchen Interaktionsbereichen die Subjektivität den Schutz des Strafrechts bedarf und in welchen nicht. Die Anknüpfung an bestimmte Berufe ist zutreffend als einfach-gesetzgeberische Wertung und Erkenntnis des Gesetzgebers zu erklären und zu respektieren[109]. Sie taugt nicht als Argument gegen den Schutz von Individualinteressen. Allenfalls wird dadurch die Frage aufgeworfen, ob neben den Individualinteressen auch Allgemeininteressen geschützt werden. Weiterhin kann auch die Regelung des § 203 Abs. 2 Satz 2 StGB für die Annahme eines Individu-

[109] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 14.

alrechtsschutzes angeführt werden. Dort werden den Geheimnissen „Einzelangaben über persönliche oder sachliche Verhältnisse“ gleichgestellt. Schließlich legt auch die systematische Stellung des § 203 StGB im 29. Abschnitt nahe, dass der Individualrechtsschutz maßgeblich ist.

Mit dem Ergebnis, dass § 203 Abs. 1 StGB jedenfalls Individualinteressen schützt, verbleibt die Frage, ob § 203 Abs. 1 StGB allein Individualinteressen schützt[110]. Durch die Beschränkung des Schutzbereichs in § 203 Abs. 1 StGB hat der Gesetzgeber den Individualrechtsschutz auf bestimmte Berufe und Institutionen eingeengt, die in erheblicher Weise von Vertrauen abhängen. Es geht dabei aber nicht nur um individuelles Vertrauen, das allein den gesellschaftlichen Bereich betrifft, sondern um ein qualifiziertes, ein institutionelles Vertrauen. Im gesellschaftlichen Bereich ist es zumutbar, den Einzelnen darauf zu verweisen, sich selbst zu schützen. Dies ist aber dann nicht mehr der Fall, wenn nach den gesellschaftlichen Verhältnissen das Vertrauen an notwendige und aus dem gesellschaftlichen Bereich herausgehobene Einrichtungen gekoppelt ist und unumgänglich abverlangt wird, sofern eine Interaktion mit den Einrichtungen stattfinden soll. Insofern lässt sich kaum bezweifeln, dass der Gesetzgeber auch die Funktion und soziale Bedeutung der aufgezählten Einrichtungen bei der Schaffung des § 203 StGB berücksichtigt wissen wollte. Dafür spricht auch, dass die Zugehörigkeit zum Kreis der Schweigepflichtigen nicht nur als Last, sondern auch als Auszeichnung angesehen wird und damit auch Vorteile gegenüber nicht Schweigepflichtigen bestehen. Als Korrelat zu dieser Auszeichnung, vergleichbar einem personalen Gütesiegel, ist dem Privatgeheimnisschutz nach § 203 StGB ein personaler Charakter beizumessen. Überzeugend ist daher die Annahme, dass der Individualrechtsschutz an der Bedeutung und Funktion bestimmter Einrichtungen ausgerichtet werden sollte und durch den Schutz von Allgemeininteressen ergänzt wird[111].

[110] Für einen alleinigen Schutz von Individualinteressen insbesondere Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 14 und Köpke, Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für Private Krankenversicherer, S. 23.

[111] Ähnlich Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 5, der aber von einer Fusion von Elementen des Individualrechtsschutzes und des Gemeinschaftsschutzes spricht; auch bei § 206 StGB, der ebenfalls im fünfzehnten Abschnitt des StGB steht, werden öffentliche Interessen geschützt, vgl. Tröndle/Fischer, StGB, § 206 Rn. 1.

Nur eine solche Einschätzung wird der Wechselwirkung bestimmter Einrichtungen mit dem persönlichen Bereich des Einzelnen gerecht. Der Einzelne muss Informationen aus dem persönlichen Bereich der aufgesuchten Einrichtung anvertrauen, wenn er in Beziehung zur Einrichtung treten will. Die Auslieferung solcher persönlicher Informationen ist für den Einzelnen mit dem Risiko behaftet, dass Informationen, die nicht für Dritte bestimmt sind, nach außen dringen. Dies kann zu erheblichen faktischen Nachteilen für den Einzelnen in der Gesellschaft führen. Gleichzeitig kann aber ein Anvertrauen solcher persönlicher Informationen zur Aufgabenerfüllung erforderlich sein. Das Vertrauensverhältnis ist dabei Grundlage wechselseitiger Einflüsse zwischen dem Einzelnen und der Einrichtung. Um diese Einflussmöglichkeit zu beschränken und gleichzeitig zu sichern, bedarf es auch eines Schutzes von Allgemeininteressen. Daher ist es vorzugswürdig, den Schutz von Gemeinschaftsinteressen als nachrangig neben dem Schutz von Individualinteressen anzusehen[112].

Dem Ergebnis zur Frage des Rechtsguts entspricht es, § 203 StGB nicht als abstraktes Gefährdungsdelikt zu begreifen. In der Literatur vertritt allerdings u.a. Rogall die Auffassung, dass § 203 StGB ein abstrakt-konkretes bzw. ein potentielles Gefährdungsdelikt ist. Dies wird daraus gefolgert, dass nicht jede Geheimnisverletzung zu einer Beeinträchtigung von Privatheit führt.

Diese Argumentation überzeugt nicht. Die Einordnung als abstraktes Gefährdungsdelikt wäre nur dann plausibel, wenn man bei § 203 StGB den Schutz von Allgemeininteressen als geschütztes Rechtsgut betrachten würde. Denn wenn beispielsweise eine funktionierende Gesundheitsfürsorge vorwiegend oder allein als geschützt betrachtet wird, dann kann man auch annehmen, dass schon gefährliche Verhaltensweisen der Berufsausübenden unabhängig vom Willen des Geheimnisträgers eine Rechtsgutbeeinträchtigung bedeuten. Gerade dies ist aber nach der hier vertretenen Auffassung nicht der Fall. Auch Rogall bezeichnet Individualinteressen als von § 203 StGB geschütztes Rechtsgut. Natürlich muss nicht jede Geheimnisverletzung zu einer Beeinträchtigung des Rechtsgutes führen. Dies ist dadurch zu erklären, dass dann keine Geheimnisse vorliegen, die verletzt oder gefährdet werden könnten. Der Tatbestand des § 203 StGB beschreibt nicht eine

[112] In diesem Sinne auch Deutsch/Spickhoff, Medizinrecht Rn. 475; so auch Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 496; von einem mittelbaren Schutz öffentlicher Interessen sprechen Arzt/Weber, Strafrecht BT, S. 204.

Verhaltensweise, die nach Auffassung des Gesetzgebers generell die Gefahr einer Rechtsgutsverletzung beinhaltet. Ist vorwiegend die Privatsphäre vor dem unbefugten Offenbaren von Geheimnissen durch einen Schweigepflichtigen geschützt, folgt daraus, dass ein Übergang des Geheimnisses, das einer bestimmten Person zuordenbar ist, aus dem Bereich der Privatsphäre nach außen verhindert werden soll. Nicht auf die abstrakte Geeignetheit einer Handlung zur Geheimnisverletzung wird dem Wortlaut nach abgezielt, sondern auf den erfolgten Übergang aus dem Bereich der Privatsphäre nach außen entgegen dem Willen des betroffenen Geheimnisträgers[113].

Einzuräumen ist dabei, dass das Tatbestandsmerkmal „Offenbaren" unscharf ist und dem Wortlaut nach die Berücksichtigung von Gefahrmomenten zulässt. Denn weder ist eine zielgerichtete Weitergabe an einen Empfänger vorgegeben, da das Gesetz einfach nur von einem „Offenbaren" spricht[114], noch ergibt sich aus dem Begriff „Offenbaren", dass die Tathandlung auf positives Tun beschränkt ist. Die Weite des Begriffs „Offenbaren" kann indes nicht dazu führen, in § 203 StGB ein abstraktes Gefährdungsdelikt zu sehen. Dies würde den Wortlaut sprengen und den beabsichtigten Rechtsgüterschutz verkennen. Dem unbefugten Offenbaren in § 203 StGB kann per se keine gefährliche Situation bzw. ein gefährlicher Zustand entnommen werden. Auch wird nicht eine an sich gefährliche oder gefahrgeneigte Tätigkeit beschrieben. Vielmehr soll die grundsätzliche Souveränität des Geheimnisträgers geachtet werden, selbst darüber zu entscheiden, welche Geheimnisse nach außen gelangen und welche nicht. Es geht nicht darum, Geheimnisse aufgrund des in ihnen enthaltenen objektiven Wertes vor einer Gefährdung zu schützen, sondern um die zu verhindernde Konsequenz eines Offenbarens, nämlich, dass dann ein Geheimnis nicht mehr geheim ist. Mehr ist der Tathandlung in Verbindung mit dem primär geschützten Rechtsgut nicht zu entnehmen. Fragen der Verwertbarkeit bzw. einer möglichen sozialen Auswirkung eines bekannt gewordenen Geheimnisses haben mit der Tathandlung nichts zu tun. Sie sind dem Offenbaren vor- bzw. nachgeschaltet.

Davon zu trennen ist die Frage, wie der Bezug Dritter zu den Geheimnissen beschaffen sein muss, um von einem vollendeten Offenbaren sprechen zu können.

---

[113] Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 481.
[114] Anders z.B. § 17 UWG, der verlangt, dass Betriebs- oder Geschäftsgeheimnisse an jemanden mitgeteilt werden müssen.

Hier ist fraglich, inwiefern vor dem Hintergrund des informationellen Selbstbestimmungsrechts, der fehlenden Versuchsstrafbarkeit und der auch generalpräventiven Wirkung des § 203 StGB Gefährdungsaspekte im Rahmen der Auslegung des weiten Tatbestandsmerkmals „Offenbaren“ Bedeutung haben können. Dies bedeutet aber nicht, dass § 203 StGB insgesamt als Gefährdungsdelikt interpretiert werden müsste.

Im Ergebnis ist § 203 StGB daher als Verletzungsdelikt[115].

III. Täterkreis

Der Qualifikation des § 203 StGB als Sonderdelikt entspricht es, dass Täter nur die in § 203 StGB genannten Personen sein können. Die Vorschrift des § 203 StGB unterteilt den tauglichen Täterkreis in zwei Gruppen. In § 203 Abs. 1 StGB sind Personen genannt, die einem bestimmten Beruf oder einer bestimmten Tätigkeit nachgehen. Dieser Täterkreis ist dem privatrechtlichen Bereich zuzuordnen. Im Gegensatz dazu ist der Täterkatalog des § 203 Abs. 2 StGB dem öffentlich-rechtlichen Bereich zugeordnet. Ergänzt wird der Täterkreis des § 203 Abs. 1 StGB durch die Regelung des § 203 Abs. 3 StGB, wonach berufsmäßig tätige Gehilfen und Personen, die zur Vorbereitung auf den Beruf tätig sind, den in § 203 Abs. 1 Satz 1 StGB Genannten gleichstellt sind. Im vorliegenden Zusammenhang ist § 203 Abs. 1 Nr. 1 StGB, der die Ärzteschaft erfasst, § 203 Abs. 1 Nr. 6 StGB, der Angehörige privater Krankenkassen erfasst, sowie § 203 Abs. 2 StGB, der Angehörige der gesetzlichen Krankenkassen erfasst, von Interesse.

[115] Für eine Einordnung Verletzungsdelikt Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 479; wohl auch Schünemann, in: Leipziger Kommentar StGB § 203 Rn. 15; diese Sichtweise wirkt tendenziell unsachgemäßen Strafbarkeitsausweitungen entgegen und wird eher der ultima ratio Funktion des Strafrechts gerecht; eine Unterscheidung zwischen konkretem Gefährdungsdelikt und Verletzungsdelikt ist nur bedingt aussagekräftig und relativiert sich vielfach, da bei beiden Kategorien ein Erfolg eintreten muss und die Trennlinie zwischen konkretem Gefährdungsdelikt und Verletzungsdelikt unscharf ist, so dass vielfach auf die Frage des Erfolgseintritts abzustellen ist und weniger auf die Intensität der Beeinträchtigung des betroffenen Handlungsobjekts; zur Einordnung als Sonderdelikt vgl. Tröndle/Fischer, StGB, § 203 Rn. 11.

IV. Geheimnisbegriff und medizinische Daten

§ 203 StGB stellt das Offenbaren fremder Geheimnisse unter Strafe. Insofern ist zu klären, ob bei möglichen Outsourcingvorhaben medizinischer Daten fremde Geheimnisse betroffen sind.

1. Elemente des Geheimnisbegriffs

Der Begriff „Geheimnis“ i.S.v. § 203 StGB ist nicht legaldefiniert. Überwiegend wird in der Literatur und Rechtsprechung ein Geheimnis definiert als eine Tatsache, die nur einem Einzelnen oder einem beschränkten Personenkreis bekannt oder zugänglich ist, deren Kenntnis nach dem Willen des Betroffenen hierauf beschränkt ist und an deren Geheimhaltung der Betroffene ein schutzwürdiges Interesse hat[116]. Verlangt werden ein Geheimsein[117], ein Geheimhaltungswille und ein objektives Geheimhaltungsinteresse[118]. Daneben finden sich Definitionen, die ausschließlich auf den Willen[119] oder das Interesse[120] des Betroffenen abstellen[121].

In der Sache ergeben sich kaum Unterschiede, denn bei der Ermittlung des schutzwürdigen Interesses hat der ausdrückliche Wille des Betroffenen Vorrang. Dies gebietet schon das Recht auf informationelle Selbstbestimmung, abgeleitet aus Art. 2 Abs. 1 i.V.m. Art 1 Abs.1 GG. Ein Geheimnis kann jemandem nicht gegen seinen Willen aufgedrängt werden. Nur wenn ein ausdrücklicher Wille fehlt, ist auf das Interesse, gefolgert aus dem mutmaßlichen Willen, abzustellen. Der Vorrang des Willens findet aber dort seine Grenze, wo vernünftigerweise eine strafrechtliche Sanktion nicht angemessen ist. Dies betrifft so genannte „Bagatell-

---

[116] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 19; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 11.

[117] Offenkundige Tatsachen unterliegen nicht dem Geheimnisschutz, vgl. Ulsenheimer, Arztstrafrecht in der Praxis, S. 357. Offenkundigkeit ist abzulehnen, wenn der Zugang nicht für jedermann gleich leicht zugänglich ist. Dies ist etwa dann der Fall, wenn für eine Auskunftserteilung aus einem öffentlichen Register die Darlegung eines berechtigten Interesses erforderlich ist, vgl. zutreffend BGH RDV 2003, S. 130 ff, und Meyer/Brocks/Nordmann, RDV 2001, S. 13; a.A. BayObLG NJW 1999, S. 1727, HansOLG Hamburg NStZ 1998, S. 358; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 48 a. E.

[118] Vgl. aus der Literatur Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 89; Schmitz, JA 1996, S. 775; aus der Rechtsprechung vgl. OLG Hamm vom 22.02.2001, Az.: 2 Ws 9/01.

[119] Jung, in: NK StGB, § 203 Rn. 4;

[120] Tröndle/Fischer, StGB, § 203 Rn. 6; Lenckner, in: Schönke/Schröder, StGB, § 203 Rn. 5.

[121] Vgl. näher dazu Bruns, Die Schweigepflicht der Sozialen Dienste der Justiz, S. 54ff.; Maurach/Schroeder/Maiwald, Strafrecht BT, Teilband 1, S. 309f.

geheimnisse“, wie beispielsweise die üblichen Personalien[122]. Dies gilt aber nur, sofern es bloß um Bagatellgeheimnisse geht. Sind über die Bagatellgeheimnisse hinaus weitere bedeutsame Geheimnisse, beispielsweise eine ärztliche Behandlung oder die Tatsache, dass jemand krankenversichert ist[123], in Erfahrung zu bringen, erfasst der Geheimnisbegriff auch Bagatellgeheimnisse[124].

In ähnlicher Weise wird eine Kombination von Wille und Interesse, bei grundsätzlichem Vorrang des ausdrücklich erklärten Willens, im Rahmen der Geschäftsführung ohne Auftrag bei § 683 BGB vorgenommen[125]. Zwar bezweckt § 683 BGB einen zivilrechtlichen Ausgleich und hat somit eine andere Funktion als § 203 StGB, inhaltlich will § 683 BGB aber ähnlich wie § 203 StGB verhindern, dass sich Außenstehende ungebeten in fremde Angelegenheiten einmischen[126]. Dies soll bei § 683 BGB zutreffend durch eine vorrangige Orientierung an dem Willen des Geschäftsherrn gewährleistet werden. Erst recht muss dies dann für die Bestimmung des Geheimnisses in § 203 StGB gelten. Ein ausschließliches einseitiges Abstellen auf den Willen oder das Interesse ist daher abzulehnen. Vielmehr bedarf es einer Kombination von Geheimhaltungswille und Geheimhaltungsinteresse in dargestellter Weise.

2. Geheimnis als personenbezogene Information

Gegenständlich erfasst der Geheimnisbegriff in § 203 StGB nur Tatsachen[127]. Nicht geschützt werden Unwahrheiten ebenso wie Werturteile[128]. Diese vom Ansatz her klare Einteilung begegnet in der praktischen Abgrenzung Schwierigkeiten. Auch Werturteile können ein „Geheimnis“ i.S.v. § 203 StGB darstellen, allein aufgrund der Tatsache ihrer Existenz. Schwierigkeiten bereitet die Abgrenzung auch bei Schlussfolgerungen, die aufgrund besonderen beruflichen Wissens gezo-

---

[122] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 27.
[123] Vgl. Ayasse, VersR 1987, S. 536f.; Rein, VersR 1976, S. 120; Köpke, Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für die private Krankenversicherung, S. 32; vgl aus der Rechtsprechung OLG Karlsruhe, RDV 2006, S. 265.
[124] BAG NZA 1987, S. 2615; vgl. auch BGHSt 33, 148 (152); BGHSt 45, 363 (366); Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 471.
[125] Palandt, BGB, § 683 Rn. 5; Beuthien, in: Soergel, BGB, § 683 Rn. 5; zweifelnd Seiler, in: Münchener Kommentar BGB, § 683 Rn. 13.
[126] Vgl. Beuthien, in: Soergel, BGB, Vor. § 677 Rn. 2; Erman, BGB, I, Vor. § 677 Rn. 3.
[127] Tröndle/Fischer, StGB, § 203 Rn. 4.
[128] Schmitz, JA 1996, S. 774; anders wird dies für den Bereich der personenbezogenen Daten i.S.v. § 3 BDSG beurteilt, vgl. Dammann, in: Simitis, Bundesdatenschutzgesetz, § 3 Rn. 12; für den Bereich der Sozialdaten vgl. Bieresborn, in Wulffen, SGB X § 67 Rn. 7, 8.

gen werden. Hier lassen sich die Tatsachen, die die Grundlage für fachliche Schlussfolgerungen bilden, nur schwer von Wertungen trennen. Daher ist es sinnvoll, solche beruflichen Schlussfolgerungen insgesamt dem Geheimnisbegriff zu unterwerfen, sofern Tatsachen und Schlussfolgerung miteinander verbunden sind[129].

Geheimnisse können nur Personen haben[130]. Daher kann nur von einem Geheimnis gesprochen werden, wenn ein Umstand einer Person zugeordnet werden kann, also über das Geheimnis die betroffene Person identifiziert werden kann. Ein Umstand, der an sich nicht ein Geheimnis darstellt, kann schließlich zu einem solchen werden, wenn er untrennbar mit einem Geheimnis verbunden ist. All dies lässt den Schluss zu, dass Geheimnisse mit dem Begriff der „personenbezogenen Informationen“ umschrieben werden können[131].

Im Hinblick auf das Outsourcing medizinischer Daten ist von Interesse, ob und wann solche personenbezogenen Informationen betroffen sind. Da Daten dargestellte Informationen sind, muss geprüft werden, wann in den Daten personenbezogene Informationen enthalten sind. Kein „Geheimnis“ i.S.v. § 203 StGB sind zumeist medizinische Daten, die medizinisches Wissen darstellen. Solche Daten werden in der Regel durch Publikation in Fachmedien der wissenschaftlichen Öffentlichkeit in anonymer Form zur Verfügung gestellt. Eine Individualisierung von Personen ist ausgeschlossen. Solche Daten bereiten bei Outsourcingvorhaben für keinen der vorliegend in Frage kommenden Outsourcinggeber relevante Probleme[132]. Sie sollen daher im Folgenden außer Betracht bleiben.

Hinsichtlich der sonstigen medizinischen Daten ist maßgeblich, ob sie einen Personenbezug haben. Dies ist für den jeweiligen in Betracht kommenden Outsourcinggeber anhand der konkreten Datenart zu bestimmen.

---

[129] Knemeyer, DB 1984, Beil. 18/84; zu weiteren Beispielen im medizinischen Bereich Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 20.
[130] Die Frage, ob auch juristische Personen des Privatrechts sowie des öffentlichen Rechts taugliche Geheimnisträger sein können, braucht hier nicht untersucht zu werden. Vgl. dazu Schünemann, in: Leipziger Kommentar StGB, § 203 StGB Rn. 31, 32.
[131] Vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 89; Tröndle/Fischer, StGB, § 203 Rn. 4.
[132] Zur Publikation von Patientenfotos vgl. Schlund, MedR 90, S. 323.

Bei privaten Krankenversicherungen fallen medizinische Daten hinsichtlich der versicherten Personen an. Dies sind alle Daten, die bei den privaten Krankenversicherungen als Einrichtungen im Gesundheitswesen im Zusammenhang mit der Vertragsdurchführung und ihren Leistungen über den Versicherten gesammelt werden und die eine Aussage über den körperlichen oder geistigen Zustand des Versicherten zulassen[133]. Maßgebliche Grundlage für den Datenfluss zum Versicherungsgeber ist der Versicherungsvertrag.

Diese Versicherungsdaten erfüllen zumeist den Geheimnisbegriff. Sie sind nur einem beschränkten Kreis von Personen zugänglich. Der Betroffene hat den Willen, dass diese Daten geheim bleiben. Dies folgt aus der Natur der in den Daten verkörperten Informationen über sensible, persönliche Bereiche des Versicherten, deren Nachaußendringen für den Betroffenen einen erheblichen sozialen Schaden bedeuten kann. Schließlich besteht auch ein objektives schutzwürdiges Interesse an der Geheimhaltung der Daten. Es handelt sich bei den Daten des Krankenversicherten in aller Regel nicht um Bagatellgeheimnisse.

Für gesetzliche Krankenkassen, die von § 203 Abs. 2 StGB erfasst werden, gilt hinsichtlich der Daten über ihre versicherten Mitglieder im Grundsatz das Gleiche wie für private Krankenversicherungen. Maßgebliche Grundlage für den Datenfluss medizinischer Daten zu den gesetzlichen Krankenversicherungen ist aber nicht ein Versicherungsvertrag, sondern die Regelungen in den §§ 284 ff SGB V. Betreffen Outsourcingvorhaben den ärztlichen Bereich, sind alle Daten, die Informationen über einen Patienten ermöglichen, unabhängig, ob der stationäre oder der ambulanten Bereich betroffen ist, personenbezogene Informationen. Dies gilt beispielsweise auch für den Patientennamen, der nicht als Bagatellgeheimnis aus dem Geheimnisbegriff ausgeschieden werden kann[134].

3. Reichweite des Personenbezugs

Beabsichtigt ein Outsourcinggeber aus diesen Bereichen medizinische Daten, die personenbezogene Informationen enthalten, outzusourcen, ist für den Outsourcer

---

[133] Vgl. Bergmann/Möhrle/Herb, BDSG, § 3 Rn. 171.
[134] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 29 mit weiteren Beispielen aus dem ärztlichen Bereich; so auch OLG Karlsruhe RDV 2006, S. 265.

von Interesse, ob sich der Personenbezug durch einfache Maßnahmen auflösen lässt, so dass kein „Geheimnis“ im Sinne von § 203 StGB vorliegt. Um dies beantworten zu können, ist vorab zu klären, wie die Verknüpfung zwischen Information und Person beschaffen sein muss, damit sie als personenbezogen bezeichnet werden kann. Ausführliche Stellungnahmen zu dieser Frage aus der Literatur unmittelbar zu § 203 StGB finden sich kaum und bleiben an der Oberfläche. So wird Personenbezug angenommen, wenn eine nicht nur theoretische Identifizierungsmöglichkeit gegeben ist[135]. Wann eine mehr als nur theoretische Identifizierungsmöglichkeit vorliegt, wird nicht näher erörtert.

a) Rückgriff auf das Datenschutzrecht

Demgegenüber wird im Rechts des Datenschutzes die Frage, ob Daten personenbezogen sind oder nicht, ausführlich diskutiert. Sie betrifft ein Kernproblem des Datenschutzrechts[136]. Es wäre hilfreich, wenn für diese Frage auf das Datenschutzrecht zurückgegriffen werden und die Bestimmung des Personenbezuges in beiden Bereichen parallel erfolgen kann. Im Datenschutzrecht findet sich in § 3 Abs. 1 BDSG eine Begriffsbestimmung personenbezogener Daten. Danach sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Keine Aussage wird darüber getroffen, wann Einzelangaben über persönliche Verhältnisse eine Person bestimmen oder als bestimmbar erscheinen lassen.

Inhaltliche Kriterien dazu finden sich in Art. 2 Abs. a der EG- Datenschutzrichtlinie. Danach sind personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person (betroffene Person). Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Hierunter fallen auch Daten wie Bild und Stimme, Fingerabdrücke und genetische Merkmale[137].

[135] Tröndle/Fischer, StGB, § 203 Rn. 4; OLG Karlruhe NJW 1984, S. 676.
[136] Vgl. Saeltzer, DuD 2004, S. 1; Dammann, in: Simitis, BDSG, § 3 Rn. 1.
[137] Ehmann/Helfrich, EG-Datenschutzrichtlinie, Art. 2 Rn. 17.

Die Feststellung, ob eine Person direkt oder indirekt identifiziert werden kann, bedarf einer konkreten Prüfung im Einzelfall[138]. Insbesondere bei Daten, die visuelle oder akustische Informationen enthalten, kann die Bestimmung schwierig sein. Neben der positiven Feststellung ist im Hinblick auf die Aufhebung des Personenbezugs die Frage bedeutsamer, wie Daten beschaffen sein müssen, damit kein Personenbezug vorliegt. Hierüber gibt § 3 Abs. 6 BDSG näher Aufschluss. Daten sind danach anonym, wenn sie derart verändert sind, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Durch Anonymisierung kann, muss aber nicht, der Personenbezug verloren gehen[139].

Ähnlich wird der Personenbezug in der Recommendation No. R (97) on the Protection of Medical Data of the Council of Europe definiert: "The expression personal data covers any information relating to an identified or identifiable individual. An individual shall not be regarded as identifiable if identification requires an unreasonable amount of time and manpower. In cases where the individual is not identifiable, the data are referred to as anonymous"[140]. Hier werden die Begriffe personal data und anonymous spiegelbildlich gebraucht[141]. Daraus kann gefolgert werden, dass das Risiko einer Identifikation und damit eine Individualisierung niemals völlig ausgeschlossen werden kann. Maßgebend für den Begriff des Personenbezugs ist danach eine Verhältnismäßigkeitsbetrachtung. Ob ein unverhältnismäßig großer Aufwand an Zeit und Arbeitskraft vorliegt, kann nur im konkreten Einzelfall bestimmt werden und hängt von mehreren Faktoren ab[142]. Zu berücksichtigen sind beispielsweise der Stand der technischen Entwicklung, die Kenntnisse der Datenverwender, die organisatorisch technische Konzeption und die zur Verfügung stehende Zeit[143].

---

[138] Vgl. Dammann, in: Simitis, BDSG, § 3 Rn. 38.
[139] Dammann, in: Simitis, BDSG, § 3 Rn. 23; Schaffland/Wiltfang, BDSG, § 3 Rn. 15.
[140] Luttenberger et al., Datenschutz in der pharmakogenetischen Forschung – eine Fallstudie, DuD 2004, S. 356f.
[141] Dies gilt nach überwiegender Meinung nicht für den Begriff „personenbezogene Daten", vgl. Dammann, in: Simitis, BDSG, § 3 Rn. 23.
[142] Vgl. Dammann, in: Simitis, BDSG, § 3 Rn. 30-32.
[143] Vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 90.

Diese Aussagen sind im Datenschutzrecht allgemein anerkannt. Es fragt sich, ob diese Aussagen auch für die Bestimmung des Personenbezugs in § 203 StGB verwendet werden können. Bedenken hiergegen könnten aus den Unterschieden zwischen dem Schutz des Privatgeheimnisses und dem Datenschutzrecht erwachsen[144]. Bedeutsam ist in diesem Zusammenhang die Auffassung, dass das Privatgeheimnis im Verhältnis zum Datenschutzrecht zu Einschränkungen in der praktischen Handhabung des Datenumgangs führe[145]. Dies wird daraus abgeleitet, dass das Privatgeheimnis ein personales Geheimnis ist und mithin eine Verankerung in der natürlichen Person hat. Es gilt nach h.M. selbst zwischen gemeinsam Schweigepflichtigen, also beispielsweise zwischen zwei Ärzten[146]. Allein die Tatsache, dass Beteiligte der Schweigepflicht unterliegen, ist unerheblich[147]. Nur innerhalb von Funktionseinheiten soll die Schweigepflicht nicht gelten[148].

Das Datengeheimnis stellt hingegen darauf ab, wo, wie und wozu der Umgang mit Daten erfolgt und ist damit zweck- und objektbezogen. Dies zeigt sich darin, dass für das Datengeheimnis die Begriffe der Zweckbindung und der verarbeitenden Stelle maßgeblich sind[149]. So verpflichtet § 5 BDSG die bei der Datenverarbeitung beschäftigten Personen auf das Datengeheimnis. Mit der Datenverarbeitung in § 5 BDSG ist zutreffend die Organisationseinheit, innerhalb der Daten erhoben, verarbeiten oder genutzt werden, zusammen mit den bei dieser Einheit in einem Beschäftigungsverhältnis stehenden Personen gemeint[150]. Die Zweckbindung ist ein prägendes Element des Datenschutzrechts und kommt in verschiedenen Vorschriften des BDSG zum Ausdruck[151]. Durchbrechungen des Privatgeheimnisses

---

[144] Vgl. zu den Unterschieden Weichert, Datenschutz-Audit und -Gütesiegel im Medizinbereich, MedR 2003 , S. 679.
[145] Weichert, Datenschutz-Audit und - Gütesiegel im Medizinbereich, MedR 2003 , S. 679.
[146] Rein, VersR 1976, S.117, 120; Weichert, Datenschutz-Audit und -Gütesiegel im Medizinbereich, MedR 2003 , S. 679.
[147] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 41; Niedermair, in: Roxin/Schroth, Medizinstrafrecht, S. 370; Bay ObLG StV 1996, S. 484.
[148] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 42.
[149] Weichert, DuD 2003, S. 679; beispielhaft für die Zweckbindung sei auf die Neufassung des § 28 BDSG als zentrale Vorschrift für die Verwendung personenbezogener Daten im nichtöffentlichen Bereich hingewiesen, dazu Simitis, in: Simitis, BDSG, § 28 Rn. 2; weitere Vorschriften, die Ausdruck des Grundsatzes der Zweckbindung sind, finden sich in §§ 4b Abs. 6, 5, 15 Abs. 3, 16 Abs. 4, 28 Abs. 5, 29 Abs. 4, 39 und 40; vgl. Dammann, in: Simitis, BDSG § 3 Rn. 244.
[150] Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 2 Rn. 8ff.; Schaffland/Wiltfang, BDSG, § 5 Rn. 5; Gola/Schomerus, BDSG, § 5 Rn. 8ff.; Walz, in: Simitis, BDSG, § 5 Rn. 17, 23; a.A. Dammann, in: Simitis, BDSG, § 2 Rn. 16, 17; vgl. zu den Auswirkungen der Unterscheidung zwischen Funktionseinheit und Organisationseinheit Bruns, Die Schweigepflicht der sozialen Dienste der Justiz, S. 117f.
[151] Die Zweckbindung ist Vorgabe des „Volkszählungsurteils“ BVerfGE 65 1, (45); vgl. § 14 Abs. 2 BDSG und dazu Sokol, in: Simitis, BDSG, § 14 Rn. 53 ff.; Bergmann/Möhrle/Herb,

sind nur ausnahmsweise möglich[152], während Durchbrechungen des Datengeheimnisses weitgehend zugelassen sind[153].

Konsequent zu diesen Unterschieden wird überwiegend vertreten, dass § 203 StGB und das Datenschutzrecht parallel gelten, und nicht § 203 StGB das Datenschutzrecht als speziellere Vorschrift verdrängt[154]. Hierfür spricht auch der Wortlaut des § 1 Abs. 3 Satz 2 BDSG, der ausdrücklich die Anwendung von Berufsgeheimnissen, die § 203 StGB schützt, unberührt lässt. Die Anforderungen des § 203 StGB und die Anforderungen des Datenschutzrechts sind grundsätzlich getrennt zu betrachten und kumulativ zu beachten.

Aus der Objektbezogenheit des Datengeheimnisses könnte gefolgert werden, dass ein Abstellen auf das Kriterium des unverhältnismäßigen Aufwandes der Identifizierung im Rahmen der Bestimmung der Personenbezogenheit bei § 203 StGB nicht zulässig ist. In der Tat kann argumentiert werden, dass die damit verbundene Verknüpfung mit tatsächlichen Entwicklungen nicht mit der Qualifizierung als personales Geheimnis in Einklang zu bringen ist. Auch nach Veränderungen der Daten unter Aufhebung des Personenbezugs müssten dann die Daten als „Geheimnisse“ i.S.v. § 203 StGB gelten.

Diese Argumentationsweise ist jedoch nicht zwingend. Die Bindung an eine verantwortliche natürliche Person ist vor dem historischen Hintergrund zu betrachten[155]. In den Anfängen der Schweigepflicht war der individuelle Schutz der Persönlichkeitssphäre nicht maßgeblich. Hier war der Blick auf die berufliche Stellung des Schweigepflichtigen, verbunden mit seiner gesellschaftlichen Stellung, entscheidend. Spätestens seit der Ausarbeitung des Rechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht ist aber eine vorwiegend individuelle Schutzrichtung des § 203 StGB anzunehmen, auch wenn das ge-

---

BDSG, § 14 Rn. 34; vgl. auch die Einführung einer Zweckbindung im nicht-öffentlichen Sektor in § 28 Abs. 7 und 8 BDSG.

[152] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 42.

[153] Weichert, DuD 2003, S. 679; vgl. für den medizinischen Bereich die Zulässigkeit einer Zweckänderung bei Gesundheitsdaten in § 14 Abs. 6 BDSG, dazu Sokol, in: Simitis, BDSG, § 14 Rn. 156; Eichelbrönner, Die Grenzen der Schweigepflicht des Arztes, S. 159.

[154] Schirmer, in: Handbuch des Datenschutzrechts, S. 1366; Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 84f.; Gola/Schomerus, BDSG, § 5 Rn. 2; Walz, in: Simitis, BDSG, § 5 Rn. 7; a.A. wohl Schlund, in: Handbuch des Arztrechts, § 76 Rn. 24.

[155] Zu der historischen Entwicklung Schlund, in: Handbuch des Arztrechts, S. 545ff.; Schäfer, Ärztliche Schweigepflicht und Elektronische Datenverarbeitung, S. 18ff.

schützte Rechtsgut nicht identisch mit dem Recht auf informationelle Selbstbestimmung ist.

Dies legt es nahe, die Frage der Personenbezogenheit an dem zu verwirklichenden Schutz des informationellen Selbstbestimmungsrechts auszurichten. Dass der Gesetzgeber den Schutzbereich auf bestimmte institutionelle Beziehungen eingeengt hat, muss nicht bedeuten, dass dies auf die inhaltliche Bestimmung der Personenbezogenheit durchschlägt. Die Beschränkung des Schutzbereichs ist plausibel zu erklären als Wertung des Gesetzgebers, in welchen Situationen mit Blick auf die gesellschaftlichen Entwicklungen der Einsatz des Strafrechts zum Schutz des persönlichen Bereichs als ultima ratio angezeigt ist[156].

Die Frage nach der Personenbezogenheit hingegen betrifft das Verhältnis Individuum und Allgemeinheit. Ob bestimmte Daten Informationen enthalten, die das betroffene Individuum identifizieren können, ist sachbezogen zu beurteilen. Es gilt das Risiko der Identifizierung zu bewerten. Dafür sind tatsächliche Einflussfaktoren maßgeblich, anhand deren das Risiko der Individualisierung abgeschätzt werden muss. Die Bindung an Berufsgruppen oder an Institutionen kann keine inhaltlichen Kriterien für die Bestimmung liefern. Die institutionellen Vertrauensbeziehungen, die in § 203 StGB erwähnt sind, bieten , wegen ihrer Inhomogenität, dafür keinen tauglichen Bewertungsmaßstab. Die Frage des Personenbezugs kann schlecht unterschiedlich beantwortet werden, je nachdem, ob die Informationen ein Arzt, ein Heilpraktiker oder ein bei einer datenverarbeitenden Stelle Beschäftigter bereithält. Die Qualifizierung muss von der Art der Information und dem Informationsgehalt ausgehen sowie von tatsächlichen Einflussfaktoren, unabhängig von der Person, die für die Daten verantwortlich ist. Davon ist die Frage zu trennen, welche Anforderungen in persönlicher Hinsicht an die für den Umgang mit den Daten Verantwortlichen gestellt werden.

Die Frage des Personenbezugs ist daher losgelöst von der konkreten Vertrauensbeziehung zwischen Schweigepflichtigen und Betroffenen zu beantworten. Ein Rückgriff auf Grundsätze des Datenschutzrechts zur Bestimmung des Personenbezugs ist somit zulässig.

---

[156] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 4, 16.

b) Maßnahmen zur Aufhebung der Personenbezogenheit

Damit bleibt zu klären, wann Daten so verändert sind, dass sie als nicht personenbezogen zu gelten haben. Für den Outsourcinggeber sind Kriterien von Interesse, anhand derer sich der zuverlässige Ausschluss des Personenbezugs und die Anonymität der Daten beurteilen lässt. Für den Bereich alphanumerischer Datenverarbeitung ist dies verhältnismäßig leicht zu beantworten. Sind Name und Adresse bekannt, lassen sich diese Informationen leicht einer bestimmten Person zuordnen. Schwieriger kann dies bei Bild-, Video- oder Audiodaten sein[157].

Als medizinische Daten entstehen solche Daten insbesondere infolge bildgebender Diagnoseverfahren oder graphisch dargestellter Befundergebnisse. Im ärztlichen Bereich werden die Daten zusammen mit weiteren Daten des Patienten gesammelt. Im Bereich der Krankenversicherung werden diagnostische Daten von den Ärzten oder Krankenhäusern aufgrund gesetzlicher Vorschriften, aufgrund vertraglicher Abreden oder aufgrund der Einwilligung der Betroffenen an die Versicherungsträger weitergegeben. Bei den Versicherungen werden dann die Daten ebenfalls zusammen mit weiteren Daten des Versicherten gesammelt. Sollen die Daten insgesamt outgesourct werden, muss sichergestellt sein, dass der Personenbezug aufgehoben ist.

Eine Möglichkeit könnte in der vollständigen Verschlüsselung der outgesourcten Daten bestehen[158]. Unter einer Verschlüsselung ist ein Verfahren zu verstehen, welches ermöglicht, Daten zu chiffrieren und für Dritte dem Sinn nach nicht lesbar zu machen[159]. Als Synonym zur Verschlüsselung wird meist der Begriff der Kryptographie gebraucht[160].

---

[157] Plastisch werden diese Schwierigkeiten dargestellt bei Saeltzer, DuD 2004, S. 218ff.
[158] Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 83, 20. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz 2003, S. 270.
[159] Kußmann, Lexikon der Kommunikations- und Informationstechnik, S. 575; Dammann, in: Simitis, BDSG, § 3 Rn. 32; Hermeler, Rechtliche Rahmenbedingungen, S. 92; Heibey, in: Rossnagel, Handbuch Datenschutzrecht, S. 592 ff.; Jürgens, in: Bäumler/Breinlinger/Schrader, Datenschutz von A-Z, S 2000, S. 3; zur Funktionsweise der Verschlüsselung Scheffler, in: Kilian/Heussen, Computerrechts-Handbuch, Teil 10, 105 Rn. 3; vgl. allgemein zu Verfahren der Kryptographie Beutelspacher/Schwenk/Wolfenstetter, Moderne Verfahren der Kryptographie, S. 1 ff.
[160] Dammann, in: Simitis, BDSG, § 3 Rn. 32; Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 92.

Bezweckt wird die Geheimhaltung der in den Daten erhaltenen Information, so dass diese über unsichere Transportmedien verschickt werden können, ohne dass Dritte den Sinn der Information zur Kenntnis nehmen können, auch wenn Sie sich unbemerkt Zugriff auf die Daten verschaffen[161]. In dieser Zwecksetzung allein, nicht im Verfahren, unterscheidet sich die Verschlüsselung von der Codierung, bei der der Code bekannt gegeben wird und die somit nicht zu einer Anonymisierung führen kann[162].

Bei der Verschlüsselung werden die Daten nicht in einem Behältnis eingeschlossen, sondern die Information wird in eine geheime Sprache transformiert. Eine alte, bekannte Form der Verschlüsselung im analogen Bereich ist ein physikalisch-chemisches Verfahren, mit dem Tinte abhängig von der Temperatur sichtbar gemacht werden kann. Bekannt geworden ist auch die mechanische Verschlüsselung mit der Verschlüsselungsmaschine „ENIGMA“ im Zweiten Weltkrieg.

Im digitalen Bereich existieren verschiedene Verschlüsselungsalgorithmen als mathematische Grundlage[163]. Grundsätzlich sind, unabhängig der Vielzahl der Verschlüsselungsalgorithmen, zwei Arten von Verschlüsselungskonzepten zu unterscheiden, das symmetrische und das asymmetrische Verschlüsselungsverfahren[164]. Der Unterschied zwischen beiden Verfahren liegt darin, dass bei der symmetrischen Verschlüsselung der Schlüssel sowohl auf der Absenderseite als auch auf der Empfängerseite gleich ist, während bei der asymmetrischen Verschlüsselung die Schlüssel auf beiden Seiten verschieden sind.

Möglich ist auch eine Kombination der asymmetrischen und der symmetrischen Verschlüsselung dergestalt, dass zunächst die Daten mit einem symmetrischen Verfahren verschlüsselt werden. Anschließend wird der verwendete Schlüssel mit einem asymmetrischen Verfahren selbst verschlüsselt. Ziel dieses Vorgehens ist es die Geschwindigkeit des aufwendigeren asymmetrischen Verfahrens zu erhö-

---

[161] Dammann, in: Simitis, BDSG, § 3 Rn. 32.
[162] Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 92; allgemein zugänglich ist die Codierung nach dem Morse-Alphabet; ebenso die Verschlüsselung von Krankheiten nach dem ICD-Diagnoseschlüssel, dazu Menzel, in: Bäumler/Breinlinger/Schrader, Datenschutz von A-Z, I 100, S. 1ff. und BVerfG vom 10.04.2000, Az.: 1 BvR 422/00. Über den ASCII Code (American Standart Code of Information Interchange) kann jede Zahl in die binäre Maschinensprache transformiert werden.
[163] Kußmann, Lexikon der Kommunikations- und Informationstechnik, S. 575.
[164] Holznagel, Recht der IT-Sicherheit, S. 89f.; Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 93.

hen. Dies gelingt dadurch, dass dieses Verfahren nur für eine kleine Datenmenge, nämlich den Schlüssel, angewandt wird. Neben den Daten können auch ganze Verbindungen verschlüsselt werden[165].

Ob eine Verschlüsselung zu einer Aufhebung des Personenbezugs führt ist nicht unumstritten. Für den speziellen Bereich der Telemedizin wird bezogen auf das Datenschutzrecht vertreten, dass eine Verschlüsselung nicht zur Aufhebung des Personenbezugs führt. Als Begründung wird angeführt, dass zwar grundsätzlich im Einzelfall festzustellen ist, ob eine Bestimmbarkeit der Person gegeben ist, allerdings soll im Bereich der Telemedizin nicht auf die relative Möglichkeit der Kenntnisnahme, sondern in einer Gesamtschau auf das eröffnete Gefährdungspotential abzustellen sein[166]. Aufgrund des Einsatzes digitaler Netze und der Vielzahl möglicher Teilnehmer bestehe immer die Möglichkeit der Entschlüsselung.

Aufgrund der raschen Entwicklung im Bereich der Kryptographie erscheint das Misstrauen in die Sicherheit von Verschlüsselungssystemen berechtigt. Es besteht die Gefahr, dass Daten, die wegen Verschlüsselung als nicht personenbezogen aus dem Anwendungsbereich heraus gefallen sind, wegen geänderter technischer Rahmenbedingungen zu einem späteren Zeitpunkt als personenbezogen gelten müssen. Zu dieser Gefahr wird eingewandt, dass eine nachträgliche Kontrolle der Datenübermittlung in der Praxis nicht möglich ist[167]. Der Entzug des Bestimmungsrechts über verschlüsselte Informationen sei mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Außerdem würde das geringe Risiko der unbefugten Entschlüsselung durch die häufige Übertragung sehr oft auftreten[168]. Schließlich sei das fachliche Wissen und die technischen Hilfsmittel auf dem Markt verfügbar, wodurch die Möglichkeit der Reindividualisierung ausreiche, um eine Aufhebung des Personenbezugs rückgängig zu machen[169]. Im Bereich des Datenschutzrechts sei daher auch bei einer Verschlüsselung der Personenbezug nicht aufgehoben[170]. Demgegenüber wird im Rahmen des § 203 StGB bei

[165] Kußmann, Lexikon der Kommunikations- und Informationstechnik, S. 575; als Beispiel kann ein VPN (Virtual Privat Network) angeführt werden.
[166] Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 155.
[167] Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 155.
[168] Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 155.
[169] Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 154.
[170] Dammann, in: Simitis, BDSG, § 3 Rn. 33.

einem sicheren Verschlüsselungsverfahren ein Geheimnis bejaht, aber ein Offenbaren verneint[171].

Diese Argumente überzeugen im Bereich des § 203 StGB in der Form nicht. Die Verschlüsselung ist nicht per se sicherer als andere Formen der Anonymisierung oder als die in § 3 Abs. 3a BDSG geregelte Pseudonymisierung. Stets muss die Gesamtkonzeption betrachtet werden. Richtig ist zunächst, dass ein isoliertes Abstellen auf die Verschlüsselung das Problem verkürzt. Zuzugeben ist auch, dass bei einer verschlüsselten Übertragung die Möglichkeit des Entschlüsselns u.a. stark von der Rechnerkapazität abhängen kann und damit von der technischen Entwicklung. Somit besteht die Gefahr, dass allein dadurch Verschlüsselungen unsicher werden können. Das mag bei anderen Formen der Verschleierung des Personenbezugs nicht im gleichen Maße der Falls sein. So sind Pseudonymisierungen vorstellbar, an denen die Sicherheit stark an die Kenntnis einzelner Personen gebunden ist[172]. Andererseits kann eine schlechte Pseudonymisierung unwirksamer als eine Verschlüsselung sein.

Auch passt das Betonen der Gefahr der Entschlüsselung wegen technischer Weiterentwicklungen systematisch nicht im gleichen Maße zum Strafrecht wie zum Datenschutzrecht, das, neben dem Bürgerlichen Recht, auch dem besonderen Sicherheitsrecht und Ordnungsrecht zugeordnet werden kann[173]. Im Datenschutzrecht mag man annehmen, dass aufgrund der eigens geregelten Anforderungen an Datenschutz und Datensicherheit eine sichere Verschlüsselung nicht notwendig die Anwendbarkeit des Datenschutzrechts entfallen lässt. Denn hier geht es auch um die Sicherung und Kontrolle eines ordnungsgemäßen Umgangs mit personenbezogenen Daten. Dementsprechend steht bei einer Verletzung von Datenschutzgrundsätzen der Systematik nach nicht die Strafe als Sanktion im Vordergrund. Zum einen können Maßnahmen der staatlichen Aufsicht erfolgen, zum anderen kann Schadensersatz verlangt werden. Ergänzt werden diese Möglichkeiten durch Auskunfts-, Löschungs- und Widerrufsrechte. Daneben besteht, gleichsam als

[171] Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 141.
[172] Beispielsweise über eine nur bestimmten Personen zugängliche Referenzliste, aufgrund derer Pseudonyme bestimmten Personen zugeordnet werden können; den Einsatz eines Datentreuhänders im Zusammenhang mit einer Pseudonymisierung beschreiben Schulte/Wehrmann/Wellbrock, DuD, 2002, S. 605ff.
[173] Zu der Vielfalt der tangierten Bereiche und der Folgen für die Gesetzgebungszuständigkeit Simitis, in: Simitis, BDSG, § 1 Rn. 1, 6ff.

Sicherung und nicht als primäre Sanktion, auch die Möglichkeit eines Bußgeldes oder einer Strafe. Darin zeigt sich die Orientierung am Recht auf informationelle Selbstbestimmung und die Ausgleichsfunktion zwischen Selbstbestimmungsrecht und notwendiger Datenverarbeitung.
Diese Systematik gilt nicht für den vorwiegend am Individualschutz orientierten § 203 StGB. Hier sind Strafzwecke maßgeblich, die nur deshalb zu rechtfertigen sind, weil anderweitige Maßnahmen für den Schutz des Einzelnen als nicht ausreichend angesehen werden (ultima ratio). Auch der Hinweis auf das Recht auf informationelle Selbstbestimmung greift nicht durch. Einerseits ist der Schutzbereich des § 203 StGB, wie oben ausgeführt wurde, nicht identisch mit dem Recht auf informationelle Selbstbestimmung. Andererseits kann dem Persönlichkeitsschutz hinreichend Rechnung getragen werden. Sollte sich erweisen, dass ein Verschlüsselungsverfahren technisch überholt ist, ohne dass die Sicherheit der Verschlüsselung angepasst wird, dann werden die Daten wieder „sichtbar“ und sind als personenbezogen zu beurteilen. Nichts zwingt zu der Annahme, dass ein einmal aufgehobener Personenbezug irreversibel ist.

Im Ergebnis kann nicht der Auffassung gefolgt werden, dass bei einer Verschlüsselung der Personenbezug im Rahmen des § 203 StGB nicht aufgehoben wird. Vielmehr kommt es bei § 203 StGB darauf an, ob nach einer Verschlüsselung in der Gesamtkonzeption eine Person nur mit unverhältnismäßigem Aufwand identifiziert werden kann.

Bei dem Einsatz von Verschlüsselungsverfahren kann nur dann eine Aufhebung des Personenbezugs angenommen werden, wenn eine wirksame Verschlüsselung erfolgt. Wirksam ist eine Verschlüsselung nur dann, wenn Dritte, vor denen die Information geheim gehalten werden soll, die Information auch mit Hilfe von zugänglichem Zusatzwissen und unter Einsatz von Experten und technischen Hilfsmitteln nicht oder nur mit unverhältnismäßigem Aufwand entschlüsseln können[174]. Dies ist letztlich eine Tatsachenfrage, die nur für den Einzelfall nach Ermittlung aller Umstände entschieden werden kann.

[174] Vgl. Dammann, in: Simitis, BDSG, § 3 Rn. 38; Schaffland/Wiltfang, BDSG, § 3 Rn. 15.

c) Bedeutung von Sicherheitsmaßnahmen

Zu beachten sind aber grundsätzliche Aspekte, an denen sich die Prüfung zu orientieren hat und die somit für die rechtliche Beurteilung bedeutsam sind. Zunächst ist grundsätzlich zu differenzieren zwischen dem technischen Bereich und dem organisatorisch-personellen Umfeld, in dem die Technik eingesetzt wird. Die Differenzierung geht von der allgemeinen Erkenntnis aus, dass Technik nur so gut ist wie der Mensch, der sie bedient.

Unter dem technischen Bereich ist das zum Einsatz kommende Verschlüsselungsverfahren mit dem jeweiligen Schlüssel zu verstehen. Schlüssel und Verschlüsselungsverfahren sind begrifflich zu unterscheiden. Durch das prinzipielle Verfahren ist die Festsetzung von konkreten Schlüsseln möglich, die zum Verschlüsseln und Entschlüsseln verwendet werden. Ist das prinzipielle Verschlüsselungsverfahren bekannt, bedeutet dies bei modernen Verschlüsselungssystemen nicht, dass die Daten entschlüsselt werden können, solange der Schlüssel geheim ist. Sind bei einem bekannten Verschlüsselungsalgorithmus keine Schwachstellen bekannt, kann es ausreichen, dass allein der Schlüssel geheim bleibt.

Dies kann jedoch nur unter der Prämisse angenommen werden, dass der Schlüssel an sich sicher ist. Ein Schlüssel ist dann als absolut sicher einzustufen, wenn er von Dritten nicht „geknackt“ werden kann. Geknackt werden und wurden[175] Schlüssel durch das Testen aller bei gegebenem Algorithmus in Betracht kommenden Schlüssel[176]. Vereinfacht kann dies zur Verdeutlichung mit einem mechanischen Zahlenschloss verglichen werden. Ohne die Zahlenfolge zu kennen, kann das Schloss, ohne es zu beschädigen und damit unbrauchbar zu machen, nur geöffnet werden, indem sämtliche Zahlenkombinationen getestet werden. Bei der Verwendung der Ziffern 0-9 pro Einstellungseinheit, hängt die Höhe der möglichen Zahlenkombinationen von der Länge der in Reihe verwendeten Einstellungseinheiten ab. Je mehr Einstellungseinheiten gewählt werden, desto sicherer wird das Schloss.

[175] Vgl. Holznagel, Recht der IT-Sicherheit, S. 89.
[176] So genannte „Brute Force Attack“, vgl. Heibey, in: Rossnagel, Handbuch Datenschutzrecht, S. 593; Kußmann, Lexikon der Kommunikations- und Informationstechnik, S. 575.

Beim Einsatz digitaler Schlüssel hängt die Sicherheit maßgeblich von der Schlüssellänge ab. Die Schlüssellänge wird in Bit gemessen. Vom Grundsatz sind alle Schlüssel angreifbar. Die Zeit, die zum „Knacken“ von Schlüsseln erforderlich ist, hängt dabei zum einen von der Länge der Schlüssel ab, zum anderen von den technischen Möglichkeiten. Die rasante Entwicklung der Rechnerkapazitäten, sowie die zunehmende Vernetzung haben dazu geführt, dass als sicher angesehene Schlüssellängen nicht mehr ausreichen. Daher muss die Schlüssellänge ständig den technischen Entwicklungen angepasst werden.

Für einen bekannten Verschlüssellungsalgorithmus, den RSA– Algorithmus, der bei dem bekannten Programm Pretty Good Privacy zum Einsatz kommt, gilt heute eine verwendete Schlüssellänge von 1024 Bit als noch sicher[177]. Es ist aber nur eine Frage der Zeit, bis diese Schlüssellänge nicht mehr ausreichend ist. Die Sicherheit des Schlüssels kann daher nur nach dem aktuellen Stand der Technik und Wissenschaft beurteilt werden. Dabei hat sich der Verwender von Schlüsseln über geltende Standards und Empfehlungen im Bereich der Kryptographie sowie über wissenschaftliche Ergebnisse aus allgemein zugänglichen Quellen zu informieren.

Der beste Schlüssel ist aber wertlos, wenn nicht dafür gesorgt wird, dass er geheim bleibt. Damit sind organisatorisch-personelle Maßnahmen sowohl beim Absender als auch beim externen Empfänger angesprochen. Hierzu zählen Schutzvorkehrungen, wie der Einsatz von Firewalls, aber auch die Beschränkung des Kreises derjenigen, die den Schlüssel kennen, sowie die sichere Aufbewahrung des Schlüssels. Werden solche Sicherungsmaßnahmen unterlassen und ist dadurch die Verschlüsselung leicht rückgängig zu machen, kann nicht von einer wirksamen Aufhebung des Personenbezugs ausgegangen werden[178]. Zwar kann argumentiert werden, dass Maßnahmen der Sicherung des Schlüssels handlungsbezogen sind und damit besser zu dem Tatbestandsmerkmal des Offenbarens oder in den Bereich der Schuld einzuordnen sind. Eine solche Betrachtung verkennt aber die einheitliche Wirkung der Verschlüsselung und der sie sichernden Maßnahmen. Ist der Schlüssel leicht zu beschaffen, so ist die Verschlüsselung der Daten Makulatur und die bezweckte Geheimhaltung wird untergraben.

---

[177] Heibey, in: Rossnagel, Handbuch Datenschutzrecht, S. 594.
[178] Ähnlich im Datenschutzrecht, vgl. Bergmann/Möhrle/Herb, BDSG, § 3 Rn. 32.

Vorzugswürdig ist daher eine Verortung im Rahmen des Geheimnisbegriffs. Dabei ist dem personalen Charakter des § 203 StGB dadurch Rechnung zu tragen, dass nur dann ein Geheimnis entfällt, wenn auch beim externen Dienstleistungserbringer die Sicherung der Verschlüsselung gewährleistet ist. Denn zur Geheimhaltung sind die tauglichen Täter nach § 203 StGB verpflichtet. Setzen sie Verschlüsselungstechnologien ein, müssen sie sicherstellen, dass diese wirksam sind, bevor externe Dritte mit diesen Daten in Kontakt kommen. Kennen Dritte, die in Kontakt mit den verschlüsselten Daten kommen sollen, den Schlüssel, kann von Anfang an nicht eine Aufhebung des Personenbezugs angenommen werden. Ist auch den externen Dritten der Schlüssel unbekannt, hängt die Aufhebung des Personenbezugs davon ab, ob eine Entschlüsselung mit einfachen Mitteln möglich ist. Dies ist nur dann auszuschließen, wenn einerseits die verwendete Verschlüsselungstechnik nach aktuellem Stand als sicher einzustufen ist und andererseits organisatorisch-personelle Maßnahmen sicherstellen, dass die eingesetzte Verschlüsselungstechnik nicht unterlaufen wird.

Bezogen auf das Heranziehen externer Dienstleistungsunternehmen bedeutet dies, dass auch bei diesen Vorkehrungen getroffen sein müssen, um den Schlüssel vor einer Entdeckung zu sichern. Dies gilt zumindest dann, wenn der Geheimnisverpflichtete und der externe Dritte verbunden sind. Eine solche Verbindung besteht beispielsweise, wenn digitalisierte Daten durch ein Netz übertragen werden. Dies gilt unabhängig davon, wie die Verbindung physikalisch, beispielsweise über Kabel oder über Funk, realisiert wird. Ist der Geheimnisverpflichtete und das externe Dienstleistungsunternehmen verbunden, dann darf dies nicht zum Einfallstor für Angriffe auf den Schlüssel werden. Die Verbindung zum Geheimnisverpflichteten ist auch auf Seiten des Outsourcingnehmers nach dem aktuellen Stand der Technik zu schützen. Nur dann kann eine Aufhebung des Personenbezuges angenommen werden.

Die Einbeziehung auch des externen Dienstleistungserbringers, also des Outsourcingnehmers, hinsichtlich der zu treffenden Schutzvorkehrungen ist deshalb geboten, weil Verschlüsselung und Entschlüsselung spiegelbildlich sind und gleichermaßen unmittelbar an dem Dateninhalt ansetzen. Dieser Zusammenhang würde zerrissen werden, wenn man den Personenbezug unabhängig von den Maßnahmen des externen Dienstleistungserbringers bestimmt. Die physikalische Verbindung

ist auf rechtlicher Seite fortzuschreiben. Insofern kann von einer tatbestandlichen Verantwortungseinheit gesprochen werden. Sind also entweder beim Outsourcer oder beim Outsourcinganbieter keine oder nur ungenügende Sicherheitsmaßnahmen getroffen, liegen „Geheimnisse" i.S.v. § 203 StGB trotz Verschlüsselung vor. Eine Strafbarkeit würde nicht am fehlenden Tatbestandsmerkmal Geheimnis scheitern. Im Umkehrschluss gilt, dass bei Verschlüsselung der Daten und dem Stand der Technik entsprechender Sicherungsmaßnahmen eine Strafbarkeit bereits tatbestandlich ausscheidet.

Die Verschlüsselung im oben beschriebenen Sinn ist unter Beachtung des Standes der Technik und geeigneter Sicherungsvorkehrungen nach der hier vertretenen Ansicht eine Möglichkeit, den Personenbezug aufzuheben. Diese Möglichkeit der Vermeidung einer Strafbarkeit nach § 203 StGB hat aber auch Nachteile. Sie ist damit verbunden, dass zumindest auf der Seite des Outsourcinggebers die IT-Infrastruktur zum Ver- bzw. Entschlüsseln vorhanden sein muss. Dies kann unter Kostengesichtspunkten nachteilig sein, sofern es nicht allein auf zu übertragende Datenmengen ankommt[179]. Als Alternativen zum Verschlüsseln sind an einfachere Möglichkeiten einer „Anonymisierung" i.S.v. § 3 Abs. 6 BDSG zu denken. Vorgeschlagen werden beispielsweise für den Bereich der Versicherungswirtschaft die Trennung von Stamm- und Vertragsdaten von den Krankheitsdaten[180]. Bevor die Daten an externe Dienstleistungsanbieter weitergegeben werden, sollen nur Daten sichtbar bleiben, die es Dritten nicht möglich machen, mit verhältnismäßigem Aufwand die betroffene Person zu bestimmen. Dies könne beispielsweise angenommen werden, wenn nur die Postleitzahl, das Geburtsdatum sowie die Hausnummer sichtbar bleiben[181].

Diese Möglichkeit der Anonymisierung kann zu einem Aufheben des Personenbezugs führen. Es gelten aber die obigen Ausführungen zur Verschlüsselung. Auch hier muss sichergestellt sein, dass das erforderliche Zusatzwissen zur Reindividualisierung geheim bleibt. Dies muss durch organisatorisch-personelle Maßnahmen gewährleistet werden. Außerdem besteht bei bestimmten medizinischen Daten die Gefahr, dass diese aufgrund ihrer Eigen- und Einzigartigkeit leichter

[179] Ein Beispiel, in dem es auf die Datenmenge ankommt, beschreiben Braunschweig/ Geis/Tolksdorf/Hansen, MedR 2004, S. 353ff.
[180] Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 86.
[181] So Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 89ff.

einen Schluss auf die Person zulassen, also eine Anonymisierung nicht zuverlässig erfolgen kann[182]. Diese Gefahr würde nicht bestehen, wenn statt einer Anonymisierung eine Pseudonymisierung erfolgen würde.

Die Pseudonymisierung ist in § 3 Abs. 6a BDSG beschrieben. Das Gesetz versteht darunter „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren". Als Beispiel kann die Verwendung von Versicherungskennnummern genannt werden. Die Pseudonymisierung führt gegenüber dem Personenkreis, der das verwendete Kennzeichen kennt, nicht zu einer Aufhebung des Personenbezugs. Bezüglich Dritter, die das Kennzeichen nicht kennen, liegen nur dann keine personenbezogenen Daten vor, wenn der Schlüssel dem Dritten nicht bekannt ist und auch nicht mit einfachen Mitteln vom Kennzeichen auf die Person geschlossen werden kann[183]. Bezüglich sichernder organisatorisch-personeller Maßnahmen gelten die Ausführungen zur Verschlüsselung entsprechend.

V. Offenbaren

Gelingt es nicht den Personenbezug aufzuheben oder ist dies nicht beabsichtigt, ist bezüglich einer Strafbarkeit nach § 203 StGB zu untersuchen, wann ein „Offenbaren" i.S.v. § 203 StGB vorliegt.

1. Bedeutung der Figur der zum Wissen Berufenen

Ein Offenbaren setzt begrifflich voraus, dass ein Geheimnis nach außen zu Personen, die nicht für das Geheimnis bestimmt sind, dringt. Um ein Offenbaren feststellen zu können, muss die Sphäre derjenigen, die bestimmungsgemäß um das Geheimnis wissen dürfen, abgegrenzt werden von der Sphäre derjenigen, die nicht um das Geheimnis wissen dürfen. Anders ausgedrückt, muss der Innenbereich und der Außenbereich eines Geheimnisses bestimmt werden.

---

[182] Zu denken ist beispielsweise an seltene Syndrome oder an genetische Daten; zu letzteren und der Schwierigkeit der Anonymisierung vgl. Luttenberger et al., DuD 2004, S. 356 ff.
[183] Schaffland/Wiltfang, BDSG, § 3 Rn. 13.

Entsprechend dieser Überlegungen wird ein Offenbaren überwiegend definiert als jede Weitergabe eines zur Zeit der Tat noch bestehenden Geheimnisses und der Identität seines Trägers an Dritte, die dieses Geheimnis nicht, nicht in dem Umfang, nicht in dieser Form oder nicht sicher kennen und die nicht zu dem Kreis der zum Wissen Berufenen gehören[184].

Zum Teil wird in der Literatur vertreten, dass auch eine Weitergabe an Personen, die zum Kreis der zum Wissen Berufenen zu zählen sind, ein Offenbaren darstellt[185]. Begründet wird dies insbesondere damit, dass bei einer Erweiterung des Kreises der faktisch Mitwissenden immer eine Preisgabe des Geheimnisses erfolgt[186]. Die Begründung kann nicht überzeugen. Zwar mag der Wortlaut die Auffassung stützen, die Betrachtungsweise ist aber zu formal. Sie verkennt, dass Personen, die durch den Schweigepflichtigen eingeschaltet werden und die von den Geheimnissen erfahren, nicht notwendig auf gleicher Ebene neben dem Schweigepflichtigen stehen und getrennte Rechtskreise bilden. Bei einer solchen Annahme würde die Funktion der mitwissenden Personen nicht hinreichend berücksichtigt. Es besteht nämlich ein sachlicher Unterschied darin, ob die mitwissende Person unabhängig vom Schweigepflichtigen die erhaltenen Geheimnisse für eigene Aufgaben verwendet, oder ob die Geheimnisse zur Aufgabenerfüllung des Schweigepflichtigen geteilt werden. Ist letzteres der Fall, wird also eine Person unmittelbar in die Funktion des Schweigepflichtigen einbezogen, dann können die Rechtskreise verschiedener Personen für den Bereich gemeinsamer Aufgabenerfüllung verschmelzen[187].

Diese Auffassung wird gestützt, wenn man die Schweigepflicht nach § 203 Abs. 2 StGB betrachtet. § 203 Abs. 2 StGB regelt die Schweigepflicht im Behördenbereich. Hier vertraut der Geheimnisträger seine Geheimnisse grundsätzlich einer Behörde bzw. einer Stelle, nicht einer einzelnen Person, für bestimmte Aufgaben

---

[184] Tröndle/Fischer, StGB, § 203 Rn. 30b; Lackner/Kühl, StGB, § 203 Rn. 17f ; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 41; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 49; Niedermair, in: Roxin/Schroth, Medizinstrafrecht, S. 367; Gössel/Dölling, Strafrecht BT 1, S. 394f.; Ulsenheimer, Arztstrafrecht in der Praxis, S. 361.
[185] Jung, in: NK StGB, § 203 Rn. 19.
[186] Jung, in: NK StGB, § 203 Rn. 19; Meier, Der Schutz patientenbezogener Gesundheitsdaten im StGB, S. 157 f., der ein Offenbaren in diesem Fall bejaht, den Tatbestand aber wegen sozialadäquaten Verhaltens verneint.
[187] Im Ergebnis ebenso LG Bonn NJW 1995, S. 2420.

an[188]. Zutreffend wird daher von der h.M. angenommen, dass eine Weitergabe an funktional zuständige Bedienstete keine Offenbarung im Sinne von § 203 Abs. 2 StGB darstellt[189]. Diese Personen innerhalb von Funktionseinheiten sind dem Kreis der zum Wissen Berufenen zuzuordnen, innerhalb dessen ein Offenbaren zu verneinen ist. Dass eine funktionale Betrachtungsweise zutreffend ist, legt auch § 203 Abs. 2 S. 2 HS. 2 StGB nahe, der die Weitergabe von Einzelangaben an Behörden oder sonstige Stellen für Aufgaben der öffentlichen Verwaltung aus dem Anwendungsbereich des § 203 Abs. 2 S. 1 StGB ausschließt.

Es ist nicht einsichtig, dass bei § 203 Abs. 1 StGB diese Überlegung nicht zutreffend ist. Zwar wird es oft so sein, dass bei § 203 Abs. 1 StGB der Geheimnisträger einem einzelnen Berufsträger persönlich seine Geheimnisse anvertraut, allerdings ist das keinesfalls immer der Fall. Man wird nicht ernsthaft sagen können, dass bei § 203 Abs. 1 Nr. 6 StGB einzelnen Angehörigen privater Versicherungsunternehmen besonderes Vertrauen, vergleichbar einem behandelnden Arzt, entgegen gebracht wird. Vielmehr wird das Vertrauen dem Unternehmen entgegengebracht. Hier kann eine Weitergabe von Geheimnissen an funktional zuständige Mitarbeiter nicht anders beurteilt werden als im Behördenverkehr, denn in beiden Fällen stehen dem Geheimnisträger größere institutionelle Einheiten gegenüber, bei denen zwangsläufig unterschiedliche Personen mit den Geheimnissen des Anvertrauenden in Berührung kommen. Um Wertungswidersprüche zu vermeiden, bedarf es neben § 203 Abs. 3 StGB und § 203 Abs. 2 S. 2 HS 2 StGB der allgemeinen Figur der zum Wissen Berufenen, innerhalb derer eine Geheimnisweitergabe kein „Offenbaren“ i.S.v. § 203 StGB darstellt. Über die Figur wird zum Ausdruck gebracht, dass jeweils eine Abgrenzung des Innenbereichs des Geheimnisses vom Außenbereich zu erfolgen hat. Dieser Grundgedanke ist sowohl für § 203 Abs. 1 i.V.m. Abs. 3 StGB als auch für § 203 Abs. 2 StGB richtig. An der Figur der zum Wissen Berufenen ist festzuhalten.

---

[188] Vogel, Zum strafrechtlichen Schutz des Sozialgeheimnisses, S. 38.

[189] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 44; Schmidt, Ärztliche Schweigepflicht und Datenschutz, S. 35f.; OLG Frankfurt, NStZ-RR 1997, S. 69; OLG Frankfurt NStZ-RR 2003, S. 170; anders noch Kreuzer, NJW 1975, S. 2236 hinsichtlich der Weitergabe an eine Aufsichtsbehörde; Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 487; vgl. auch Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 98, der zutreffend darauf hinweist, dass dann, wenn einen nach § 203 Abs. 2 StGB Schweigepflichtigen zusätzlich eine Schweigepflicht nach § 203 Abs. 1 StGB trifft, innerbehördliche Schweigepflichten entstehen können. In der Tat kann es unter dem Gesichtspunkt des Rechtsgutschutzes nicht überzeugen, dass der Umstand, der die Schweigepflicht nach § 203 Abs. 1 StGB begründet, wegen einer gleichzeitigen Amtsträgereigenschaft unberücksichtigt bleibt und damit insgesamt ein geringerer Rechtsgutschutz besteht.

2. Abgrenzung des Kreises der zum Wissen Berufenen

Wer zum Kreis der zum Wissen Berufenen gehört, richtet sich zunächst grundsätzlich nach dem ausdrücklichen Willen des Berechtigten. Ist ein solcher Wille nicht geäußert, kann auf den mutmaßlichen Willen, gefolgert aus dem objektiven Interesse, abgestellt werden. Damit ist für die Bestimmung des Kreises der zum Wissen Berufenen die Sicht des Berechtigten maßgeblich. Dies ist richtig, da er die Verfügungsbefugnis über seine Geheimnisse hat und grundsätzlich selbstbestimmt entscheiden können muss, wem und im welchem Umfang er die Geheimnisse anvertraut. Damit bestimmt zunächst der Berechtigte, welcher Person er unmittelbar ein Geheimnis anvertraut.

Der Kreis der zum Wissen Berufenen ist aber nicht allein subjektiv zu bestimmen. Der Geheimnisverpflichtete kann und muss bestimmte Aufgaben innerhalb der konkreten Vertrauensbeziehung nicht allein bewältigen[190]. Bezüglich der in § 203 Abs. 1 StGB genannten Täter erstreckt § 203 Abs. 3 S. 2 StGB die Schweigepflicht auf die berufsmäßig tätigen Gehilfen und die Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Letztere Personengruppe, die beispielsweise Referendare, Famuli oder Lehrlinge erfasst, ist für Outsourcingprojekte praktisch irrelevant. Bedeutsam ist der Gehilfenstatus nach § 203 Abs. 1 S. 1 StGB.

3. Der Gehilfe im Kreis der zum Wissen Berufenen

Werden solche Gehilfen eingesetzt und haben sie Zugang zu den Geheimnissen des Betroffenen, dann bedeutet dies keine Verletzung des § 203 StGB sowie des Rechts auf informationelle Selbstbestimmung, da es für den Betroffenen vorhersehbar ist, dass in dem Vertrauensverhältnis zu dem Schweigepflichtigen bestimmte Personen die Funktionen des Schweigepflichtigen unterstützen. Dies gilt unabhängig davon, ob die Konstruktion einer mutmaßlichen Einwilligung zur Begründung herangezogen wird oder eine Interessenabwägung zwischen dem geschützten Recht auf informationelle Selbstbestimmung und dem verfolgten Zweck der Aufgabenerfüllung vor dem Hintergrund der Berufsfreiheit erfolgt. Entscheidend ist, dass nur dann keine Verletzung des Rechts auf informationelle

[190] Für den Bereich des § 203 Abs. 2 StGB vgl. ausführlich Vogel, Zum strafrechtlichen Schutz des Sozialgeheimnisses, S. 36ff.

Selbstbestimmung vorliegt, wenn objektiv und nicht aus Sicht des Schweigepflichtigen, die Personen, die eingesetzt werden, unmittelbar die beruflich Funktion unterstützen.

Allein eine gemeinsame Schweigepflicht ist jedenfalls für die Frage des Offenbarens nach zutreffender h.M. unerheblich[191]. Denn aus Sicht des Geheimnisträgers kann gerade in der Weitergabe an einen anderen Schweigepflichtigen ein Eingriff in sein Recht auf informationelle Selbstbestimmung liegen[192]. Welchem Schweigepflichtigen der Geheimnisträger vertraut und deshalb sein Geheimnis anvertraut, muss grundsätzlich der individuellen, selbstbestimmten Entscheidung des Berechtigten überlassen sein. Hinnehmen muss der Berechtigte nur, dass der Innenbereich des Geheimnisverpflichteten sich nach Funktionseinheiten richtet.

Dies folgt daraus, dass durch § 203 StGB neben Individualinteressen auch Allgemeininteressen geschützt sind, zu denen die Funktionstüchtigkeit der Berufe zählt. Für den Bereich des § 203 Abs. 1 StGB spielt zudem die Berufsfreiheit aus Art. 12 GG herein, die als einheitliches Grundrecht auch die Berufsausübung schützt. Für den Bereich des § 203 Abs. 2 StGB ist die Organisationshoheit der Verwaltung zu beachten. Dem Individualschutzinteresse ist hinreichend genüge getan, wenn der Betroffene absehen kann, dass sein Geheimnis nur dem Schweigepflichtigen und den ihn objektiv in seiner Funktion unmittelbar unterstützenden Personen zugänglich ist[193]. Ist dies der Fall, dann ist konsequenterweise eine Strafbarkeit nach § 203 StGB zu verneinen, unabhängig von der Tatsache, dass die Personen, die unmittelbar unterstützend tätig werden, selbst schweigepflichtig sind. Stehen die Personen außerhalb von Funktionseinheiten, dann sind sie im Umkehrschluss, auch wenn sie selbst schweigepflichtig sind, nicht dem Kreis der zum Wissen Berufenen zuzurechnen[194]. Ein weitergehender Schutz ist angesichts der Berufsfreiheit bzw. der Organisationshoheit der Verwaltung nicht erforderlich.

---

[191] Vgl. bereits Fußnoten 139 und 140 sowie ausdrücklich beim Offenbaren einordnend Ulsenheimer, Arztstrafrecht in der Praxis, S. 361.
[192] Vgl. Niedermair, in: Roxin/Schroth, Medizinstrafrecht, S. 368.
[193] Für den Bereich der berufsmäßigen Gehilfen ebenso Tröndle/Fischer, StGB, § 203 Rn. 21.
[194] Die Tathandlung des Offenbarens wird auch in der Rechtsprechung nach Funktionseinheiten bestimmt, vgl. für den Bereich des § 203 Abs. 2 StGB OLG Frankfurt, NStZ-RR 1997, S. 69; OLG Frankfurt NStZ-RR 2003, S. 170.

Dies wird in der Rechtsprechung und der Literatur weitgehend ebenso beurteilt[195]. Allerdings bestehen Unterschiede in der Begründung. Ein Teil der Rechtsprechung und der überwiegende Teil der Literatur vertreten, dass kein Offenbaren im Sinne des § 203 StGB vorliegt[196]. Eine Strafbarkeit scheidet nach dieser Auffassung bereits auf Tatbestandsebene aus. Demgegenüber wird von einem Teil der Literatur und Rechtssprechung vertreten, dass es an einem unbefugten Offenbaren fehlt[197]. Abhängig von der Einordnung des Merkmals unbefugt[198] auf Tatbestandsebene, auf Rechtswidrigkeitsebene, so die h.M.[199], oder auf beiden Ebenen[200], scheitert eine Strafbarkeit ebenfalls auf Tatbestandsseite oder ist jedenfalls gerechtfertigt. Die Lösung dieses Problems kann praktisch für eine Beurteilung der Strafbarkeit bei Irrtumsfällen und im Teilnahmebereich bedeutsam sein[201].

Für die Lösung auf der Rechtswidrigkeitsebene kann angeführt werden, dass im Weitergeben der Information innerhalb von Funktionseinheiten unabhängig einer Einwilligung des Patienten immer ein Interessensverlust enthalten ist[202]. Denkbar ist es, zu argumentieren, dass in jedem Weitergeben der Information durch den unmittelbar Geheimnisverpflichteten der Bereich des Vertrauensverhältnisses verlassen wird. Im Hinblick auf Art. 1 Abs. 1 und 2 Abs. 1 GG ist dann in der Weitergabe der Information ein Eingriff in das Recht auf informationelle Selbstbestimmung anzunehmen. Erst auf der Ebene der Rechtfertigung ist dann zu fragen, ob dieser Eingriff auf Grundlage gesetzlicher Schranken gerechtfertigt ist. Diese Schranken müssen Befugnisse für einen Grundrechtseingriff darstellen und sind ihrerseits an der Verfassung zu messen, die den Gebrauch dieser Befugnisse be-

---

[195] BGH NJW 1995, S. 2915; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 41; Niedermair, in: Roxin/Schroth, Medizinstrafrecht, S. 367.
[196] Tröndle/Fischer, StGB, § 203 Rn. 30b; OLG Frankfurt NStZ-RR, 1997, S. 69; OLG Frankfurt NStZ-RR 2003, S. 170 f.
[197] Vgl. Niedermair, in: Roxin/Schroth, Medizinstrafrecht S. 368.
[198] Umfassend zum Merkmal „unbefugt" Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, S. 3ff.
[199] Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 493; Tröndle/Fischer, StGB, § 203 Rn. 31.
[200] Sog. Doppelfunktionalität, vgl. BVerfG NJW 1981, S. 329; Lenckner, in: Schönke/Schröder, StGB, § 203 Rn. 21.
[201] Es geht hierbei insbesondere um die Abgrenzung von Tatbestandsirrtum, Erlaubnistatbestandsirrtum und Verbotsirrtum sowie um Fragen der Strafbarkeit wegen Anstiftung zu einer Straftat nach § 203 StGB, vgl. Klöcker/Meister, Datenschutz im Krankenhaus, S. 38f; Ulsenheimer, in: Laufs/Uhlenbruck, Handbuch des Arztrechts, § 145 Rn. 4 ff.; ausführlich Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, S. 9ff.; die Frage wird dadurch verkompliziert, dass das Problem des unbefugten Offenbarens verbunden wird mit dem Problem, ob eine Einwilligung rechtfertigend oder tatbestandsausschließend wirkt, vgl. LG Bonn NJW 1995, S. 2916; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 54.
[202] Lackner/Kühl, StGB, vor § 201 Rn. 2.

grenzt. Insbesondere müssen sie dem Verfassungsgebot der Verhältnismäßigkeit genügen[203]. Schließlich muss auch der Eingriff selbst auf der Grundlage der Befugnisse verhältnismäßig sein, was notwendig eine Interessenabwägung voraussetzt.

Konsequenterweise müsste eine solche Auffassung eine Zustimmung durch den Betroffenen im Straftatbestand des § 203 StGB als rechtfertigende Einwilligung und nicht als tatbestandsausschließendes Einverständnis begreifen[204]. Auf Ebene der Rechtswidrigkeit ist eine Interessenberücksichtigung, so insbesondere bei der mutmaßlichen Einwilligung, besser einzuordnen als auf der Tatbestandsebene[205]. Argumentiert werden kann schließlich, dass eine Ansiedlung des Problems auf Tatbestandsebene zu Strafbarkeitslücken im Bereich der Teilnahme führen kann.

Sieht man in dem geschützten Rechtsgut entgegen der hier vertretenen Meinung vorwiegend oder allein Allgemeininteressen, kann dies zusätzlich als Argument für einen Interessens- bzw. Sozialkonflikt herangezogen werden, der bei einer Weitergabe von Geheimnissen auch innerhalb von Funktionseinheiten entsteht und allenfalls gerechtfertigt sein kann.

Die Berücksichtigung einer Weitergabe von geheimen Informationen innerhalb von Funktionseinheiten auf der Ebene der Rechtswidrigkeit überzeugt letztlich nicht. Zunächst ist ein Hinweis auf das Grundrecht auf informationelle Selbstbestimmung nicht treffend. Der Schutzbereich des Art. 1 Abs. 1, Art. 2 Abs. 2 GG ist funktionell nicht auf die Weitergabe von Geheimnissen an die unmittelbar den Schweigepflichtigen unterstützenden Personen auszuweiten. Die Interessen des Geheimnisträgers erfordern eine solche Ausdehnung richtigerweise nicht. Der Geheimnisträger wird hinreichend dadurch geschützt, dass sich Funktionseinheiten objektiv aus der Sicht des Betroffenen bestimmen und nicht aus der Sicht des

---

[203] So genannte Schranken-Schranken, vgl. zum Begriff Jarass/Pieroth, GG, Vorb. v. Art. 1 GG Rn. 44.

[204] Lackner/Kühl, StGB, Vor § 201 Rn. 2.

[205] Die Trennung zwischen dem tatbestandlichen Einverständnis und rechtfertigender Einwilligung mit jeweils unterschiedlichen Voraussetzungen wird in Frage gestellt, vgl. Rönnau in: Leipziger Kommentar StGB, Vor § 32 Rn. 148; Eser, in: Schönke/Schröder, StGB, Vorb. §§ 211 Rn. 28; vertreten wird, dass die Einwilligung tatbestandsausschließend wirkt, aber an weitergehende Voraussetzungen als ein tatbestandsausschließendes Einverständnis geknüpft ist; vgl. auch Roxin, Strafrecht AT 1, § 13 Rn. 2ff.; zum Teil wird bei § 203 StGB auch von einer konkludenten bzw. stillschweigenden rechtfertigenden Einwilligung und daneben von einem tatbestandsausschließenden ausdrücklichen Einverständnis gesprochen, vgl. Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, S. 56.

Geheimnisverpflichteten. Dass der Geheimnisverpflichtete sich anderer Personen zur Erfüllung seiner Aufgaben bedient, ist eine dem Willen des Betroffenen entzogene Erscheinung in einer arbeitsteiligen Welt. Damit muss und kann jeder Betroffene rechnen. Damit wird nicht die prinzipielle Verfügungsbefugnis des Einzelnen beschnitten. Die Organisation der Aufgabenerfüllung des Geheimnisverpflichteten ist dem Willen des Geheimnisträgers entzogen. Ein Eingriff durch eine Weitergabe von Geheimnissen an solche Personen, die zum Kreis der zum Wissen Berufenen gehören, ist somit abzulehnen.

Auch ein Abstellen auf das Rechtsgut des Allgemeininteresses vermag nicht zu überzeugen. Sieht man entgegen der hier vertretenen Auffassung bei § 203 StGB Allgemeininteressen als allein oder vorwiegend geschützt an, entfällt ein Interessenskonflikt, wenn der Betroffene von vornherein damit rechnen kann, dass „seine“ Geheimnisse innerhalb von Funktionseinheiten weitergegeben werden. Dies spricht ebenfalls für eine Berücksichtigung auf Tatbestandsebene. Sofern man annimmt, dass der Sozialkonflikt aufgrund einer ausdrücklichen oder mutmaßlichen Einwilligung entfällt, kann dies konstruktiv dadurch erklärt werden, dass die Einwilligung bei § 203 StGB tatbestandsausschließend wirkt[206]. Überzeugender ist es allerdings, das Problem von der Frage des Willens zu trennen und anzunehmen, dass innerhalb von Funktionseinheiten erst gar kein Interessenskonflikt entsteht und es somit an einem Offenbaren fehlt[207].

Hinzu kommt noch folgende Überlegung: Regelungen außerhalb des Strafrechts, beispielsweise berufsrechtliche Regelungen[208], können durchaus abweichend von Funktionseinheiten die Weitergabe untersagen oder ermöglichen[209]. Sie können damit abweichend vom Strafrecht einen Präventions- und Lenkungsgesichtspunkt in den Vordergrund stellen. Zum Strafrecht als ultima ratio passt dieser Gedanke nur beschränkt. Zwar mag § 203 StGB generalpräventiv wirken, dennoch darf, vor dem primären Schutzzweck des § 203 StGB, nicht über Gefährdungsgesichtspunkte eine teleologische Auslegung im Sinne einer Erweiterung des Tatbestan-

---

[206] Dies wird dann auch bei § 203 StGB überwiegend so gesehen, vgl. Lenckner, in: Schönke/Schröder, StGB, § 203 Rn. 22.
[207] Ulsenheimer, in: Laufs/Uhlenbruck, Handbuch des Arztrechts, § 70 Rn. 9; Langkeit, NStZ 1994, S. 7; ähnlich auch Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 486.
[208] Zur ärztlichen Schweigepflicht vgl. § 9 MBOÄ; vgl. auch Meier, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, S. 75.
[209] Vgl. § 49b BRAO.

des erfolgen. Anders als das Berufsrecht oder Bereiche des Sicherheits- und Ordnungsrechts ist das Strafrecht nicht der Ort für eine Lenkungsfunktion. Solche Überlegungen dürfen dann auch nicht maßgeblich für die Interpretation des § 203 StGB sein.

Insgesamt ist es demnach vorzugswürdig, den Tatbestand zu verneinen. Festzuhalten ist, dass eine Strafbarkeit ausscheidet, wenn objektiv ein Gehilfenstatus anzunehmen ist, die Person also dem Innenbereich einer Funktionseinheit zuzuordnen ist. Davon abgesehen ist weiterhin eine Strafbarkeit ausgeschlossen, wenn Personen unabhängig ihres Gehilfenstatus der Funktionseinheit des Schweigepflichtigen und damit dem Kreis der zum Wissen Berufenen zugerechnet werden können[210].

4. Integration in den Kreis der zum Wissen Berufenen

Werden beim Outsourcing medizinischer Daten private IT-Dienstleistungsunternehmen herangezogen, scheidet eine Funktionseinheit außerhalb des Gehilfenstatus aus. Denn es bestehen zwei selbständige Zuordnungseinheiten, Outsourcer und IT-Dienstleistungsunternehmen, die auch getrennt in Erscheinung treten. Es existiert also nicht eine nach außen in Erscheinung tretende Einrichtung, innerhalb derer mehrere Funktionseinheiten bestehen. Daher stellt sich im Hinblick auf die strafrechtliche Beurteilung des Outsourcings von medizinischen Daten die Frage, ob über eine Einbindung von Mitarbeitern des privaten externen IT-Dienstleistungsunternehmens eine Funktionseinheit mit dem schweigepflichtigen Outsourcer gebildet werden kann und somit Personen dem Innenbereich und nicht externen Dritten zuzuordnen sind. Dies wäre dann der Fall, wenn man sie als Gehilfen i.S. des § 203 Abs. 3 S. 2 Var. 1 StGB einordnen kann. Um dies beurteilen zu können, muss auf die näheren Voraussetzungen des Gehilfenstatus eingegangen werden.

[210] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 41; der Gesetzgeber hat durch Gesetz vom 22.06.06 Datenschutzbeauftragte in den Kreis möglicher Täter einbezogen. § 203 Abs. 2a geht davon aus, dass dem Datenschutzbeauftragten (auch dem externen Datenschutzbeauftragten) Geheimnisse anvertraut werden können, ohne dass ein unbefugtes Offenbaren vorliegt. Hier ist also gesetzlich ein zum Wissen Berufener bestimmt worden.

a) Gehilfe im Sinne des § 203 Abs. 3 StGB

Voraussetzung für die Annahme eines Gehilfenstatus ist, dass der Schweigepflichtige in seiner Funktion nach § 203 StGB unmittelbar unterstützt wird[211]. Die Qualifikation des Tätigwerdenden ist dabei richtigerweise nicht maßgeblich. Erfasst werden nicht nur einfache Hilfstätigkeiten[212]. Man könnte einwenden, dass bei hoher Qualifikation des Gehilfen eine Kontrolle des Gehilfen kaum denkbar ist. Dies überzeugt nicht. Allenfalls fachliche Weisungen mögen praktisch schwer vorstellbar sein. Es ist aber auch nicht notwendig, dass der Schweigepflichtige in jedem fachlichen Detail eingreifen kann, solange er den Ablauf und die Art und Weise der Gehilfentätigkeit insgesamt über Weisungen und Vereinbarungen steuert. Außerhalb des rein fachlichen Bereiches sind Weisungen sehr wohl denkbar und notwendig. Ein Gehilfe i.S.v. § 203 StGB kann somit auch jemand sein, der hochqualifizierte Tätigkeiten erbringt. Insofern ist der Begriff Gehilfe nicht mit dem allgemeinen Sprachgebrauch zu erklären.

Dies muss auch deshalb angenommen werden, weil es bezüglich des Rechtsgüterschutzes keinen Unterschied machen kann, welcher Art die Tätigkeit ist. Es ist schlecht vorstellbar, dass die Individualinteressen allein dadurch unterschiedlich beeinträchtigt werden, dass die unterstützende Tätigkeit eine ähnliche Qualifikation wie die des Schweigepflichtigen verlangt. Zudem würde eine Beschränkung auf einfache Tätigkeiten an den Anforderungen einer modernen, technisierten Arbeitswelt vorbeigehen. Vielmehr ist für die Annahme einer unterstützenden Gehilfentätigkeit maßgeblich darauf abzustellen, dass der Betroffene in den Bereich der spezifischen, vertrauensbegründenden Tätigkeit des Schweigepflichtigen erkennbar eingebunden ist[213]. Maßgeblich ist dabei nicht eine intern gebildete Organisationseinheit, sondern das Entstehen einer Funktionseinheit[214]. Erforder-

---

[211] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 77; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 114; Tröndle/Fischer, StGB, § 203 Rn. 21; zu den unterschiedlichen, sachlich sich kaum unterscheidenden Formulierungen vgl. Sieber, in: Handbuch Multimedia Recht, Teil 19 Rn. 488.

[212] Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 118; Klöcker/Meister, Datenschutz im Krankenhaus, S. 36; OLG Oldenburg NStZ 83, S. 39, das auch die Verwaltungsleitung als Gehilfen ansieht.

[213] Tröndle/Fischer, StGB, § 203 Rn. 21; Lenckner, in: Schönke/Schröder, StGB, § 203 Rn. 64; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 77, der darauf hinweist, dass der Herangezogene nicht lediglich organisatorisch „eingebaut“ werden kann.

[214] Anders bei der Bestimmung des Dritten im Datenschutzrecht, vgl. Gola/Schomerus, BDSG, § 3 Rn. 51f. und § 2 Rn. 6ff.

lich ist, dass die unterstützende Person in das spezifische Vertrauensverhältnis integriert wird und damit dem Kreis der zum Wissen Berufenen zuzurechnen ist.

Nicht weiterführend ist die Unterscheidung nach Haupt- oder Nebenaufgabe. Denn nach dem Dargelegten kann jemand als Gehilfe eingebunden werden, der in seiner Hauptfunktion nichts mit dem Schweigepflichtigen gemein hat. So kann im Einzelfall beispielsweise auch ein herangezogener selbständiger Detektiv[215] im Verhältnis zum Rechtsanwalt oder ein selbständiger Zahntechniker im Verhältnis zum Zahnarzt[216] Berufshelfer sein, soweit eine hinreichende Einbindung erfolgt. Der Helfer muss dann nicht notwendig solche Aufgaben erledigen, die als spezifische Hauptaufgaben des Schweigepflichtigen bezeichnet werden können, also beispielsweise bei einem Arzt die Behandlung und Untersuchung des Patienten. Ausreichend ist auch das Erledigen von Nebenaufgaben, zu denen der Schweigepflichtige verpflichtet ist, beispielsweise das Ausstellen von Rechnungen oder das Verarbeiten von Daten. Zu fordern ist aber, dass die Aufgaben unmittelbar der Berufsausübung dienen und hinreichend eingebunden in die Vertrauensbeziehung zwischen Schweigepflichtigen und Geheimnisträger erfolgen. Wird also die Reinigungskraft unter Anleitung durch den schweigepflichtigen Arzt zum Sortieren von Rechnungen eingesetzt, kann sie im Einzelfall Gehilfenstatus haben. Gleiches muss für Personen gelten, die der Schweigepflichtige im Rahmen eines Outsourcingvorhabens zur Datenverarbeitung von medizinischen Daten, die aus dem spezifischen Vertrauensverhältnis zwischen Schweigepflichtigen und Geheimnisträger stammen, einsetzt.

Ob für eine solche Bindung an die spezifische Funktion des Schweigepflichtigen ein Weisungsrecht zwingend erforderlich ist, ist umstritten[217]. Regelmäßig wird man ein Weisungsrecht verlangen müssen[218], denn ohne ein solches Weisungsrecht wäre eine Zuordnung zu einer Funktionseinheit bzw. zum Geheimnisverpflichteten willkürlich und unbeständig. Hinzu kommt, dass insbesondere bei dem Heranziehen von Personen, die nicht eine ähnliche Funktion wie die des Hauptberufsträgers ausüben, das Weisungsrecht erst einen unmittelbaren Zusammenhang

[215] LG Frankfurt NJW 1959, S. 589; a.A. Neubeck, in: KMR StPO, § 53a Rn. 3.
[216] LBerufsG für Zahnärzte Stuttgart NJW 1975, S. 2255; a.A. Neubeck, in: KMR StPO, § 53a Rn. 3.
[217] Taupitz, MedR 1993, S. 374.
[218] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 77; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 115; Ehmann, CR 91, S. 295.

mit der Tätigkeit des Hauptberufsträgers herstellt. Eine Zuordnung ohne ein tatsächliches Weisungsrecht wäre vor dem Hintergrund des geschützten Rechtsgutes nicht hinnehmbar und würde das Geheimnis vollkommen von der Person des Schweigepflichtigen abkoppeln. Dies entspricht nicht dem Willen des Gesetzgebers, der über die Einschränkung in § 203 Abs. 1 StGB aufgrund der enumerativen Aufzählung von Schweigepflichtigen auch der Person des Schweigepflichtigen Bedeutung zumessen wollte.

Ein Weisungsrecht ist aber zutreffend dann entbehrlich, wenn sich die Zuordnung zu einer Funktionseinheit schon erkennbar aus anderen Umständen ergibt. Wird beispielsweise innerhalb eines Krankenhauses ein weiterer Arzt in die Behandlung eingeschaltet, ergibt sich schon aus der Zugehörigkeit zu derselben Organisation eine eindeutige Zuordnung, so dass es nicht auf ein vereinbartes oder tatsächliches Weisungsrecht ankommt. Der Patient kann mit solch einer Einschaltung von Personen aus einem von vornherein abgegrenzten Bereich rechnen. Werden aber Personen außerhalb eines solchen Bereichs herangezogen, wie dies beim Outsourcing der Fall ist, dann kann auf ein tatsächliches Weisungsrecht als weiteres notwendiges Kriterium für eine eindeutige Zuordnung nicht verzichtet werden[219].

Schließlich ist Voraussetzung für die Annahme eines berufsmäßig tätigen Gehilfen, dass er die Funktion des Schweigepflichtigen unmittelbar unterstützt[220]. Zum Teil wird dafür verlangt, dass der Unterstützende die Tätigkeit als Hauptberuf bzw. als Nebenberuf ausübt und nicht nur gelegentlich tätig wird[221]. Gefolgert wird dies aus dem Zusatz „berufsmäßig“. Berufsmäßig könne nur der handeln, der die Tätigkeit beruflich ausübt. Auch kann ein Vergleich mit § 53a StPO herangezogen werden, in dem der Zusatz berufsmäßig fehlt.

Dieser Auffassung ist nicht zu folgen. Sie ist weder zwingend durch den Wortlaut, noch durch den Sinn und Zweck des § 203 StGB geboten[222]. In der Beziehung des

[219] Zutreffend Taupitz, MedR 1993, S. 375.
[220] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 77.
[221] So Lackner/Kühl, StGB, § 203 Rn. 11b; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 116, mit dem Hinweis auf den Wortlaut; auch Senge, in: Karlsruher Kommentar StPO, § 53a Rn. 2; vgl. auch Köpke, Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für Private Krankenversicherer, S. 230f.
[222] Im Ergebnis ebenso Bartsch, Ärztliche Schweigepflicht und Zeugnisverweigerungsrecht im Strafprozess, S. 29f.

Geheimnisträgers zum Geheimnisverpflichteten darf der Geheimnisträger darauf vertrauen, dass seine Geheimnisse geschützt bleiben. Nur solche Personen können in diese Vertrauensbeziehung eingebunden sein, die im unmittelbaren Zusammenhang mit der Aufgabenerfüllung des Schweigepflichtigen innerhalb der in § 203 StGB genannten Funktion stehen. In diesem Sinne ist der Zusatz berufsmäßig zu verstehen. Ein solches Verständnis ist auch vom Wortlaut noch gedeckt, da unter berufsmäßig auch der Zusammenhang mit einem Beruf verstanden werden kann.

Ein solcher Zusammenhang ist nicht davon abhängig, ob die unterstützende Tätigkeit als ein typischer Hilfsberuf zu den in § 203 Abs. 1 StGB genannten Hauptberufen bezeichnet werden kann[223]. Ein Abstellen auf typische Hilfsberufe wäre angesichts der Inhomogenität der aufgeführten Berufsgruppen in § 203 Abs. 1 StGB wenig hilfreich und dürfte kaum dem gesetzgeberischen Zweck entsprechen. Können solche Berufe bei § 203 Abs. 1 Nr. 1 StGB noch verhältnismäßig leicht qualifiziert werden, ist dies bei § 203 Abs. 1 Nr. 6 StGB kaum zu leisten. Hinzu kommt, dass technische und gesellschaftliche Veränderungen auch auf die Art der Berufsausübung durchschlagen, mitunter neue Tätigkeitsfelder entstehen[224]. Es überzeugt vor dem Hintergrund des Art. 12 GG nicht, Personen aus solchen neuen Tätigkeitsfeldern aus dem Gehilfenstatus auszuklammern, allein weil sie nicht einem typischen Hilfsberuf zugeordnet werden können[225]. Maßgeblich muss vielmehr sein, ob die Tätigkeit im Zusammenhang mit der Berufsausübung des Schweigepflichtigen tatsächlich so erfolgt, dass sie den Schweigepflichtigen unmittelbar in seiner Funktion unterstützt.

Ist der unmittelbare Zusammenhang gegeben, ist es unerheblich, ob die Personen die Tätigkeit nur gelegentlich oder als Haupt- bzw. Nebenberuf ausüben, sofern sie nur weisungsgebunden in das Vertrauensverhältnis eingebunden sind. Damit wird auch Kongruenz zum Strafprozessrecht erzielt, da § 53a StPO nach im Vordringen befindlicher Auffassung derart eingebundene Personen ebenfalls als Gehilfen erfasst und über § 97 Abs. 4 StPO Beschlagnahmefreiheit für Gegenstände,

[223] Vgl. zum Begriff der „ Heilhilfsberufe“ Schnitzler, Das Recht der Heilberufe, S. 36 f.
[224] Insbesondere die Entwicklungen im Informations- und Kommunikationsbereich haben zu solchen neuen Tätigkeitsfeldern geführt, aus denen sich zum Teil in der Rechtswirklichkeit neue Berufsbezeichnungen herausgebildet haben.
[225] Anders wohl die h.M., vgl. Tröndle/Fischer, StGB, § 203 Rn. 21.

die im Gewahrsam der Gehilfen sind, gewährleistet[226]. Werden hingegen Aufgaben von gleichgeordneten Personen selbstständig erfüllt, sind diese als externe Dritte und nicht als Gehilfen zu bezeichnen[227].

Fraglich ist, ob bezüglich der erforderlichen Weisungsgebundenheit die Begründung eines wirksamen Arbeitsverhältnisses erforderlich ist. In der Literatur wird das Erfordernis eines Arbeitsvertrages überwiegend verneint[228]. So werden auch ehrenamtlich Tätige als Gehilfen angesehen. Selbst Personen, die rein faktisch Weisungen befolgen, können Gehilfenstatus haben.

Für die Beurteilung, ob Outsourcingnehmer als externe Dienstleistungsunternehmer Gehilfenstatus haben können, ist diese Frage mit von entscheidender Bedeutung. Denn die das Outsourcing anbietenden Dienstleistungsunternehmen sind oft selbständig tätige, rechtlich vom Outsourcer getrennte Unternehmen, die für mehrere Outsourcer tätig werden können. Werden Personen des Outsourcingnehmers für den Outsourcer aufgrund vertraglicher Abrede tätig, bedeutet dies, dass nicht eigenes Personal, sondern fremdes Personal, das keinen Arbeitsvertrag mit dem Outsourcinggeber hat, tätig wird.

Nach der oben dargestellten Auffassung ist ein fehlendes Arbeitsverhältnis kein Hinderungsgrund. Allerdings wird stark auf Einzelfälle abgestellt, ohne dass eine nähere Begründung in einem größeren Zusammenhang erfolgt. Insofern bedarf dieser Aspekt einer näheren Untersuchung. Für das Erfordernis eines Arbeitsvertrages spricht zunächst, dass typischerweise mit einem Arbeitsvertrag über das Direktionsrecht eine starke Eingliederung in das Unternehmen erfolgt. Die Bindung an das Unternehmen zeigt sich auch darin, dass durch das Arbeitsverhältnis Fürsorge- und Treuepflichten begründet werden[229].

Vertreten werden könnte, dass erst durch eine solche Sonderbeziehung für den Außenstehenden ersichtlich eine Funktionseinheit gebildet wird. Andernfalls wird der Bereich der Funktionseinheit konturenlos. Der außen stehende Geheimnisträ-

---

[226] Fritzemeyer, in Söbbing: IT-Outsourcing, S. 755.
[227] Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 114; Neubeck, in: KMR StPO, § 53a Rn. 2ff.
[228] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 77; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 115.
[229] Vgl. nur Palandt, BGB, § 611 Rn. 96 zur Fürsorgepflicht und Rn. 39 zur Treuepflicht.

ger vertraut nicht darauf, dass in die Vertrauensbeziehung Personen eingeschaltet werden, die in keinem Arbeitsverhältnis zum Schweigepflichtigen stehen. Auch der personale Charakter des § 203 StGB spricht für eine Berücksichtigung eines Arbeitsverhältnisses als notwendige Voraussetzung einer Gehilfenstellung. Argumentiert werden kann, dass bei Aufgabe dieses Erfordernisses, zumindest im Bereich des § 203 Abs. 1 StGB, dem personalen Charakter nicht genügt wird. Insbesondere wenn die Beteiligten mehrschichtige, korporativ verfasste Institutionen sind, könnte eine Zuordnung für den Geheimnisträger nicht ersichtlich sein.

Dies wäre beispielsweise anzunehmen, wenn private Kranken-, Lebens- oder Versicherungsunternehmen in der Rechtsform einer GmbH oder AG, aber auch Krankenhäuser oder neuerdings medizinische Versorgungszentren in der zuvor erwähnten Rechtsform, medizinische Daten outsourcen wollen und auf der anderen Seite Dienstleistungsunternehmen gleicher Rechtsform stehen. Die Zuordnung zum Geheimnisträger würde aufgrund der Vermischung für den Betroffenen nicht mehr den Schluss auf einen Geheimnisverpflichteten zulassen, dem er ursprünglich die Geheimnisse anvertraut hat. Denn wenn man auch annehmen mag, dass es für den Betroffenen vorhersehbar ist, dass innerhalb eines Unternehmens Informationen zur Funktionserfüllung notwendigerweise an von vornherein feststehende Personen weitergegeben werden müssen, ist dies nicht mehr annehmbar, wenn Personen aus einem anderen Unternehmen eingesetzt werden.

Die Argumente, die für das Erfordernis eines Arbeitsverhältnisses sprechen, sind indes nicht durchgreifend. Für die Ablehnung des Erfordernisses eines Arbeitsverhältnisses kann zunächst generell angeführt werden, dass es für die strafrechtliche Beurteilung nicht maßgeblich auf die Wirksamkeit oder das Vorhandensein zivilrechtlicher Verträge ankommen kann. Für das Strafrecht sind in diesem Bereich vielmehr faktische Gegebenheiten maßgeblich. Dies kann aus den Unterschieden zwischen dem Strafrecht und dem privaten Vertragsrecht abgeleitet werden, die es grundsätzlich nicht erlauben, dass zivilrechtliche Vorgänge den Inhalt von Straftatbestandsnormen determinieren. Auch wenn man die zivilrechtliche Bedeutung im Einzelfall, nach dem jeweiligen Straftatbestand differenzierend, betrachtet und nur dann eine Übereinstimmung von Vertragsrecht und Strafrecht nach dem Gebot der Einheit der Rechtsordnung ablehnt, wenn es die Besonderheiten des Strafrechts erforderlich machen, ist hinsichtlich des Straftatbestandes des

§ 203 StGB eine faktische Unterwerfung unter die Weisungen des Geheimnisverpflichteten ausreichend. Hierfür spricht der Wortlaut des § 203 Abs. 3 Satz 2 StGB, nach dem die berufsmäßigen Gehilfen denjenigen gleichstellt sind, die hinsichtlich der nach § 203 Abs. 1 StGB Schweigepflichtigen „bei ihnen zur Vorbereitung auf den Beruf tätig sind". Tätig werden bedeutet aber nicht, dass dafür ein Arbeitsvertrag erforderlich ist[230].

Für die fehlende Notwendigkeit eins Arbeitsvertrags kann auch ein Vergleich mit § 53a StPO angeführt werden[231]. Bei dieser Vorschrift wird nach h.M. der Begriff „Gehilfe" ebenfalls dahingehend interpretiert, dass derjenige, der nur faktisch tätig wird, ein Gehilfe sein kann[232]. Als maßgeblich wird die Veranlassung der Tätigkeit durch den Hauptberufsgeheimnisträger gesehen. Lediglich Tätigkeiten, die nicht im unmittelbaren Zusammenhang mit der Berufstätigkeit stehen, werden nicht vom Begriff des Gehilfen erfasst[233]. Zwar bestehen Unterschiede zwischen dem Strafprozessrecht und dem materiellen Strafrecht, dies spricht aber nicht gegen eine parallele Bestimmung des Gehilfenstatus bei § 203 Abs. 3 StGB und § 53a StPO. Denn der objektive Gehilfenstatus wird durch die Unterschiede zwischen Verfahrensrecht und materiellem Strafrecht nicht beeinflusst. Der Gehilfenstatus ist sowohl von dem nicht deckungsgleichen Personenkreis der nach § 203 StGB Schweigepflichtigen bzw. nach § 53 StPO Zeugnisverweigerungsberechtigten [234] als auch vom Geheimnisbegriff unabhängig. Er betrifft die allgemeine Frage der Zuordnung einer Person zu einem Hauptberufsträger.

Gegen das Erfordernis eines wirksamen Arbeitsverhältnisses ist schließlich entscheidend der Sinn und Zweck der Gleichstellungsklausel in § 203 Abs. 3 S. 2 StGB anzuführen. Die Gleichstellung der berufsmäßigen Gehilfen gegenüber den in § 203 Abs. 1 StGB genannten Schweigepflichtigen bezweckt die Ausdehnung

---

[230] Ähnlich Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 95.
[231] Für eine „harmonisierte Auslegung des Gehilfenbegriffs in StGB und StPO" Hoenike/Hülsdunk, MMR 2004, S. 789.
[232] Meyer-Goßner, StPO, § 53a Rn. 2; Senge, in: Karlsruher Kommentar StPO, § 53a Rn. 2; Rogall, in: Systematischer Kommentar StPO, § 53a Rn. 8; Lemke, in: Heidelberger Kommentar StPO, § 53a Rn. 2.
[233] Senge, in: Karlsruher Kommentar StPO, § 53a Rn. 2.
[234] Beispielsweise sind die Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung, die nach § 203 Abs. 1 Nr. 6 StGB schweigepflichtig sind, nicht als zeugnisverweigerungsberechtigte Personen in § 53 StPO aufgelistet. Allerdings wollte der Gesetzgeber nur bei den Hauptberufsträgern eine enumerative Auflistung, die sich im materiellen Strafrecht und im Prozessrecht unterscheidet. Dass er auch den akzessorischen Gehilfenbegriff unterschiedlich behandeln wollte, ist nicht ersichtlich.

auf Personen, die typischerweise mit den Geheimnissen in Kontakt gelangen. Dies können aber entsprechend der Gestaltung im Einzelfall auch Personen sein, die kein Arbeitsverhältnis mit dem Outsourcer haben oder auch Personal, das von externen Dienstleistungsunternehmen dem Outsourcer für bestimmte Tätigkeiten überlassen worden ist.

Dies wird noch durch folgende Überlegung gestützt. In der heutigen Arbeitswelt ist das Berufsausübungsverständnis, das im Bereich des § 203 Abs. 1 StGB zu Grunde gelegt worden ist, überkommen. Es ist im zunehmenden Maße durch Konzentration und Arbeitsteilung gekennzeichnet. Die typische Konstellation, dass ein Einzelner sich einem lauteren Berufsausübenden aufgrund individueller Integrität des einzelnen Berufsausübenden anvertraut, entspricht für die in § 203 Abs. 1 StGB genannten Berufe zunehmend nicht mehr den tatsächlichen Gegebenheiten. Dies gilt vermehrt auch für die freien Berufe, etwa den des Arztes oder des Rechtsanwalts. Beleg dafür sind beispielsweise die Zulassung von Kooperationsformen der GmbH oder AG im Berufsrecht[235] sowie die Verstärkung der Wettbewerbsmöglichkeit durch die höchstrichterliche Rechtsprechung[236]. Dies spricht dafür, dass auch der personale Charakter des Berufsgeheimnisses nach § 203 Abs. 1 StGB einer Anpassung bedarf und der Fokus mehr auf einen institutionellen Bezug gelegt wird oder anders ausgedrückt, dass bei der Bestimmung des Gehilfenstatus verstärkt die Ausgestaltung der Zusammenarbeit zu berücksichtigen ist[237].

---

[235] So ist die Berufsausübung in Form einer Anwalts- GmbH ermöglicht worden, vgl. § 59c ff. BRAO; durch das GKV-Modernisierungsgesetz wurde erstmals die Möglichkeit kapitalistisch verfasster Behandlungseinrichtungen geschaffen, vgl. § 95 Abs. 1 SGB V.

[236] Die Ausweitung der Wettbewerbsmöglichkeiten erfolgte durchweg gestützt auf die Berufsfreiheit. In den Urteilen klingt die Veränderung der Wirtschaftsverhältnisse, die auch Einfluss auf die freien Berufe hat, durch; vgl. nur zur Internetwerbung von Ärzten die Entscheidungen des BVerfG vom 17.07.2003, Az.: 1 BvR 2115/02, vom 26.08.2003, Az.: 1 BvR 1003/02 und vom 26.09.2003, Az. 1608/02.

[237] Freilich erscheint die Annahme von Berger Kurzen, E-Health und Datenschutz, S. 2f., „ das Arzt-Patienten-Verhältnis entwickelt sich zu einer professionellen Partnerschaft mit einem selbstverantwortlichen Patienten und einem Dienstleistungserbringer ohne hierarchisches Gefälle, wobei der Patient zum Klienten und der Arzt zum Gesundheitsberater wird“, etwas geschönt. Der Patient wird in der Regel angesichts der Informationsflut schon aus zeitlichen Gründen kaum fachwissenschaftliche Artikel auswerten, geschweige denn prüfen können, selbst wenn die Informationen online verfügbar wären. Dies ist schon für die Berufsausübenden kaum zu leisten. Alle anderen Informationsquellen müsste der Patient erst auf ihre Verlässlichkeit prüfen. Denn Gesundheitstipps aus dem Internet, die zuvor in der TV-Zeitschrift standen oder umgekehrt, mögen im Einzelfall vielleicht hilfreich sein, als Grundlage einer professionellen Zusammenarbeit taugen sie nicht. Insofern wird die Veränderung wahrscheinlich weniger einschneidend stattfinden und ist eher darin zu sehen, dass der Berufsausübende sich nicht auf seine Autorität qua professione verlassen kann, sondern sich im eigenen Interesse auf die neuen Techniken einzustellen hat und diese unter

Unter Zugrundelegung dieser Erkenntnisse ist für das Outsourcing medizinischer Daten zu differenzieren. Das Vorliegen eines wirksamen Arbeitsvertrages ist nicht entscheidend. Wohl aber bedarf es der Existenz überhaupt einer vertraglichen Vereinbarung, durch die eine eindeutige Ausgestaltung der Beziehung im Sinne einer weisungsgebundenen, unmittelbaren Unterstützung erfolgt. Ohne eine solche vertragliche Vereinbarung wäre bei komplexen Rechtsbeziehungen eine nachvollziehbare Zuordnung eines Gehilfen zu einem Schweigepflichtigen illusorisch[238]. Soweit ein Vertragsverhältnis in der Literatur nicht für erforderlich erachtet wird, ist dies an Einzelfällen, beispielsweise für ehrenamtlich Tätige, festgemacht worden, bei denen die Zuordnung im Innenbereich zu natürlichen Personen relativ leicht erfolgen kann[239]. Hier auf das Veranlassungsprinzip abzustellen und nicht auf einen Arbeitsvertrag, erscheint möglich.

Dies gilt aber dann nicht, wenn Personal eines rechtlich und organisatorisch selbständigen Unternehmens für den Outsourcer tätig wird. Auch wenn der Einsatz des Fremdpersonals kontinuierlich über längere Zeit erfolgen soll, steht doch das Fremdpersonal in zwei Beziehungen, zum einen in der Tätigkeitsbeziehung zum Outsourcer, zum anderen in der arbeitsvertraglichen Beziehung zum anbietenden Dienstleistungsunternehmen. Diese Vermischung der Sphären muss organisatorisch kompensiert werden. Ansonsten würde man das Prinzip der Personenbezogenheit bei § 203 Abs. 1 StGB aufgeben und nicht nur den tatsächlichen Veränderungen im Wirtschaftsleben anpassen.

Daher bedarf es einer vertraglichen Vereinbarung mit dem Outsourcingnehmer hinsichtlich des Tätigwerdens des eingesetzten Fremdpersonals. Darin ist das Direktionsrecht hinsichtlich der auszuführenden Tätigkeit sowie die organisatorische Einbindung in den Bereich des Outsourcers so zu regeln, dass eine klare Zuordnung zum Outsourcer möglich ist. Das rein faktische Tätigwerden reicht in diesen Fällen nicht aus. Hinsichtlich der unterstützenden Tätigkeit darf kein Weisungs- oder Kontrollrecht beim Outsourcingnehmer verbleiben. Durch das Direktions-

---

Informationsgesichtspunkten, aber auch unter Wettbewerbsgesichtspunkten ergänzend einbinden muss.

[238] Auch das Veranlasserprinzip kann nicht weiterhelfen, weil kein Anknüpfungspunkt für eine Veranlassung sinnvoll festgestellt werden kann.

[239] So mag es einsichtig sein, dass der gelegentlich unterstützende Ehegatte oder der Sohn als Gehilfe bezeichnet wird, vgl. Bartsch, Ärztliche Schweigepflicht und Zeugnisverweigerungsrecht im Strafprozess, S. 29.

recht muss sichergestellt sein, dass hinsichtlich des Umgangs mit medizinischen Daten der Schweigepflichtige eindeutig die Kontrolle und die Steuerung der Tätigkeiten behält. Das Fremdpersonal muss in diesem Punkt einem Arbeitnehmer des Outsourcers gleichgestellt sein. Die Einräumung eines solchen Direktionsrechts beim Überlassen von Personal des IT-Dienstleistungsunternehmens an den Outsourcer ist arbeitsrechtlich möglich.

Die Vereinbarung allein eines Direktionsrechts innerhalb einer Kooperation auf vertraglicher Grundlage ist in diesen Fällen nicht ausreichend. Damit würde die Tatsache, dass es sich bei dem anbietenden IT-Dienstleistungsunternehmen um eine rechtlich, funktional und organisatorisch getrennte und selbständige Einheit handelt, nicht hinreichend berücksichtigt. Wechselt personenbezogene Information zwischen solchen Einheiten, liegt darin grundsätzlich ein „Offenbaren“ i.S. v. § 203 StGB. Zu der vertraglichen Vereinbarung müssen Maßnahmen hinzutreten, die das Verhältnis zwischen Outsourcer und eingesetztem Fremdpersonal vom Outsourcingnehmer abschirmen.

Anerkannt ist nämlich, dass ein Offenbaren nicht nur durch positives Tun, sondern auch durch Unterlassen verwirklicht werden kann und den in § 203 StGB genannten Personen aufgrund ihrer Tätereigenschaft eine besondere Pflichtenstellung und damit Garantenstellung aus § 13 StGB zukommt[240]. Daraus wird abgeleitet, dass ein Schweigepflichtiger Maßnahmen ergreifen muss, um zu verhindern, dass ein Außenstehender Kenntnis von den Geheimnissen erlangt[241].

Durch das Entsenden von Fremdpersonal wird über die Brücke des entsendeten Mitarbeiters eine Verbindung zwischen Outsourcer und dem IT- Dienstleistungsunternehmen hergestellt. Um von einer Funktionseinheit oder von einem Gehilfenstatus sprechen zu können, in dem das Personal zum Kreis der zum Wissen Berufenen zu zählen ist und der Kontrolle durch den Schweigepflichtigen unterliegt, muss die Verbindung zum IT- Dienstleistungsunternehmen abgeschirmt werden, um zu verhindern, dass über die oben beschriebene Brücke Geheimnisse nach außen dringen. In die Abschirmung muss das Fremdpersonal einbezogen sein. Dadurch muss erreicht werden, dass das Fremdpersonal nicht die eingesehe-

[240] Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 52; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 46; Ulsenheimer/Heinemann, MedR 1999, S. 202f.
[241] Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 52.

nen Geheimnisse innerhalb der Rechtsbeziehung zum entsendenden IT- Dienstleistungsunternehmen weitergeben darf. Erforderlich ist eine Vereinbarung zwischen den Beteiligten, dass eingesehene Geheimnisse nicht an das entsendende Unternehmen weitergeleitet werden dürfen, wobei das IT- Dienstleistungsunternehmen an dieser Vereinbarung teilnehmen muss.

Wird das Fremdpersonal physisch nicht im räumlich- gegenständlichen Bereich des Outsourcers tätig, sondern ist das Fremdpersonal mit dem Outsourcer vernetzt, verbleibt aber sonst im räumlich- gegenständlichen Bereich des IT-Dienstleistungsunternehmens aus dem es stammt, ist zusätzlich ein wirksamer Schutz der Verbindung erforderlich. Dabei ist der Schutzkreis um das Fremdpersonal und den Outsourcer zu ziehen, damit eine Eingliederung des Fremdpersonals in den Kreis der zum Wissen Berufenen angenommen werden kann[242].

Aus dem Angeführten ergibt sich zugleich, dass eine vertraglich begründete Zusammenarbeit zwischen Outsourcer und privatem IT- Dienstleistungsunternehmen, ein sog. „joint venture“[243], nicht ausreicht, um den Personen des IT-Dienstleistungsunternehmen einen Gehilfenstatus zu verschaffen. In solchen Fällen erfolgt lediglich eine Verbindung zweier rechtlich selbständiger Institutionen, aber keine Einbindung. Entsprechendes gilt für mit dem Outsourcer verbundene Unternehmen oder für Tochterunternehmen des Outsourcers, da auch hier grundsätzlich rechtlich selbständige Unternehmen bestehen, die nicht über gesellschaftsrechtliche Qualifikationen zu i.S.v. § 203 StGB maßgeblichen Funktionseinheiten werden.

Wie der Schutz der Verbindung organisatorisch- technisch erreicht werden kann, beispielsweise in der Verschlüsselung der kompletten Verbindung oder in dem Einsatz portabler Speichermedien mit spezifischen Zugangskarten, ist grundsätzlich den Beteiligten überlassen[244]. Eine strafrechtliche Verpflichtung zum Einsatz einer bestimmten Technik besteht nicht. Tatsächlich müssen die Maßnahmen aber eine klare und wirksame Trennung und Absicherung der Funktionsbereiche herstellen. Eine Orientierung kann dabei an § 11 Abs. 5 BDSG erfolgen.

---

[242] Dazu für den Bereich des Outsourcings von Versicherungsdaten Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 97.
[243] Zum Begriff vgl. Tepper, in: Arens, Gesellschaftsrecht, S. 1494f.; Schücking, in: Münchener Handbuch des Gesellschaftsrechts, Band 1, § 4 Rn. 37.
[244] Zu einzelnen Maßnahmen vgl. Münch, Technisch-organisatorischer Datenschutz, S. 1 ff.

b) Der Bereich des § 203 Abs. 2 StGB

Der Gehilfenstatus nach § 203 Abs. 3 StGB gilt nicht für § 203 Abs. 2 StGB. Daher scheint in diesem Bereich die Möglichkeit einer Einbindung als Gehilfe auszuscheiden. Der Gesetzgeber ist davon ausgegangen, dass sich im Behördenverkehr das Problem der Kenntnisnahme durch einen Gehilfen nicht stellt. Dies ist in der Allgemeinheit nicht zutreffend[245]. Neben der Möglichkeit auf gesetzlicher Grundlage private Dritte über das Rechtsinstitut der Beleihung mit hoheitlichen Aufgaben zu betrauen und damit für einen bestimmten funktionalen Bereich zu Verwaltungsträgern zu machen, besteht auch die Möglichkeit der Einschaltung privater Dritter als Verwaltungshelfer[246]. Wird ein privater Dritter außerhalb der Behörde tätig, stellt sich das Problem des Offenbarens an einen Gehilfen in ähnlicher Weise wie bei § 203 Abs. 1 i.V.m. § 203 Abs. 3 StGB. Es stellt sich die Frage, ob auf andere Weise ein Dritter in den Kreis der zum Wissen Berufenen integriert werden kann.

§ 203 Abs. 2 S. 1 Nr. 2 StGB ermöglicht die straflose Weitergabe von Geheimnissen an Personen, die für den öffentlichen Dienst nach dem Verpflichtungsgesetz besonders verpflichtet worden sind. Dies scheint dafür zu sprechen, dass Personen, die bei einem externen Dienstleistungsunternehmen beschäftigt sind, über eine förmliche Verpflichtung nach dem Verpflichtungsgesetz in den Bereich der zum Wissen Berufenen integriert werden können[247].

Eine solche Interpretation des § 203 Abs. 2 S. 1 Nr. 2 StGB ist nicht überzeugend. Dies würde dem durch § 203 StGB verwirklichten Schutz des Rechts auf informationelle Selbstbestimmung nicht gerecht werden. Denn jede Weitergabe an Dritte, die außerhalb der Behörde stehen, stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts sind grundsätzlich spezialgesetzliche Regelungen erforderlich, damit personenbezogene Informationen weitergegeben werden dürfen[248]. In § 203 Abs. 2 S. 1 Nr. 2 StGB ist lediglich geregelt, dass für den öffentlichen Dienst be-

---

[245] So zutreffend Otto, wistra 1999, S. 203.
[246] Dazu Maurer, Allgemeines Verwaltungsrecht, § 23 Rn. 56 und 60; Wolff/Bachof/Stober, Verwaltungsrecht, Band 2, S. 414; zu einem Beispiel, das die praktische Relevanz im Bereich des Gesundheitswesens belegt, vgl. BGH NJW-RR 1999, S. 767.
[247] So wohl Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 52 und Köpke, Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für Private Krankenversicherer, S. 235.
[248] BVerfGE 65, 46 (61).

sonders Verpflichtete einer Schweigepflicht unterliegen. Allein die Tatsache, dass jemand einer Schweigepflicht unterliegt, ist für die Frage eines unbefugten Offenbarens weder bei § 203 Abs. 1 i.V.m. § 203 Abs. 3 StGB noch bei § 203 Abs. 2 StGB entscheidend. Maßgeblich muss sein, ob das Geheimnis innerhalb einer Funktionseinheit verbleibt oder in den ungeschützten Außenbereich gelangt. Daher ist mit der h.M. nur dann eine straflose Geheimnisweitergabe im Behördenverkehr anzunehmen, wenn das Geheimnis an funktional zuständige Behördenmitarbeiter weitergegeben wird[249]. Dabei muss das Geheimnis nicht zwingend innerhalb einer Behörde bleiben. So bildet beispielsweise eine Aufsichtsbehörde, soweit sie Kenntnis von dem Geheimnis nimmt, um ihre Aufgaben zu erfüllen, mit der beaufsichtigten Behörde eine Funktionseinheit, innerhalb derer eine Geheimnisweitergabe zutreffend nicht nach § 203 StGB strafbar ist[250].

Wird aber außerhalb solcher Strukturen ein privater Dritter als Verwaltungshelfer herangezogen, kann die bloß förmliche Verpflichtung nach dem Verpflichtungsgesetz den Verwaltungshelfer nicht in den innerbehördlichen Bereich eingliedern. Aus dem Verpflichtungsgesetz lässt sich im Voraus materiell nichts zu einer funktionellen Eingliederung entnehmen. Die Behörde regelt das Tätigwerden vielmehr autonom. Die Einschaltung eines Verwaltungshelfers kann hinsichtlich des Rechtsgutschutzes in § 203 StGB nur dann akzeptabel sein, wenn der Verwaltungshelfer entsprechend einem Gehilfen nach § 203 Abs. 3 StGB in den Innenbereich des Schweigepflichtigen einbezogen wird. Eine funktionale Eingliederung kann nur unter den gleichen Voraussetzungen wie bei § 203 Abs. 1 i.V.m. § 203 Abs. 3 StGB erfolgen. Werden diese Voraussetzungen erfüllt, dann kann zwischen Verwaltungshelfer und primär Schweigepflichtigen von einer tatbestandlichen Verantwortungseinheit gesprochen werden.

c) Zwischenergebnis

Im Ergebnis ist festzuhalten, dass über eine Einbindung externer Mitarbeiter eines privaten IT- Dienstleistungsunternehmen als Gehilfen eine Tatbestandsverwirklichung des § 203 StGB beim Outsourcing medizinischer Daten entfallen kann. Nach der hier vertretenen Ansicht liegt kein „Offenbaren“ i.S.v. § 203 StGB vor.

[249] Vgl. bereits oben Fußnote 170.
[250] Vgl. OLG Frankfurt NStZ-RR 2003, S. 170; a.A. Kreuzer, NJW 1975, S. 2236.

Die Einschränkung des Tatbestandes wird dadurch ausgeglichen, dass auf der Ebene des Tatbestandes Sicherheitsanforderungen einfließen. Erreicht werden muss eine wirksame Abschirmung des Funktionsbereichs Outsourcer und eingebundener Mitarbeiter vom außen stehenden Unternehmen.

5. Vollendung und der Bezug Dritter zum Geheimnis

Neben der Bestimmung von Funktionseinheiten ist die Frage von Interesse, wann Dritte mit einem Geheimnis so in Berührung gekommen sind, dass ein Offenbaren angenommen werden kann. Dies betrifft die Frage der Vollendung des § 203 StGB. Als Dritte sind nach den vorausgegangenen Ausführungen alle Personen zu verstehen, die außerhalb einer Funktionseinheit stehen. Bei verkörperten Geheimnissen in der Form herkömmlicher Schriftstücke wird angenommen, dass dann ein Offenbaren vorliegt, wenn die Sache, also das Schriftstück, dem Dritten zugegangen ist.

a) Gewahrsam und tatsächliche oder potentielle Kenntnisnahme

Dafür muss der Dritte nach h.M. Gewahrsam, also die Ausübung der vom Herrschaftswillen getragenen tatsächlichen Sachherrschaft, an der Sache erworben haben[251]. Ob dies der Fall ist, beurteilt sich nach der Verkehrsanschauung.

Soweit besteht in der Literatur weitgehend Einigkeit. Umstritten ist jedoch, ob sowohl bei verkörperten Daten als auch bei nicht verkörperten Daten für ein Offenbaren durch Unterlassen auch die Möglichkeit der Kenntnisnahme des Geheimnisses ausreicht[252]. Dies wird praktisch z.B. dann relevant, wenn Schriftstücke offen liegen gelassen werden oder ausreichende Sicherungsmaßnahmen unterbleiben. Hier besteht die Möglichkeit, dass Dritte, die nicht bestimmungsgemäß mit dem Geheimnis in Kontakt kommen sollen, Einsicht nehmen können. Im Bereich elektronischer Kommunikation ist die Integration des Internets zu nennen. Denkbar ist, dass private Unternehmen Softwaredienste im Internet anbieten, die

[251] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 4; zum Gewahrsamsbegriff vgl. Tröndle/Fischer, StGB, § 242 Rn. 11.
[252] Tröndle/Fischer, StGB, § 203 Rn. 30a f.

für einen bestimmten Kreis von Nutzern Anwendungen ermöglichen[253]. In solchen Konstellationen könnte ein Offenbaren in der Form des Unterlassens angenommen werden.

Dieses Problem wird kontrovers diskutiert[254]. Zum Teil wird angenommen, dass die Möglichkeit der Kenntnisnahme nicht ausreiche, sondern der Dritte tatsächlich Kenntnis erlangen muss bzw. das Schriftstück an sich genommen haben muss[255]. Begründet wird dies überwiegend damit, dass eine Entsprechung zum positiven Tun eine tatsächliche Kenntnisnahme erfordert, weil andernfalls das Rechtsgut nur gefährdet aber nicht verletzt wird[256]. Dem gegenüber wird vertreten, dass eine Gewahrsamsverschaffung wegen der Weite des Begriffs Offenbaren nicht erforderlich ist[257].

Bei der Lösung dieses Problems ist eine differenzierende Betrachtung angezeigt. Zunächst ist zuzugeben, dass bei § 203 StGB nicht maßgeblich auf Gefährdungsgesichtspunkte abgestellt werden darf. Notwendig ist eine Verletzung i.S. eines Bruchs des Geheimnisses. Allerdings ist unzutreffend, dass in der Möglichkeit der Kenntnisnahme keine Verletzung liegen kann. Die Unterscheidung zwischen Gefährdungsdelikt und Verletzungsdelikt zwingt nicht zu der Annahme, dass nur bei einer tatsächlichen Kenntnisnahme im Sinne einer Gewahrsamsverschaffung ein Geheimnisbruch angenommen werden kann. Denn der Übergang zwischen konkreten Gefährdungsdelikten und Verletzungsdelikten ist nicht trennscharf und mit dem angenommenen Erfordernis eines zum Tatbestand zählenden Erfolges ist die abzulehnende Berücksichtigung einer abstrakten Gefährdung ausgeschlossen. Außerdem bedingt die Handlungsform des Unterlassens zwangsläufig ein Gefährdungsmoment. Auch vor dem Hintergrund, dass maßgeblich der Schutz der Privatsphäre durch § 203 StGB bezweckt wird, ist für die Frage des Geheimnisbruchs daher überzeugender auf den Aspekt des Erfolgseintritts abzustellen und nicht auf die Frage Gefährdung oder Verletzung.

---

[253] Im einfachsten Fall kann dies darin liegen, einen sicheren Datenaustausch zu gewährleisten oder einen zentralen Speicherplatz zur Verfügung zu stellen. Denkbar sind aber auch telemedizinische Anwendungen.
[254] Vgl. Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 474ff.
[255] Vgl. Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 52; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 46; Lenckner, in: Schönke/Schröder StGB, § 203 Rn. 20.
[256] Vgl. Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 52; a.A. Lackner/Kühl, StGB, § 203 Rn. 17.
[257] Langkeit, NStZ 1994, S. 7.

Der Erfolgseintritt bei § 203 StGB ist nicht notwendig davon abhängig, dass ein Außenstehender Gewahrsam an dem Informationsträger erhält, um die Möglichkeit einer Kenntnisnahme für ein Offenbaren ausreichen zu lassen. Zwar wird ein Offenbaren durch positives Tun zumeist in einer Übergabe der Information an eine bestimmte Person liegen, die dann darüber verfügen kann, was bei einer gerichteten mündlichen Übermittlung regelmäßig Kenntnisnahme voraussetzt, weil keine Verkörperung erfolgt. Allerdings ist es aus Sicht des Betroffenen nicht in erster Linie erheblich, ob die Information an eine bestimmte Person gelangt und diese daran Gewahrsam hat. Vielmehr ist maßgeblich, dass die Information aus dem Kreis der zum Wissen Berufenen nach außen in den Kontakt mit Dritten entlassen wird. Eine besondere Qualität der Handlung Offenbaren, die einer Entsprechung im Bereich des Unterlassens bedürfte, besteht nicht. Dem möglichen Einwand, dass bei einer solchen Betrachtungsweise § 203 StGB unzulässig zu einem Fahrlässigkeitsdelikt ausgeweitet wird, ist zu entgegnen , dass über eine sachgerechte Begrenzung der Garantenstellung sowie über das Merkmal des Vorsatzes Strafbarkeitsausweitungen zu Lasten des Täters verhindert werden können, so dass der Schweigepflichtige nicht aufgrund übertriebener Sorgfaltsanforderungen mit sämtlichen Möglichkeiten einer Kenntnisnahme rechnen muss.

Dies wird auch deutlich, wenn man die herkömmliche Art der Weitergabe verkörperter Informationen betrachtet. Die Informationen werden auf Papier festgehalten und gegebenenfalls in Akten gesammelt. Sollen Informationen an Außenstehende weitergegeben werden, werden Schriftstücke mit einem Umschlag versehen und versendet[258]. Dies ist eine gerichtete und abgeschirmte Form der Weitergabe, die sich eines bestimmten Versendungsweges bedient und ein relativ klares Bezugsverhältnis zwischen Absender und Empfänger schafft. Daneben können verkörperte Daten auch nicht derart gerichtet an Außenstehende gelangen, beispielsweise durch mündliche Weitergabe. Hier kann sich die Information auf einen unüberschaubaren Kreis von (mithörenden) Personen verbreiten. Mit dem Begriff „Gewahrsam“ kommt man dann nicht weiter. Hier wird vielfach darauf abgestellt, dass die Information zur Kenntnis genommen werden muss[259]. Vollends ungerichtet ist eine Veröffentlichung beispielsweise in Zeitschriften. Soll, wenn die Veröf-

[258] Digitale Information wird auf portable Datenträger kopiert und dann verschickt.
[259] Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 52.

fentlichung durch den Schweigepflichtigen erfolgt, ein Offenbaren davon abhängen, dass jemand die Zeitschrift liest?

Vom Schutzzweck des § 203 StGB her kann die Frage des Gewahrsams im Rahmen des Tatbestandmerkmals Offenbaren insgesamt keine maßgebliche Bedeutung haben. Das Kriterium der Sachherrschaft greift zu kurz, weil der Fokus einseitig auf das Substrat der Information gerichtet ist. Soll ein abgeschickter Brief, der vom Empfänger nicht gelesen, sondern vernichtet wird, ein Offenbaren darstellen, während ein offenes Liegenlassen von Schriftstücken mit sensiblen Daten keines ist, weil sie keiner mitnimmt. Das kann auch im Bereich verkörperter Information nicht überzeugen. Maßgeblich muss der Gedanke sein, ob die Information den Bereich der zum Wissen Berufenen verlassen hat und dem Kreis der Außenstehenden zuzuordnen ist. Über den Gewahrsam als notwendiges Kriterium lässt sich die Frage nicht immer zutreffend beantworten. Vielmehr ist zu fordern, dass das Geheimnis aufgrund einer Handlung des Schweigepflichtigen die Bindung an den Kreis der zum Wissen Berufenen verloren hat. Hierfür ist eine normative Betrachtung erforderlich, die geänderten technischen Rahmenbedingungen und geänderten Arbeitsbedingungen gerecht wird.

Dass das Offenbaren nicht auf eine besondere Art der Weitergabe abstellt, wird auch deutlich, wenn man einen Vergleich zum Datenschutzrecht anstellt. Das Datenschutzrecht verwendet nicht den Begriff des Offenbarens, sondern den Begriff des Übermittelns[260]. Das Übermitteln ist in § 3 Abs. 4 S. 2 Nr. 4 BDSG legaldefiniert. Unter einer Übermittlung ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten zu verstehen. Das Gesetz konkretisiert die Bekanntgabe dahingehend, dass eine solche vorliegt, wenn die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Für die erste Variante des Weitergebens ist ein aktives Tätigwerden erforderlich. Nicht ausreichend ist beispielsweise ein versehentliches Liegenlassen[261]. In der zweiten Variante geht die Aktivität vom Dritten aus. Erforderlich ist ein Einsehen oder Abrufen, also eine konkrete Inbesitznahme der Daten durch den Dritten[262]. Damit soll den Entwicklungen in der Online- Kommunikation Rechnung getragen wer-

[260] Umfassend zum Begriff des Übermittelns Heinzelmann, Die Datenübermittlung, S. 14 ff.
[261] Dammann, in: Simitis, BDSG, § 3 Rn. 152.
[262] Dammann, in: Simitis, BDSG, § 3 Rn. 154; vgl. auch Taraschka, CR 2004, S. 283.

den, weil die vorangegangene Regelung nahezu einem Verbot der Online-Übermittlung gleichgekommen ist[263]. Entsprechend ist nicht mehr im Merkmal der Übermittlung der Schutz vor möglicher Kenntnisnahme zu suchen. Vielmehr erfolgt der Schutz auf einer anderen Ebene durch Regelungen zur Zulässigkeit entsprechender Verfahren und zu den Anforderungen an solche Verfahren.

Eine solche Differenzierung findet im Rahmen des § 203 StGB nicht statt. Das Tatbestandsmerkmal Offenbaren erfasst sowohl ein Unterlassen als auch ein positives Tun. Auch stellt sich bei digitalisierten Informationen, anders als bei schriftlich in Papierform verkörperten Informationen, das Problem, dass aufgrund der Technik der Standort der Information nahezu beliebig verschiebbar ist, eine räumliche Barriere nicht besteht und bei ungenügenden Schutzvorkehrungen eine Vielzahl von Personen auf die Nachricht zugreifen kann. Die daraus resultierende Nähe Dritter kann bei einer Möglichkeit der Kenntnisnahme zu der Annahme führen, dass das Geheimnis die Bindung an den Schweigpflichtigen verloren hat und dem Außenbereich zuzuordnen ist. Der mögliche Einwand, dass bereits die Möglichkeit der Kenntnisnahme zur Uferlosigkeit führen oder zu einer unzulässigen Auslegung als Gefährdungsdelikt führen würde, kann bei § 203 StGB sowohl im Bereich verkörperter als auch im Bereich nicht verkörperter Informationen nicht überzeugen. Über den Begriff des Offenbarens können keine Aussagen über eine spezifische Qualität der Begehungsform getroffen werden. Maßgeblich bei einer Verwirklichung durch ein Unterlassen bei § 203 StGB ist der Erfolg, nicht die Art der Tatbegehung, wie etwa im Bereich des § 211 StGB. Daher führt das Entsprechungserfordernis des § 13 StGB nicht weiter[264]. Auch wird dadurch keineswegs bei § 203 StGB nur auf eine Gefährdung des Rechtsgutes und nicht auf eine Verletzung abgestellt. Eine Berücksichtigung von Gefährdungsgesichtspunkten bei normativer Betrachtung ist bei Verletzungsdelikten nicht unbekannt. So wird überwiegend in der Rechtsprechung und der Literatur im Rahmen des Betrugstatbestandes angenommen, dass der Eintritt eines Vermögensschadens auch bei einer konkreten Vermögensgefährdung angenommen werden

[263] Vgl. Dammann, in: Simitis, BDSG, § 3 Rn. 153, 154.
[264] Allgemein zur Gleichwertigkeitsproblematik des § 13 StGB, BGHSt 28, 307ff.; Roxin, JuS 1973, S. 199 f.

kann[265]. Dass dies bei § 203 StGB nicht erfolgen darf, allein weil hier primär das informationelle Selbstbestimmungsrecht geschützt ist, überzeugt nicht.

Kommt es entscheidend auf die Bindung des Geheimnisses an den Kreis der zum Wissen Berufenen an, bedarf es für die Frage, ob die Möglichkeit der Kenntnisnahme ausreicht, weiterer Differenzierung. Ist eine verkörperte Information innerhalb einer Funktionseinheit offen liegen gelassen worden und ist eine räumliche Abgrenzung nicht gegeben, dann ist aus normativ- objektiver Sicht die Bindung an den Geheimnisträger hinreichend aufgehoben worden, um von einem Offenbaren sprechen zu können. Wird beispielsweise eine Akte offen liegen gelassen und ist ein Kontakt Dritter mit den Daten vorhersehbar und ohne nennenswerte Überwindung von Barrieren möglich, dann liegt darin ein Offenbaren. Lässt der Arzt im Wartezimmer Patientenunterlagen liegen, dann ist dies normativ nicht anders zu beurteilen als die aktive Übergabe an einen Dritten.

Die ausgeführte Ansicht bestätigt sich, wenn man sich dem Bereich der digitalisierten Geheimnisse zuwendet. Im Zuge der Entwicklung moderner Kommunikationsmöglichkeiten ist eine Vielzahl weiterer Kommunikations- und Informationstechniken geschaffen worden. Die Frage, ob ein Offenbaren vorliegt, wenn die Möglichkeit zur Kenntnisnahme besteht, ist hier umstritten[266]. Diskutiert worden ist das Problem insbesondere bei der externen Wartung einer EDV- Anlage oder eines Computernetzwerks. Zum Teil wird in solchen Fällen nur dann ein Offenbaren bejaht, wenn der Dritte tatsächlich die Information zur Kenntnis nimmt. Zur Begründung wird angeführt, dass eine Wartung erfolgen kann, ohne dass das Personal die Information versteht[267]. Argumentiert wird weiterhin, dass bei der Masse der gespeicherten Daten für die reale Kenntniserlangung ein gesonderter Zugriff erfolgen muss, etwa im Wege eines Ausdrucks oder einer Speicherung[268].

Demgegenüber vertritt ein Teil der Literatur die Ansicht, dass unabhängig davon, ob ein schriftlich verkörpertes oder digitalisiertes Geheimnis vorliegt, die tatsäch-

---

[265] BGH vom 13.06.1985, Az.: 4StR 413/85; BGH vom 21.12.2001, Az.: 2StR 260/01; Tröndle/Fischer, StGB, § 263 Rn. 94 ff.
[266] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 41; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 52; Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 475ff.
[267] Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 144.
[268] So Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 41; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 52.

liche Möglichkeit der Kenntnisnahme für ein Offenbaren ausreicht[269]. Eine nähere Begründung erfolgt nicht.

Beiden Meinungen kann nicht in vollem Umfang zugestimmt werden. Zunächst ist festzuhalten, dass das Argument, bei großen Datenmengen sei die Möglichkeit einer Kenntnisnahme unzureichend für ein Offenbaren und es einer tatsächlichen Kenntnisnahme bedürfe, nicht überzeugt. Abgesehen von der Schwierigkeit festzulegen, ab welcher Quantität dies gelten soll, passt ein Abstellen auf die Größe des Datenbestandes systematisch nicht zur Tathandlung, sondern lässt sich besser der Kausalität bzw. der Rechtsfigur der objektiven oder subjektiven Zurechnung zuordnen. Hinzu kommt, dass die Unterscheidung zwischen Tun und Unterlassen gerade im Bereich digitalisierter Informationen unscharf ist. Die Übermittlung von Daten online und das Ermöglichen des Zugriffs auf Daten durch Dritte über ein Netz kann gerade wegen der Vernetzung uno actu erfüllt sein, da eine Übermittlung unter Unterlassung von Sicherheitsmaßnahmen in bestimmten Konstellationen einen ungehinderten Zugriff auf die Daten erst ermöglicht[270]. Eine Abgrenzung von positivem Tun oder Unterlassen ist kaum zu leisten. Dies gilt auch für das Beispiel der externen Fernwartung. Die Auftragsvergabe an ein externes Wartungsunternehmen bedingt zugleich die Verschaffung des Zugangs zu den Daten. Dies als positives Tun oder als Unterlassen zu qualifizieren ist nicht zweifelsfrei möglich. Auch ein Abstellen auf den Schwerpunkt der Handlung wäre eher willkürlich. Aus der Handlungsform Konsequenzen für das Offenbaren zu ziehen, erscheint daher nicht tragfähig.

Auf den Gewahrsamsgedanken zu rekurrieren und daraus bei digitalisierten Informationen generell eine Inbesitznahme durch Speicherung oder eine Einsichtsnahme zu verlangen, ist nicht überzeugend. Ist nach der hier vertretenen Auffassung auch bei verkörperten Geheimnissen die Erlangung des Gewahrsams nicht der maßgebliche Aspekt, muss dies bei digitalisierten Informationen erst recht gelten. Hier ist der Gedanke der Sachherrschaft angesichts der Überwindung

---

[269] Otto, wistra 1999, S. 202 allerdings ohne Eingehen auf das Unterlassen; deutlich Ehmann, CR 1991, S. 294, der von einem Zulassen des Zugriffs spricht, durch den sich der Arzt strafbar macht, außer das Wartungspersonal hat Gehilfenstatus; vgl. auch Sieber, in Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 480, der dann ein Offenbaren annimmt, wenn „eine Kenntnisnahme ohne weiteres möglich ist".

[270] So beispielsweise in Funknetzwerken, wenn die Verschlüsselung nicht eingeschaltet wird. Dann kann mit wenig Aufwand und handelsüblicher Technik jeder die gesendeten Daten mitlesen.

räumlicher Grenzen durch die Vernetzung und der damit einhergehenden Aufhebung der Bindung der Information an ein bestimmtes Substrat kein taugliches Kriterium.

Auf der anderen Seite kann allein die Möglichkeit der Kenntnisnahme nicht ausreichend sein, um ein Offenbaren zu bejahen. Die Möglichkeit ist theoretisch nie auszuschließen. Daher würde, bei einer solchen Auffassung, § 203 StGB zu einem abstrakten Gefährdungsdelikt ausgeweitet werden. Damit kollidiert aber der durch § 203 StGB bezweckte Rechtsgüterschutz sowie die Einordnung als Verletzungs- und Sonderdelikt. Nicht das Allgemeininteresse ist vorwiegend geschützt, sondern Individualinteressen. Reicht bei digitalisierten Geheimnissen bereits allein die Möglichkeit der Kenntnisnahme aus, würden die Verhältnisse beim Rechtsgüterschutz ins Gegenteil verkehrt. Zudem würde unter Verletzung von Art. 103 Abs. 2 GG die strafbare Handlung zu weit in den Versuchsbereich verschoben werden. Der Versuch ist aber bei § 203 StGB gerade nicht strafbar.

Daher muss auch im Bereich der digitalisierten Geheimnisse für die Frage des Offenbarens der Gedanke leitend sein, ob bei objektiv- normativer Betrachtung die Bindung des Geheimnisses an den Geheimnisverpflichteten diesem zurechenbar derart gelockert worden ist, dass von einem Offenbaren ausgegangen werden kann[271]. Maßgeblich muss sein, dass im Vergleich zum analogen Bereich die bestehende Warnfunktion und der Personenbezug bei § 203 StGB nicht erodiert werden, sondern auf demselben Niveau unter den geänderten technischen Rahmenbedingungen erhalten bleiben.

b) Unterschiedliche Bezugsverhältnisse

Davon ausgehend sind für den Bereich des Umgangs mit digitalisierten Geheimnissen unterschiedliche Konstellationen hinsichtlich des Bezugs Dritter zu den Geheimnissen (ist der Personenbezug etwa durch Verschlüsselung, Anonymisierung oder Pseudonymisierung aufgehoben worden, scheitert der Tatbestand schon am fehlenden Geheimnis) differenzierbar: (1) Der Zugriff kann sicher feststehen. (2) Der Zugriff ist möglich, ohne dass Sicherungsmaßnahmen erfolgt sind. (3) Der

[271] Vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 99, der von unterschiedlichen Näheverhältnissen spricht.

Zugriff ist möglich, wobei Sicherungsmaßnahmen zu überwinden sind. (4) Ein Zugriff ist aufgrund von Sicherungsmaßnahmen praktisch ausgeschlossen.

Vergleichsweise einfach ist der Fall zu beurteilen, wenn ein Zugriff sicher erfolgt ist. Steht ein Zugriff sicher fest, kommt es für ein Offenbaren darauf an, ob dieser Zugriff ausreicht, um die Information aus der ursprünglichen Bindung zwischen Schweigepflichtigem und Geheimnisträger herauszulösen. Dies ist sicher dann anzunehmen, wenn der Dritte die Möglichkeit hat, Daten, die im Klartext vorliegen, zu speichern. Damit ist die Information sicher in den Bereich des Dritten übergegangen.

Darüber hinaus ist aber auch dann ein Offenbaren anzunehmen, wenn der Dritte lediglich einen Lesezugriff erlangt und er die Möglichkeit hat, die Information zu verstehen. Hier kann die Beurteilung nicht anders ausfallen als bei herkömmlichen Schriftstücken. Hat jemand einen Brief erhalten, der nicht für ihn bestimmt ist, dann liegt ein Offenbaren vor, unabhängig davon, ob er in den Brief hineinschaut. Die Information ist der Kontrolle des Schweigepflichtigen entzogen und dem Bereich des Dritten überlassen.

Davon unterschieden werden kann der Fall, dass ein Zugriff erfolgt ist, der Zugreifende aber die Information nicht verstehen kann. Zum Teil wird in der Literatur gefordert, dass ein Verstehen der Informationen erforderlich sei, um ein „Offenbaren“ i.S.v. § 203 StGB annehmen zu können[272]. Diese Auffassung überzeugt nicht. Sie schränkt den Begriff des Offenbarens im Bereich digitalisierter Informationen ohne Notwendigkeit zu sehr ein. Auch aus einer Parallele zum Datenschutzrecht lässt sich kein Argument für eine solche Auffassung herleiten. Zutreffend ist lediglich, dass eine „Übermittlung“ i.S.d. Bundesdatenschutzgesetzes eine Einsicht der Daten erfordert. Daraus kann aber nicht zwingend gefolgert werden, dass der Einsichtnehmende die Daten verstanden haben muss.

Zu differenzieren ist wie folgt. Ist bei gespeicherten, digitalisierten Informationen der Personenbezug wirksam aufgehoben, etwa durch Verschlüsselung oder Anonymisierung, dann liegen nach hier vertretener Auffassung keine Geheimnisse vor, so dass ein Offenbaren ausscheidet. Ist der Personenbezug dagegen nicht auf-

[272] Vgl. Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 142.

gehoben, dann reicht die Möglichkeit des Verständnisses aus. Denn die digitalisierte Form stellt für ein Verständnis der Information keine ins Gewicht fallende Schranke dar, sofern allgemein zugängliche Codierungen und Formate benutzt werden. Auch ist die Annahme, dass nach einem unbefugten Eindringen in geschützte Systeme der Inhalt der gesicherten sensiblen Dateien nicht zur Kenntnis genommen werden soll, wenig überzeugend. Vielmehr ist das Eindringen notwendige Vorstufe für ein beabsichtigtes Erfassen des verborgenen Informationsinhalts[273]. Nur soweit spezifische Codierungen und Formate verwendet werden, die nicht von Dritten mit herkömmlichen Mitteln gelesen werden können, ist der Zugriff nicht ausreichend, um ein Offenbaren anzunehmen.

Fraglich ist, ob eine generelle Zugriffsmöglichkeit ohne bestehende Sicherungsvorkehrungen für ein Offenbaren ausreicht. Daran könnte man zweifeln, weil die konkreten Geheimnisse erst noch durch den Dritten aufgerufen werden müssen. Bis dahin liegen sie in der Masse der gespeicherten Daten maskiert auf Datenträgern. So wird in der Literatur für den Bereich der Software-Fernwartung vertreten, dass selbst in dem Einräumen von Zugangsrechten zu einem kompletten EDV-System oder Computernetzwerk kein Offenbaren gegeben ist, wenn es sich um große Datenbestände oder Archive handelt. Hier fehle es wegen der Masse der Daten an einer konkreten Zugriffsmöglichkeit auf jedes einzelne Geheimnis[274].

Dies überzeugt nicht. Die Masse der Daten ist, wie schon erwähnt, kein taugliches Kriterium für die Bestimmung, ob eine Geheimnis dem Bereich des Dritten zugeordnet werden kann. Unabhängig von der Schwierigkeit, eine bestimmte Größenordnung festzulegen, vernachlässigt ein Abstellen auf die Größe der Daten das potentielle Verhalten des Dritten. Besteht ein ungehinderter Zugang, dann liegt es allein an dem Dritten, nach sensiblen Daten zu suchen. Dass bei einzelnen Zugriffen die Wahrscheinlichkeit sehr gering ist, auf personenbezogene Informationen zu stoßen, mag bei großen Datenbeständen zutreffen. Allerdings ist es bei uneingeschränkten Zugriffsmöglichkeiten nur eine Frage der Zeit, bis auch personenbezogene Daten betroffen sind.

---

[273] Vgl. Tröndle/Fischer, StGB, § 202a Rn. 11; Hilgendorf, Jus 96, S. 994.
[274] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 41.

Die Größe der Datenmenge kann nicht das Unterlassen von Sicherungsmaßnahmen kompensieren. Die Größe der Datenmenge relativiert sich im Übrigen auch, wenn man beachtet, dass auf der Seite der Zugreifenden eine Vielzahl von Personen stehen können, die aufgrund einer Vernetzung Zugriff erhalten. Ist eine Türe in einem Gebäude immer offen, dann wird auch irgendwann jemand den Raum betreten und Einsicht nehmen, sofern Personen das Gebäude betreten und das Gebäude in einer bewohnten Gegend steht. Dies gilt im vergleichbaren Maße für virtuelle Türen. Daher ist bei solchen Konstellationen der Dritte derart in die Nähe der Information gerückt, dass objektiv- normativ von einer Aufhebung der Bindung an den Geheimnisverpflichteten ausgegangen werden muss.

Nach der hier vertretenen Ansicht ist damit eine sachgerechte Bestimmung des objektiven Tatbestands erfolgt, ohne dass die Grenze zu einem bloßen Gefährdungsdelikt oder zum straflosen Versuch verwischt wird. Rechnung getragen wird lediglich der Tatsache, dass beim Einsatz digitalisierter Informationen die räumlichen Grenzen und die Bindung der Information an ihr Substrat gelockert werden. Erfolgt der Einsatz digitalisierter Informationen ohne Sicherungsmaßnahmen, kommt dies einem öffentlichen Aushang oder einer Einladung zum Mitlesen gleich. Damit würde die Warnfunktion des § 203 StGB völlig missachtet. Erweitert der Geheimnisverpflichtete den Einflussbereich Dritter auf die ihm anvertrauten Geheimnisse, ist der Erweiterung auch auf Tatbestandseite Rechnung zu tragen. Denn mit dieser Erweiterung darf objektiv keine Auslagerung der Verantwortung einhergehen. Die im Bereich des Geheimnisbegriffs bestehende tatbestandliche Verantwortungseinheit findet hier konsequenterweise ihre Fortsetzung.

Eine andere Beurteilung ist nur dann gerechtfertigt, wenn keine Verbindung benutzt wird, auf die eine Vielzahl von Dritten Zugriff haben. Dies ist etwa dann der Fall, wenn ein physisch isoliertes Netzwerk benutzt wird. Haben aufgrund der Organisationsstruktur zu diesem Netzwerk nur der Schweigepflichtige und seine Gehilfen Zugang, bedarf es hier keiner zusätzlichen Sicherungsmaßnahmen im Netzwerk. Dritte werden dann objektiv- normativ nicht in einen näheren Bezug zu der Information gebracht, da keine eingerichtete Verbindung nach außen besteht. Die Kontaktmöglichkeit wird nicht strukturell ausgeweitet, die Information verbleibt im Innenbereich der Schweigepflichtigen.

Zweifelhaft ist weiterhin der Fall, bei dem die Möglichkeit, auf die Geheimnisse zuzugreifen, nur besteht, wenn Sicherungsmaßnahmen überwunden werden[275]. Sind die Sicherungsmaßnahmen um die jeweilige Funktionseinheit gezogen, dadurch können, wie oben festgestellt, auch Funktionseinheiten gegründet werden, erscheint ein Offenbaren fraglich, da die Information nur im geschützten Kreis der zum Wissen Berufenen verbleibt. Allerdings greift diese Beurteilung zu kurz. Sie übergeht die Frage der Wirksamkeit der vorhandenen Schutzvorkehrungen. Sind die Schutzvorkehrungen mit einfachen und allgemein zugänglichen Mitteln zu überwinden, dann kann dies im Ergebnis dazu führen, dass die Geheimnisse ebenso offen herumliegen, wie wenn keine Sicherungsvorkehrungen bestünden. Bedient sich der Schweigepflichtige digitaler Kommunikationstechniken, die eine Außenverbindung ermöglichen, dann muss er gleichzeitig dafür sorgen, dass diese Außenverbindung bezüglich der zu schützenden Geheimnisse nicht für unbefugte Dritte offen steht. Denn ein ungenügend geschütztes System kann im gleichen Ausmaß eine Schwachstelle darstellen wie ein plaudernder Gehilfe, der nicht durch den Schweigepflichtigen aufgefordert wird, sein Verhalten einzustellen.

Fraglich ist, welche Anforderungen an die Schutzvorkehrungen zu stellen sind. Dabei geht es auch um eine sachgerechte Bestimmung des objektiven Tatbestandes. Es überzeugt nicht, nur solche Maßnahmen als ausreichend anzusehen, die einen Zugriff Dritter praktisch ausschließen. Diese Anforderungen wären bei der Komplexität moderner Kommunikationssysteme kaum zu erfüllen. In Konsequenz dazu würde der Einsatz moderner Kommunikationsmittel mit einem hohen und schwer einschätzbaren Strafbarkeitsrisiko einhergehen. Vor dem Hintergrund des durch Art. 103 Abs. 2 GG und § 1 StGB gewährten Grundsatzes „nulla poena sine lege certa“ erscheint dies bedenklich. Dagegen spricht auch, dass das Strafrecht nur ultima ratio sein soll. Eine Strafe soll nur verhängt werden, wenn andere Sanktionsmechanismen versagen. Daher passt ein Anforderungsniveau, das darauf abzielt, sämtlichen Gefährdungen zu begegnen, nicht zu § 203 StGB. Diese Aufgabe ist sachgerechter anderen Rechtsgebieten des öffentlichen Rechts, dem Datenschutzrecht oder gar dem Zivilrecht zuzuweisen. Darüber hinaus ist ein solches

[275]Sieber spricht in solchen Fällen von der Möglichkeit eines „mittelbaren“ Offenbarens, vgl. Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 482. Unterschieden werden können technische und normative Sicherungsmaßnahmen, vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 102. Zu einzelnen technischen Sicherungsmaßnahmen Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 92 ff.; Berger Kurzen, E-Health und Datenschutz, S. 164 ff.

Anforderungsniveau auch deswegen abzulehnen, weil ansonsten § 203 StGB primär als ein Gefährdungsdelikt interpretiert werden würde.

Aufgrund dieser Argumente ist es vorzugwürdig, die Anforderungen an die Schutzvorkehrungen zu begrenzen. Nicht erforderlich ist eine bestimmte, bestmögliche Sicherheitsstruktur, sondern eine solche, die nach dem aktuellen Stand der Technik tatsächlich ein wirksames Hindernis für den unbefugten Zugriff Dritter erwarten lässt, so dass der Verantwortliche nach zumutbarer Ausschöpfung externer Informationsquellen nicht mit einer Umgehung rechnen muss. Zu einem Offenbaren kann danach nur ein Unterlassen solcher Schutzmaßnahmen führen, deren Fehlen einem Zugriff durch Dritte voraussehbar keine ernsthaften Hindernisse entgegenstellt, so dass mit einem Zugriff gerechnet werden kann. Dies ist beispielsweise dann der Fall, wenn in einem an das Internet angebundenem Netzwerk elementare Sicherungsvorkehrungen nicht ergriffen werden beispielsweise, wenn eingesetzte Virensoftware nicht aktualisiert wird oder bekannte Sicherheitslücken nicht behoben werden.

Das Absenken der Anforderungen im Vergleich zu den Anforderungen an eine wirksame Verschlüsselung rechtfertigt sich daraus, dass hier ein vom Bereich des Schweigepflichtigen getrennter, schwer überschaubarer und seinem unmittelbaren Einflussbereich entzogener Bereich betroffen ist. Hier spielt ein mögliches und nicht sicher feststehendes Verhalten Dritter, die auf die Geheimnisse zugreifen könnten, eine Rolle. Dieses auf der Ebene des objektiven Tatbestands zu berücksichtigen ist dann gerechtfertigt, wenn angenommen werden kann, dass das Verhalten Dritter absehbar ist, weil der Schweigepflichtige elementare Schutzmaßnahmen unterlassen hat. Geht es hingegen um das Handlungsobjekt oder um die der Kontrolle des Schweigepflichtigen unmittelbar unterliegenden Bereiche, sind strengere Anforderungen an Sicherheitsvorkehrungen sachgerecht. Festzuhalten ist, dass dann ein Offenbaren vorliegen kann, wenn der Zugriff durch Dritte wegen ungenügender Sicherungsmaßnahmen mit leichten Mitteln möglich und absehbar ist.

Unproblematisch ist der Fall, dass ein Zugriff aufgrund der ergriffenen Schutzvorkehrungen praktisch ausgeschlossen ist. Eine immer bestehende theoretische Möglichkeit des Zugriffs kann nicht ausreichen, um das Tatbestandmerkmal Of-

fenbaren zu bejahen. Die theoretische Möglichkeit vermittelt nicht einen konkreten Bezug des Dritten zum Geheimnis und kann daher keinesfalls für ein Offenbaren ausreichend sein.

c) Zwischenergebnis

Im Ergebnis genügt daher für ein Offenbaren die Möglichkeit des Zugriffs. Dies gilt nur dann nicht, wenn aufgrund des Zugriffs einem Verständnis der Information noch Hindernisse entgegenstehen, die nicht mit einfachen, allgemein zugänglichen Mitteln überwunden werden können.

6. Schweigerecht und Beschlagnahmeverbot

Gegenstände, die sich im Gewahrsam eines nach § 53 oder § 53a StPO Schweigeberechtigten befinden, unterliegen nach § 97 Abs. 1 bzw. Abs. 4 StPO einem Beschlagnahmeverbot. Das Beschlagnahmeverbot sichert das Zeugnisverweigerungsrecht des § 53 bzw. § 53a StPO vor Umgehung und ergänzt die materiellrechtliche Schweigepflicht des § 203 StGB im Prozess[276]. Schweigepflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot stehen in einem sachlichen Zusammenhang. Werden Geheimnisse an Personen weitergegeben, ohne dass das Beschlagnahmeverbot des § 97 StPO eingreift, bedeutet dies für den Geheimnisträger einen Nachteil.

Es fragt sich daher zum einen, ob nur dann ein Offenbaren verneint werden kann, wenn auch Beschlagnahmefreiheit gegeben ist. Diese Frage ist zu verneinen. Der Personenkreis der Schweigepflichtigen und der Zeugnisverweigerungsberechtigten ist unterschiedlich. Auch geht § 53 StPO, an den § 97 StPO anknüpft, sachlich weiter als § 203 StGB, weil er auch Tatsachen erfasst, die nicht „Geheimnisse“ i.S.v. § 203 StGB sind[277]. Schließlich betreffen die §§ 97, 53, 53a StPO keinen § 203 StGB vergleichbaren Geheimnisschutz. Bezweckt wird nämlich durch die §§ 97, 53, 53a StPO der verfahrensrechtliche Schutz des Beschuldigten in seiner

[276] Meyer-Goßner, StPO, § 97 Rn. 1.
[277] Meyer-Goßner, StPO, § 53 Rn. 4.

Beziehung zum Schweigepflichtigen[278]. Dieser besondere und ergänzende verfahrensrechtliche Schutz ist für die inhaltliche Bestimmung der Reichweite des materiellen Privatgeheimnisschutzes nach § 203 StGB nicht tauglich[279].

Zum anderen ist von Interesse, wann ein Beschlagnahmeverbot eingreift, wenn Geheimnisse vom Schweigepflichtigen an andere Personen weitergegeben werden[280]. Beschlagnahmefrei sind die in § 97 Abs. 1 Nr. 1-3 StPO aufgezählten Gegenstände. § 97 Abs. 2 S. 1 StPO verlangt, dass sich der Gegenstand im Gewahrsam des Zeugnisverweigerungsberechtigten befindet. Nach § 97 Abs. 4 StPO gilt ein Beschlagnahmeverbot auch dann, wenn „Gehilfen" i.S.v. § 53a StPO die in § 97 Abs. 1 StPO bezeichneten Gegenstände im Gewahrsam haben. Ausreichend ist nach zutreffender Auffassung auch Mitgewahrsam des Zeugnisverweigerungsberechtigten[281]. Gegenstände nach § 97 Abs. 1 Nr. 1-3 StPO, die ein „Geheimnis" i.S.v. § 203 StGB enthalten und im Wege des Outsourcings weiteren Personen zugänglich gemacht werden, unterliegen somit nur dann der Beschlagnahmefreiheit des § 97 StPO, wenn sie entweder zumindest im Mitgewahrsam des Outsourcers sind oder im Gewahrsam seines Gehilfen sind. Gewahrsam bedeutet dabei die tatsächliche Sachherrschaft und Verfügungsmacht über die Gegenstände[282].

Soweit digitalisierte Daten vom Outsourcing betroffen sind, ist auf den Gewahrsam über den Datenträger abzustellen. Liegt der Datenträger außerhalb von Räumen, über die der Schweigeberechtigte oder der Gehilfe die tatsächliche Sachherrschaft haben, dann greift das Beschlagnahmeverbot des § 97 StPO nicht ein. Dies ist dann der Fall, wenn medizinische Daten an Personen weitergegeben werden, die diese Daten auf Datenträgern aufbewahren und die nicht der tatsächlichen Verfügungsmacht des schweigepflichtigen Outsourcers oder eines Gehilfen i.S.v. § 203 Abs. 3 StGB unterliegen.

---

[278] Meyer-Goßner, StPO, § 53. 1.
[279] § 53 StPO wird dementsprechend nicht als Rechtfertigungsgrund für § 203 StGB angesehen, vgl. Meyer-Goßner, StPO, § 53, Rn. 5; die Unterschiede zwischen Strafprozessrecht und materiellem Strafrecht sprechen nicht gegen eine einheitliche Interpretation des Gehilfenbegriffs, vgl. S. 72.
[280] Freilich stellt sich die Frage nur, wenn die schweigepflichtige Person, die outsourct, auch zeugnisverweigerungsberechtigt ist.
[281] Meyer-Goßner, StPO, § 97 Rn. 12; Beulke, Strafprozessrecht, Rn. 248.
[282] Meyer-Goßner, StPO, § 97 Rn. 11.

Hier stellt sicht die Frage, ob durch geeignete Maßnahmen der Gewahrsam des schweigepflichtigen Outsourcers begründet werden kann. Denkbar ist, dass durch vertragliche und technische Schutzvorkehrungen, beispielsweise durch Verschlüsselung der Daten und der Verbindung, sichergestellt wird, dass nur der Outsourcer und nicht das externe IT-Dienstleistungsunternehmen über die Daten verfügen kann. Im Ergebnis ist die Möglichkeit einer solchen Gewahrsamsbegründung abzulehnen. Zwar wird für den analogen Bereich zu § 97 StPO vertreten, dass der Zeugnisverweigerungsberechtigte auch Gewahrsam an Gegenständen in gemieteten Schließfächern hat, selbst wenn die Schließfächer nur gemeinsam mit dem Vermieter geöffnet werden können[283]. Insofern könnte daran gedacht werden, dass dies auch für virtuelle Schließfächer gilt. Hiergegen spricht aber, dass Gegenstand im Sinne des § 97 StPO der Datenträger als der physikalische Ort, an dem die Daten aufbewahrt werden, ist. Gewahrsam über diesen hat aber nicht der Outsourcer, sondern das aufbewahrende IT-Dienstleistungsunternehmen. Nur wenn der Datenträger selbst in Räumen verschlossen ist, zu denen nur der schweigepflichtige Outsourcer Zugang hat, kann die Sachherrschaft und damit auch ein Beschlagnahmeverbot nach § 97 StPO der Verkehrsanschauung nach bejaht werden.

Für den Übertragungsweg der Daten über ein Netz besteht kein Beschlagnahmeverbot. Schon für den analogen Bereich wird zutreffend von der h.M. davon ausgegangen, dass auf dem Postweg § 97 StPO nicht eingreift[284]. Gleiches muss für die Phase der Übertragung im Netz gelten. Der Online Versand wird nicht durch § 97 StPO geschützt, sondern durch Art. 10 GG.

VI. Sozialadäquanz

Neben den bisher ausgeführten Aspekten ist zu prüfen, ob eine Strafbarkeit daran scheitert, dass das Outsourcen von medizinischen Daten sozialadäquat ist. Nach der ursprünglich von Welzel entwickelten Lehre der Sozialadäquanz sind bestimmte an sich tatbestandsmäßige Verhaltensweisen nicht zu bestrafen, weil sie gesellschaftlich betrachtet üblich und völlig normal erscheinen und damit vom

[283] Meyer-Goßner, StPO, § 97 Rn. 11.
[284] Meyer-Goßner, StPO, § 97 Rn. 11; Rudolphi, in: SK StPO, § 97 Rn. 15; Lemke, in: Lemke/Julius/Krehl/Kurth/Rautenberg/Temming, StPO, § 97 Rn. 8; Schäfer, in: LR StPO, § 97 Rn. 17.

Strafrecht nicht erfasst werden sollten[285]. Dem Gedanken der Sozialadäquanz verwandt ist die Figur des „erlaubten Risikos“[286]. Auch hier geht es letztlich darum, bestimmte tatbestandsmäßige Verhaltensweisen aus dem Bereich der Strafbarkeit auszuschließen. Über die Figur des „erlaubten Risikos“ lässt sich das Ergebnis der Straffreiheit genauso erzielen wie mit der Lehre der Sozialadäquanz.

Sind sich die Vertreter der Lehre von der Sozialadäquanz im Ergebnis der Straffreiheit noch einig, ist die Einordnung in den Deliktsaufbau äußerst umstritten. Teilweise wird in der Lehre von der Sozialadäquanz ein Tatbestandskorrektiv gesehen[287], während andere darin einen Rechtfertigungsgrund sehen[288].

Neben der Einordnung ist auch die Notwendigkeit der Figur der „Sozialadäquanz“ nicht unumstritten[289]. Denn welche Handlungen als sozial adäquat zu bewerten sind, hängt von der Beurteilung der jeweiligen Sozialordnung ab, in der die Handlung sich ereignet und enthält somit eine historisch-normative Komponente. Andererseits ist die Qualität und Intensität der Handlung selbst ein möglicher Anknüpfungspunkt für die Beurteilung der Sozialadäquanz. Beide Aspekte sind schwer greifbar und objektivierbar. Zudem ist die Sozialordnung naturgemäß keine feststehende Größe, sondern ständiger Veränderung unterworfen. Wegen dieser Unschärfe des Begriffs der „Sozialadäquanz“ und der Probleme bei der Bestimmung derjenigen Verhaltensweisen, die als sozialadäquat zu gelten haben, stellt sich die Frage, ob mit dem herkömmlichen Instrumentarium die Fälle mit größerer Rechtssicherheit und Objektivität zu lösen sind. Denkbar ist beispielsweise, dass die Fälle möglichen sozialadäquaten Verhaltens bereits durch Auslegung aus dem Bereich der Strafbarkeit ausgeschieden werden[290]. Auch das Institut der „Einwilligung“, § 34 StGB oder das Prinzip der „Interessen- und Güterabwägung“ als solcher ist in Betracht zu ziehen. Insofern könnte sich ein Zurückgreifen auf den Begriff der „Sozialadäquanz“ erübrigen.

---

[285] Welzel, ZStW 58, 516; Lenckner, in: Schönke/Schröder, Vorb. §§ 13 ff. Rn. 69; Rönnau, in: Leipziger Kommentar StGB, Vor § 32 Rn. 48.
[286] Tröndle/Fischer, StGB, Vor § 32 Rn. 13.
[287] So die h.M. Tröndle/Fischer, StGB, Vor § 32 Rn. 12; Lenckner, in: Schönke/Schröder, StGB, Vorb. §§ 13ff. Rn. 70; offen gelassen von BGHSt 23, 228.
[288] Welzel, ZStW 58, S. 516; weitere Nachweise bei Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, S. 5; Tröndle/Fischer, StGB, Vor § 32 Rn. 12.
[289] Tröndle/Fischer, StGB, Vor § 32 Rn. 12; Lenckner, in: Schönke/Schröder StGB, Vorb. §§ 13 ff. Rn. 70; Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, S. 5; ablehnend Rönnau, in: Leipziger Kommentar StGB Vor § 32, Rn. 52.
[290] Hierfür Lenckner, in: Schönke/Schröder, StGB, Vorb. § 13 Rn. 70.

Die Frage bedarf nur vertiefter Erörterung, wenn für die strafrechtliche Beurteilung von Outsourcingvorhaben die Figur der „Sozialadäquanz“ eine Rolle spielt. Im Rahmen einer möglichen Strafbarkeit nach § 203 StGB könnte der Gedanke sozialadäquaten Verhaltens bereits im objektiven Tatbestand beim Merkmal Offenbaren bzw. unbefugtes Offenbaren Bedeutung gewinnen. In Betracht zu ziehen ist ein Tatbestandsausschluss, sofern das Outsourcing medizinischer Daten als sozialadäquat zu bewerten ist.

Auch wenn man die Lehre von der Sozialadäquanz grundsätzlich akzeptiert, erscheint eine solche Bewertung äußerst fraglich. Zweifelhaft ist schon, ob das Outsourcing als wirtschaftliches Phänomen in der Sozialordnung derart verbreitet und üblich ist, dass es als völlig normal und damit als sozialadäquat bezeichnet werden kann. Eine Einordnung als bloß umkehrbarer, wirtschaftlich motivierter Trend ist gleichfalls möglich. Insbesondere die maßgebliche Überlegung der Kostenersparnis spricht gegen eine Bewertung als sozialadäquates Verhalten. Denn dieser Aspekt kann genauso gut für ein „Insourcing“ sprechen, sofern aufgrund veränderter technischer und wirtschaftlicher Rahmenbedingungen ein „Insourcing“ rentabler erscheint. Weiterhin ist die Digitalisierung und der Einsatz moderner Informationstechnologie als Massenerscheinung eine verhältnismäßig junge und sich ständig im Fluss befindliche Errungenschaft.

Entscheidend gegen die Annahme eines sozialadäquaten Verhaltens spricht, dass dem Outsourcing ein aufwendiger und komplexer Entscheidungsfindungsprozess vorangeht. Betroffen sind nicht „im sozialen Leben gänzlich unverdächtige, weil im Rahmen der sozialen Handlungsfreiheit liegende Handlungen“, auf die überwiegend das Eingreifen der Sozialadäquanz beschränkt wird[291].

Weiterhin bewirkt das Outsourcing eine erhebliche Veränderung der Beziehungen zwischen den Beteiligten, aber auch hinsichtlich der durch das Outsourcing Betroffenen. Betrachtet man Qualität und Intensität einer Outsourcingentscheidung und -durchführung, ist von einem besonderen Verhalten auszugehen, das nicht routinemäßig abläuft[292]. Es ist keinesfalls vergleichbar mit Erscheinungen im technischen und wirtschaftlichen Massenverkehr, für die vorwiegend die Lehre

[291] Zu dieser Beschränkung vgl. BGHZ 23, 228.
[292] Zur Schwierigkeit der Feststellung der Üblichkeit bei der Auslagerung der Abrechnung an externe Abrechnungsstellen vgl. Wolf, Externer Honorareinzug und Schweigepflicht, S. 60f.

der Sozialadäquanz herangezogen wird und die vielfach ähnlich, gehäuft und mit geringer Verletzungsintensität ablaufen. Demgegenüber haben Outsourcingprozesse i.d.R. einen hohen Individualisierungsgrad und beinhalten gewichtige Entscheidungen. Daher kann im Ergebnis nicht angenommen werden, dass das Outsourcing medizinischer Daten sozialadäquat ist und deswegen eine Strafbarkeit ausscheidet.

VII. Kausalität, objektive und subjektive Zurechnung

Werden medizinische Daten im Rahmen eines Outsourcingprojekts planmäßig an Dritte außerhalb des Kreises der zum Wissen Berufenen weitergegeben, so ist der objektive Tatbestand des § 203 StGB erfüllt. Die Zurechnung solchen Verhaltens bereitet keine größeren Schwierigkeiten. Problematisch sind die Fälle, in denen Dritte außerhalb des Kreises der zum Wissen Berufenen durch eigene Initiative in Kontakt mit sensiblen Daten gelangen. Strafrechtlich relevant für den Outsourcer kann dies insbesondere dann werden, wenn er keine wirksamen Schutzvorkehrungen getroffen hat. Gelangen dann mangelhaft geschützte Daten zufällig an Dritte oder können Dritte Sicherheitsvorkehrungen überwinden, kann nach der hier vertretenen Ansicht ein Offenbaren vorliegen, wenn unwirksame Schutzvorkehrungen getroffen worden sind.

Fraglich ist aber, ob die Handlung des Geheimnisverpflichteten kausal für den Erfolg ist. Die Prüfung der Kausalität erfolgt in der Rechtsprechung und in der Lehre nach der „conditio-sine-qua-non-Formel“[293]. Diese Formel, die von einem natürlichen Ursachenzusammenhang ausgeht, wird durch die Lehre, aber auch durch die Rechtsprechung, in besonderen Fallgestaltungen modifiziert und um normative Gesichtspunkte ergänzt. Solche Gesichtspunkte finden sich beispielsweise bei der alternativen Kausalität oder bei Unterlassungsdelikten, bei denen die Rechtsprechung von einem normativen Kausalitätsbegriff ausgeht und prüft, ob der Erfolg in seiner konkreten Gestalt entfallen wäre, wenn die Bedingung (die fragliche Handlung, die unterlassen wurde) hinzugedacht wird [294].

[293] Wessels/Beulke, Strafrecht AT Rn. 156, 159; Hilgendorf, GA 1995, S. 515.
[294] Tröndle/Fischer, StGB, Vor § 13 Rn. 20; Joecks, StGB, Vor § 13 Rn. 28ff.

Keine besonderen Schwierigkeiten bereitet die Fallgestaltung, in der Daten aufgrund eines Fehlers versehentlich an Dritte gelangen. Hier ist Kausalität gegeben. Schwieriger ist die Fallgestaltung, in der Dritte sich durch die Umgehung von Schutzvorkehrungen Zugriff auf die Daten verschafft haben. Als Dritte kommen dabei sowohl Mitarbeiter des externen privaten IT-Dienstleistungsunternehmens, als auch am Outsourcingverhältnis unbeteiligte Dritte in Betracht.

1. Kausalität

Grundsätzlich wird der Kausalzusammenhang durch eine weitere mitverursachende und durch Dritte gesetzte Bedingung nicht unterbrochen[295]. Eine Unterbrechung des Kausalverlaufs wird nur angenommen, wenn die neue Bedingung dem Kausalverlauf eine völlig neue Richtung gibt und die alte Ursache verdrängt[296]. Diese Fallgestaltung wird auch als überholende Kausalität bezeichnet. Bei der Umgehung von Schutzvorkehrungen liegt eine solche Fallgestaltung nicht vor. Die durch den Outsourcer gesetzte Bedingung kann zum einen im Heranziehen eines Mitarbeiters eines privaten Unternehmens und dem damit verbundenen aus den Händen Geben der Datenverarbeitung liegen. Zum anderen kann, sofern ungenügende Schutzmaßnahmen getroffen worden sind, auch auf das Unterlassen von wirksamen Schutzvorkehrungen abgestellt werden. In beiden Fällen wird dadurch erst ermöglicht, dass Dritte auf die Daten zugreifen können. Dass auch ein Tatbeitrag Dritter hinzukommt, bedeutet nicht, dass dadurch die ursprüngliche Handlung verändert wird. Vielmehr stehen beide Bedingungen in einem Ergänzungsverhältnis, in dem die ursprüngliche Handlung fortwirkt und als Grundlage für die auf ihr aufbauenden weiteren Handlung dient. Damit liegt ein Fall kumulativer Kausalität vor, da mehrere voneinander unabhängige Bedingungen nur zusammen den Erfolg herbeiführen können[297]. In diesen Fällen ist jede Handlung für sich erfolgsursächlich.

---

[295] Tröndle/Fischer, StGB, Vor § 13 Rn. 18a.
[296] Tröndle/Fischer, StGB, Vor § 23 Rn. 18c.
[297] Wessels/Beulke, Strafrecht AT Rn. 157; vgl. auch Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 145.

2. Objektive Zurechnung

Ein großer Teil der Lehre steht der Prüfung des Ursachenzusammenhangs nach der conditio-sine-qua-non-Formel kritisch gegenüber[298]. Die Kausalitätsformel wird vielfach nur als Minimalanforderung gesehen, gleichsam als erster Filter zur Bestimmung tatbestandlich relevanter Handlungen. Auf der nächsten Stufe wird dann geprüft, ob die Bedingung dem Handelnden objektiv zugerechnet werden kann.

Nach der Lehre von der objektiven Zurechnung ist nicht ein Ursachenzusammenhang, sondern ein normativ zu bestimmender objektiver Zurechnungszusammenhang maßgeblich. Verursachung und Zurechnung sind zu trennen. Innerhalb der Lehre von der objektiven Zurechnung haben verschiedene Varianten der Lehre mehrere objektive Zurechnungskriterien entwickelt. Diese sind nicht unter einem einheitlichen Konzept vereint, sondern erscheinen eher als Fallgruppenbildung, wobei die einzelnen Fallgruppen gewisse Ähnlichkeiten aufweisen[299]. Im Einzelnen ist die Anwendung und Gewichtung der unterschiedlichen objektiven Zurechnungskriterien umstritten[300]. Als integrativer Ausgangspunkt der unterschiedlichen Fallgruppen wird vielfach eine Grundformel verwendet, nach der ein Erfolg dann objektiv zurechenbar ist, wenn der Täter eine rechtlich relevante Gefahr geschaffen hat, die sich im tatbestandsmäßigen Erfolg realisiert[301].

a) Zurechnung in Rechtsprechung und Lehre

Die Lehre von der objektiven Zurechnung wird von der Rechtsprechung nur partiell und in Einzelfällen aufgegriffen. In die Kausalitätsprüfung fließen, ohne dass dies ausdrücklich benannt wird, Elemente der objektiven Zurechnung ein[302]. Weitgehend lehnt die Rechtsprechung es aber ab, das Problem der Zurechnung bereits in den objektiven Tatbestand einzubeziehen. In weiten Bereichen, insbesondere im Fahrlässigkeitsbereich, werden Ursachenzusammenhang und subjekti-

---

[298] Puppe, in: NK StGB, Vor § 13 Rn. 83.
[299] Lackner/Kühl, StGB, Vor § 13 Rn. 14; vgl. zu den Fallgruppen Wessels/Beulke, Strafrecht AT Rn. 179; Jescheck/Weigend, Strafrecht AT, § 28 IV; Roxin, Strafrecht AT 1, § 11 Rn. 39 ff.
[300] Wessels/Beulke, Strafrecht AT Rn. 17 und 179.
[301] Tröndle/Fischer, StGB, Vor § 13 Rn. 17; Jescheck/Weigend, Strafrecht AT, § 28 IV.
[302] Tröndle/Fischer, StGB, § 203 Rn. 18.

ve Erkenntnismöglichkeit verknüpft. Auf der Schuldebene prüft die Rechtsprechung bei Vorsatztaten und atypischen Kausalverläufen zumeist, ob ein Irrtum über den Kausalverlauf nach § 16 StGB den Vorsatz entfallen lässt[303]. Damit wird das Problem der Zurechnung nicht losgelöst von individueller Vorwerfbarkeit betrachtet, sondern durch die Rechtsprechung als Problem des Vorsatzes gesehen, das insgesamt auf der Schuldebene angesiedelt wird. In der Literatur wird diese Position ebenfalls vertreten[304]. Überwiegend wird dabei allerdings das Problem innerhalb der Wertungsstufe „Tatbestand" im subjektiven Tatbestand geprüft, womit dem unrechtsbegründenden Charakter des Tatbestandsvorsatzes als Verhaltensform Rechnung getragen werden soll. In der Sache sind die Unterschiede gering, da auch die Rechtsprechung auf der Schuldebene zwischen Vorsatz als Verhaltensform und Schuldform unterscheidet.

Für die Position der Rechtsprechung sprechen gute Gründe[305]. So erscheint bei atypischen Kausalverläufen die Aufspaltung in eine vermeintlich vorrangige objektive Zurechung und eine anschließende subjektive Zurechnung künstlich. Weiterhin wird angeführt, die Bestimmung der rechtlich relevanten Gefahr bleibt, trotz und wegen der Fallgruppenbildung, unpräzise[306]. Die Frage, wann eine Gefahr von der Rechtsordnung missbilligt wird und damit rechtlich relevant ist, wirft die Schwierigkeit auf, Gefahren objektiv in ihrer Qualität und Intensität zu beurteilen. Vielfach wird diese Schwierigkeit dadurch gelöst, dass gefragt wird, ob eine über das allgemeine, normale Lebensrisiko hinausgehende Gefährdung geschaffen worden ist. Was aber das „allgemeine Lebensrisiko" ist, kann kaum sicher festgestellt werden. Dafür ist der Begriff zu unbestimmt. Hinzu kommt, dass bei Verletzungsdelikten durch das Betonen des Gefahrmoments eine unzulässige Auslegung als abstraktes Gefährdungsdelikt droht.

Es erscheint daher zweifelhaft, ob, angesichts der Vagheit des Begriffs, auf eine vermeintlich objektiv-normative Betrachtung losgelöst von der subjektiven Erkenntnismöglichkeit abzustellen ist und die Lösung stets auf der Ebene des objek-

---

[303] Wessels/Beulke, Strafrecht AT Rn. 181, 258.
[304] Baumann/Weber/Mitsch, Strafrecht AT, § 14 Rn. 100.
[305] Der Rechtsprechung im Ergebnis zustimmend Hilgendorf, in: FS Weber, S. 34; zur neueren Kritik an der Lehre von der objektiven Zurechnung vgl. Samson, in: FS Lüderssen, S. 587ff.
[306] Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 103.

tiven Tatbestands gesucht werden sollte[307]. Dass ein Eingehen auf den Vorsatz bei einem Irrtum über den Kausalverlauf erst nach der objektiven Zurechnung geprüft werden darf, mag abstrakt betrachtet schlüssig durchführbar sein, im Einzelfall verschwimmen jedoch die klaren Grenzen zwischen objektiver und subjektiver Zurechnung.

Dies zeigt sich insbesondere an der Schnittstelle zwischen positivem Tun und Unterlassen, in der Handlungspflichten und Fahrlässigkeitsmomente einwirken. Bei dem Outsourcing von medizinischen Daten geht es um Verhaltenspflichten des Outsourcers hinsichtlich des Schutzes der sensiblen Daten vor dem Zugriff Dritter. In die Beurteilung fließt somit grundsätzlich eine Versäumnis- bzw. Unterlassenskomponente ein. Dass ein Versäumnis objektiv betrachtet eine rechtlich relevante Gefahr schaffen soll, aber bei demselben Versäumnis subjektiv betrachtet der Vorsatz wegen eines nicht vorhersehbaren Kausalverlaufs entfällt, erscheint konstruiert. Denn in beiden Fällen ist bezüglich des Risikos eine Prognose erforderlich.

Außerdem kommt nicht Absicht, sondern dolus eventualis als Vorsatzform in der Praxis und bei den meisten Fällen in Betracht. Ob der Täter ein Offenbaren billigend in Kauf genommen hat, lässt sich nicht allein nach den subjektiven Erkenntnismöglichkeiten des Täters bestimmen. Hier fließen auch objektive Betrachtungen mit ein, aufgrund derer auf die Vorsatzart geschlossen werden kann[308]. Vor bestimmten Erkenntnissen kann auch ein „blinder Täter“ seine Augen nicht verschließen. Damit ist aber auch notwendig, dass die objektiven Anhaltspunkte in Bezug zu den individuellen Fähigkeiten des Täters gesetzt werden.

Dies gewinnt insbesondere dann Bedeutung, wenn arbeitsteiliges Vorgehen in Frage steht. Wird beispielsweise durch einen Geheimnisverpflichteten auf die Aussage Dritter oder auf die Aussage des Outsourcingpartners hinsichtlich der Sicherheit und des Schutzes eines Systems vertraut, ist die Annahme bedingten

[307] Vgl. Hilgendorf, in: FS Weber, S. 34, 45f., der für eine Fortentwicklung der Lehre von der objektiven Zurechnung eintritt und einige Probleme aus dem Bereich des objektiven Tatbestandes herausnehmen will.

[308] Vgl. Tröndle/Fischer, StGB, § 15 Rn. 10, 10a; BGH NStZ 1984, S. 19; zwar trennt die Rechtsprechung zwischen den begrifflichen Voraussetzungen und der beweismäßigen Feststellung dieser Voraussetzungen im Prozess, aber in der Sache arbeitet die Rechtsprechung auch mit objektivnormativen Prämissen, wie insbesondere die Ausführungen zur höheren Hemmschwelle bei Tötungsdelikten zeigen, vgl. BGHSt 36, 1; BGH, NStZ 1984, S. 19 und BGH NStZ 2001, S. 475.

Vorsatzes, zumindest sofern objektive Anhaltspunkte das Vertrauen rechtfertigen, zweifelhaft. Tendenziell wird eher bewusste Fahrlässigkeit anzunehmen sein.

Die aufgezeigten Schwierigkeiten bieten gute Gründe, die Frage der Zurechnung als Vorsatzproblem anzusehen. Damit würde auch tendenziell der Straftatbestand des § 203 StGB restriktiver behandelt und der Forderung, dass das Strafrecht nur als ultima ratio zum Einsatz gelangt, entsprochen. Dies würde auch eher dem Schuldprinzip gerecht werden, da Handlungsabläufe weniger aus der Kategorie der persönlichen Vorwerfbarkeit herausgelöst werden.

Auf der anderen Seite sprechen auch gute Gründe für eine objektive Zurechnung. Die Fälle, in denen eine Verbindung zwischen Handlung und Verletzung bzw. Erfolg aufgrund des Schutzzwecks der Norm verneint werden, können schwer als subjektive Zurechnung aufgefasst werden. Vielmehr geht es in diesen Fällen um eine von der Vorhersehbarkeit losgelöste normative Beurteilung der Reichweite rechtlich vorgeschriebener Verhaltenspflichten[309]. Vorwiegend betroffen sind davon Fahrlässigkeitstaten. Aber auch bei Vorsatzdelikten kann angenommen werden, dass eine Abschichtung von objektiver und subjektiver Zurechnung Sinn macht. Dies gilt insbesondere bei der so genannten eigenverantwortlichen Selbstgefährdung. In diesem Bereich verwendet die Rechtsprechung Elemente der objektiven Zurechnung, da hier der Gesichtspunkt der subjektiven Vorhersehbarkeit kaum weiterhilft, um zu sachgerechten Ergebnissen zu gelangen[310].

Weiterhin prüft die Rechtsprechung selbst bei erfolgsqualifizierten Delikten in einer Zweiteilung, ob sich objektiv auf der Tatbestandseite die dem Grunddelikt innewohnende Gefahr verwirklicht hat. Dabei fragt sie, ob eine nicht außerhalb allgemeiner Lebenserfahrung liegende Wahrscheinlichkeit für die Realisierung der Gefahr besteht[311]. Dabei muss zur Bestimmung der allgemeinen Lebenserfahrung, soll diese nicht einfach behauptet werden, auf einen objektiven, vom Täter losgelösten Maßstab zurückgegriffen werden. Anschließend wird gefragt, ob der Erfolg subjektiv vorhergesehen werden konnte[312]. Zwar spricht die Rechtsprechung auf der ersten Stufe von einem Ursachenzusammenhang im Sinne einer

[309] Vgl. Wessels/Beulke, Strafrecht AT Rn. 182.
[310] Vgl. nur BGHSt 37, 179 und BGHSt 46, 279 (284).
[311] BGHSt 31, 96 (100).
[312] BGHSt 31, 96 (101).

Adäquanzbetrachtung, allerdings ähnelt die Prüfung durchaus derjenigen der objektiven Zurechnung. Hier kann berechtigt eingewandt werden, dass statt eines vagen Abstellens auf die allgemeine Lebenserfahrung besser gleich ein eigener Gesichtspunkt der objektiven Zurechnung herausgearbeitet werden sollte.

b) Objektive Zurechung beim Outsourcing

Akzeptiert man die Lehre von der objektiven Zurechnung, ist zu untersuchen, ob ein Offenbaren im Sinne des § 203 StGB dem Outsourcer medizinischer Daten objektiv zugerechnet werden kann. Nach dem Ausgeführten ist maßgeblich, ob eine rechtlich relevante Gefahr für einen unbefugten Zugriff Dritter geschaffen worden ist. Durch das Outsourcing wird ein privater Dienstleistungsanbieter in die Datenverarbeitung miteinbezogen. Im weitestgehenden Fall wird die Verarbeitung medizinischer Daten dem Outsourcingnehmer übertragen. Damit bindet der geheimnisverpflichtete Outsourcer einen dienstleistungsanbietenden Outsourcingnehmer in einen exklusiven Vertrauens- und Verantwortungsbereich ein. Von einer rechtlich missbilligten Gefahr kann dann nicht ausgegangen werden, wenn durch diese Einbindung keine Schwachstelle für einen Zugriff Dritter entstanden ist. Anders ausgedrückt darf durch das Heranziehen des privaten IT-Partners keine Exposition der Daten erfolgt sein.

Dies kann dann verneint werden, wenn wirksame Schutzmaßnahmen um die Beziehung zwischen Outsourcer und Outsourcingnehmer gelegt sind, die einen Zugriff Dritter wirksam verhindern. Nur dann kann es in der Beurteilung keinen Unterschied machen, ob der Schweigepflichtige die Daten allein verarbeitet oder Private im Rahmen des Outsourcings heranzieht, wenn er für die Sicherheit verantwortlich bleibt. Dies kann nur angenommen werden, wenn die Schutzmaßnahmen nach dem aktuellen Stand der Technik als wirksam anzusehen sind und ein unbefugter Zugriff durch Dritte auf die medizinischen Daten damit verhindert wird.

Allerdings kann argumentiert werden, dass allein durch das Heranziehen eines privaten Dritten die Möglichkeit potentiellen Missbrauchs erhöht wurde, weil der Kreis der Personen, die in Kontakt mit den Geheimnissen geraten, vergrößert worden ist. Darin könnte man unabhängig von der Intensität der Schutzmaßnah-

men eine erhöhte Gefahr für eine unbefugte Kenntnisnahme sehen. Diese Überlegungen überzeugen nicht. Das Heranziehen eines Dritten kann nicht per se missbilligt werden und gefahrerhöhend wirken. Auch § 203 StGB sieht ein Heranziehen von Gehilfen vor. Das Heranziehen Dritter ist nur dann gefahrerhöhend, wenn im Vergleich ohne das Heranziehen eines Dritten davon ausgegangen werden kann, dass die Gefahr eines unbefugten Zugriffs erhöht wird.

Dabei ist die technische und organisatorische Ausgestaltung von Schutzmaßnahmen sowohl beim Outsourcer als auch beim privaten Dienstleistungsanbieter zu betrachten. Diese Betrachtungsweise ist angezeigt, weil nur dann eine Aussage darüber getroffen werden kann, ob die Gefahr eines unbefugten Zugriffs durch Dritte aufgrund des Heranziehens eines privaten IT-Dienstleistungserbringers erhöht worden ist. Bietet das organisatorisch-technische Gesamtkonzept nach dem aktuellen technischen Stand wirksamen Schutz, dann ist ein dennoch erfolgter unbefugter Zugriff auf sensible Daten dem Geheimnisverpflichteten nicht zurechenbar.

3. Subjektive Zurechnung

Die Schwierigkeiten im Bereich der objektiven Zurechnung liegen darin, objektiv die Art und Intensität von Schutzmaßnahmen zu bestimmen, die erforderlich sind, um eine Gefahrerhöhung auszuschließen. Lehnt man die Lehre von der objektiven Zurechnung mit der Rechtsprechung und Teilen in der Literatur ab, ist die Problematik insgesamt im Bereich des Vorsatzes zu behandeln. Aber auch nach der Lehre der objektiven Zurechnung folgt im Anschluss an die objektive Zurechnung die Prüfung von Vorsatz oder Fahrlässigkeit als Problem subjektiver Zurechnung.

§ 203 StGB sieht nur eine vorsätzliche Begehungsform vor. Unter Vorsatz versteht man den Willen zur Verwirklichung eines Straftatbestandes in Kenntnis all seiner objektiven Tatumstände. Häufig verwendet wird die Kurzformel, dass Vorsatz das Wissen und Wollen der Tatbestandsverwirklichung ist[313]. Der Vorsatz besteht somit aus zwei Komponenten, einer Wissenskomponente und einer Wollenskomponente. Unterschieden werden drei Formen des Vorsatzes: die Absicht

[313] Wessels/Beulke, Strafrecht AT Rn. 203.

(dolus directus 1. Grades), das Wissen (dolus directus 2. Grades) und der bedingte Vorsatz (dolus eventualis).

a) Dolus eventualis und bewusste Fahrlässigkeit

Im Rahmen von Outsourcingvorhaben ist der Fall, dass absichtlich oder wissentlich Gestaltungen gewählt werden, die eine Verletzung von Privatgeheimnissen bedeuten, selten. Wesentlich häufiger und bedeutsamer ist die Frage, ob mit dolus eventualis gehandelt worden ist. Die Voraussetzungen des bedingten Vorsatzes sind umstritten[314]. Im Kern geht es bei dem Streit darum, ob eine Willenskomponente für die Annahme von dolus eventualis erforderlich ist. Damit verknüpft ist das Problem der Abgrenzung von bedingtem Vorsatz und bewusster Fahrlässigkeit, da nach h.M. sowohl dolus eventualis als auch bewusste Fahrlässigkeit in Betracht kommen, wenn der Täter nach seinen Vorstellungen die Tatbestandsverwirklichung konkret für möglich hält[315]. Da fahrlässiges Handeln nicht nach § 203 StGB strafbar ist, kommt der Frage nach der Abgrenzung zwischen dolus eventualis und bewusster Fahrlässigkeit für die strafrechtliche Beurteilung von Outsourcingvorhaben erhebliche Bedeutung zu.

Nach der Rechtsprechung erfordert dolus eventualis sowohl eine Wissens- als auch eine Wollenskomponente. Bedingt vorsätzlich handelt danach, wer die Tatbestandsverwirklichung konkret für möglich hält und die Tatbestandsverwirklichung billigend in Kauf nimmt. Teilweise finden sich auch Formulierungen in der Rechtsprechung, nach denen sich der Täter mit der Tatbestandverwirklichung abfinden muss bzw. einverstanden sein muss[316]. Der Unterschied zur bewussten Fahrlässigkeit wird nach der Rechtsprechung in der Wollenskomponente gesehen. Bei bewusster Fahrlässigkeit vertraut der Täter darauf, dass der Erfolg ausbleibt[317]. Diese Grundposition wird auch von der Lehre zum Teil vertreten, wobei im Einzelnen die Abgrenzung umstritten ist. Teilweise wird die Wissenskomponente betont, teilweise die Wollenskomponente. Eine Mindermeinung stellt sich

[314] Wessels/Beulke, Strafrecht AT Rn. 214 ff.
[315] Tröndle/Fischer, StGB, § 15 Rn. 9.
[316] BGHSt 36, 1; auch in der Literatur findet sich diese Formulierung, vgl. Roxin, Strafrecht AT 1, § 12 Rn. 21 bis 31; Jescheck/Weigend, Strafrecht AT, § 29 III 3a; Kühl, Strafrecht AT, 5/84f, Joecks, StGB, § 15 Rn. 21.
[317] Wessels/Beulke, Strafrecht AT Rn. 216.

demgegenüber auf den grundsätzlichen Standpunkt, dass für bedingten Vorsatz keine Wollenskomponente erforderlich ist[318].

Jenseits dieser Auffassungen stellt sich die Schwierigkeit der Feststellung von dolus eventualis im Prozess. Naturgemäß sind Fragen des inneren Tatbestandes nur schwer dem Beweis zugänglich. Da bedingter Vorsatz und bewusste Fahrlässigkeit im Wissensbereich sich überschneiden, stellt die Rechtsprechung hohe Anforderungen an die Begründung für die tatsächliche Annahme von dolus eventualis[319]. Geboten sei eine Gesamtschau aller objektiven und subjektiven Tatumstände. Dabei kann auch die Rechtsprechung nicht umhin, objektive Tatumstände für die Feststellung als Beweisanzeichen heranzuziehen und daraus auf das Vorliegen bzw. Nicht-Vorliegen von dolus eventualis zu schließen.

b) Vorliegen von dolus eventualis

Für das Outsourcing medizinischer Daten ist somit auf die Umstände einzugehen, die eine Aussage über das Vorliegen bedingten Vorsatzes ermöglichen. In der Praxis wird es dabei vor allem um Schutzmaßnahmen hinsichtlich der unbefugten Kenntnisnahme der medizinischen Daten gehen. Ergreift der Outsourcer aus Kostengründen keine Schutzmaßnahmen, um die sensiblen Daten gegen den Zugriff Dritter zu schützen, liegt die Annahme von dolus eventualis nahe. Dies gilt insbesondere, wenn im Rahmen des Outsourcings potentiell eine Vielzahl von Außenstehenden mit den Daten in Berührung kommen können. Dies ist etwa dann der Fall, wenn eine ungeschützte Anbindung an das Internet erfolgt oder die Daten planmäßig einen hohen Grad an Umsatz und Mobilität besitzen und bei der Übermittlung dieser Daten in unsicheren Netzen keine Verschlüsselung erfolgt. Ein Untätigbleiben des Outsourcers wird regelmäßig zu der Schlussfolgerung führen, dass der Outsourcer sich mit der Möglichkeit einer Kenntnisnahme durch Dritte abgefunden hat und somit mit dolus eventualis handelt.

Dies gilt auch dann, wenn nicht der Outsourcer, sondern der anbietende IT-Dienstleister keine Schutzmaßnahmen getroffen hat und der Outsourcer dies weiß. Dabei kann sich der Outsourcer nicht damit verteidigen, dass er auf die Aussage

[318] Puppe, in: NK StGB, § 15 Rn. 88 ff.
[319] Vgl. BGHSt 46, 30, (35); 46, 53, (59), BGH, NStZ 1984, S. 19; BGH NStZ 2001, S. 475.

des IT- Dienstleisters, dass Schutzmaßnahmen nicht erforderlich seien, vertraut hat. Die Erfüllung der Schweigepflicht kann nicht Anderen zur eigenverantwortlichen Erfüllung übertragen werden, da die Schweigepflicht untrennbar mit einer Person verbunden ist. Daran ändert auch die Ausdehnung der Schweigepflicht auf berufsmäßig tätige Gehilfen nichts. Hierdurch wird der Schweigepflichtige nicht entlastet. Die Vorschrift will nur verhindern, dass durch die Einbeziehung eines Gehilfen Strafbarkeitslücken dadurch entstehen, dass der Gehilfe eigenmächtig Informationen an außenstehende Dritte weitergibt. Die Ausdehnung der Schweigepflicht auf die Gehilfen erfolgt im Interesse des Geheimnisträgers als Ausgleich für ein in bestimmten Bereichen notwendiges arbeitsteiliges Vorgehen. Sie verfolgt nicht den Zweck, den Schweigepflichten von Handlungspflichten zu entbinden. Vielmehr hat der Schweigepflichtige seinen Gehilfen zu überwachen und zu kontrollieren. Auch wenn Personen des IT-Dienstleistungsunternehmens Gehilfenstatus zukommt, bleibt der primär Schweigeverpflichtete für Schutzmaßnahmen verantwortlich. Weiß der Outsourcer also, dass keine Schutzmaßnahmen getroffen sind und bleibt er untätig, wird darin regelmäßig ein Abfinden mit der Möglichkeit der Kenntnisnahme zu erblicken sein.

Schwieriger ist die Situation zu beurteilen, bei der Schutzmaßnahmen zwar ergriffen worden sind, diese sich aber als unwirksam erweisen. Hier ist auf der einen Seite zu berücksichtigen, dass abhängig von der Konzeption des Outsourcingprojekts der Verantwortungskreis mehr oder weniger erweitert wird. Das Heranziehen weiterer Personen bedeutet eine potentielle Schnittstelle für einen unbefugten Zugriff durch Dritte oder eine missbräuchliche Weitergabe an Dritte. Andererseits ist auch ohne ein Outsourcing im analogen Bereich ein unbefugter Zugriff Dritter möglich. Zu denken ist beispielsweise an einen Einbruch in Räumlichkeiten, in denen unverschlossen medizinische Daten aufbewahrt werden. Weiterhin ist an das Versenden der medizinischen Daten per einfacher Post zu denken. In beiden Fällen können Dritte unbefugt Zugriff auf die Daten nehmen. Mit dieser durch den Schweigepflichtigen nicht beherrschbaren Möglichkeit muss der Schweigepflichtige aber nicht rechnen. Dies wird allein durch das Verhalten Dritter gesteuert. Zudem ist die Information verkörpert, lokalisiert und nicht sichtbar in einem umschlossenen Raum. Dies sind objektive Erschwernisse, deren unbefugte Über-

windung eine Straftat darstellt[320]. In solchen Fällen kann der Schweigepflichtige von einem hinreichenden Schutz ausgehen. Einen absoluten Schutz vor solchen punktuellen Gefahren gibt es nicht und kann auch nicht gefordert werden. Die Annahme von dolus eventualis scheidet daher regelmäßig aus. Übertragen auf die Beurteilung von Outsourcingvorhaben bedeutet dies, dass zu prüfen ist, ob mit den Schutzvorkehrungen gleich wirksame Erschwernisse geschaffen worden sind, so dass der Outsourcer mit einem unbefugten Zugriff auf die Daten nicht rechnen muss, weil sich der Zugriff als unbeherrschbares Ereignis darstellt. Dafür muss, abhängig von der eingesetzten Technologie, die objektive Wirksamkeit der Schutzmaßnahmen betrachtet werden. Bewirken die Schutzmaßnahmen, dass zu erwartende Zugriffsversuche wirksam abgehalten werden, ist ein dennoch im Einzelfall erfolgter Zugriff als unerwartet zu qualifizieren.

Dies gilt aber nur, wenn ein Einbruch in der digitalen Welt vergleichbar dem Einbruch in der analogen Welt erschwert ist. Setzt der Outsourcer in Zusammenarbeit mit dem IT-Dienstleistungsanbieter eigene oder fremde IT ein, ist es ihm zumutbar, für die Sicherheit der eingesetzten Technik zu sorgen. Insofern kann der Outsourcer sich nicht allein auf vertragliche Verhaltensge-/verbote oder persönliche Verschwiegenheitsverpflichtungen beschränken, sondern muss jedenfalls auf der Technikebene Schutzvorkehrungen ansetzen lassen. Verschafft er sich die dafür notwendige Sachkunde über ein IT-Dienstleistungsunternehmen, hat er vertraglich sicherzustellen und zu überprüfen, dass ein wirksamer Schutz gegen unbefugte Zugriffe eingesetzt und aufrechterhalten wird.

Beherrschbar und zumutbar für den Outsourcer ist eine Ausrichtung an anerkannten aktuellen Sicherheitsstandards, deren Befolgen ein objektiv wirksames Hindernis für einen unbefugten Zugriff darstellt. Nicht erforderlich ist, dass der Outsourcer eine bestimmte Schutztechnik einsetzt oder die größtmögliche Intensität in einer Schutzmaßnahme wählt. Maßgeblich ist, ob der Outsourcer nach der Gesamtkonzeption davon ausgehen darf, dass das eingesetzte Verfahren wirksam einen Zugriff Dritter verhindert.

[320] In Betracht kommen insbesondere §§ 123, 303, 202, 206 StGB.

Einzubeziehen sind nach der Rechtsprechung alle objektiven und subjektiven Gesichtspunkte im konkreten Einzelfall[321]. Dabei muss als Grundsatz gelten, dass je stärker die Daten dem potentiellen Kontakt mit außen stehenden Personen ausgesetzt werden, desto intensiver müssen die Schutzvorkehrungen sein. In der Bewertung der Wirksamkeit der Schutzmaßnahmen für den Outsourcer kann eine Auditierung[322] durch eine unabhängige Stelle ein zusätzlicher Aspekt sein, der gegen dolus eventualis spricht. Ein virtuelles Einbrechen ist trotz wirksamer Sicherungsvorkehrungen niemals völlig auszuschließen. Ein dennoch erfolgtes Hacking der Daten wäre vom Outsourcer nicht beherrschbar und im Übrigen tatbestandlich von § 202a StGB erfasst. In solchen Fällen verbietet sich regelmäßig die Annahme von dolus eventualis.

Dolus eventualis kommt aber auch dann in Betracht, wenn in einem wirksamen Schutzkonzept Schwachstellen auftreten, die der Verantwortliche erkennen kann und die nicht behoben werden. Solche Schwachstellen können auf der technischen Ebene auftreten, aber auch auf der organisatorisch-personellen Ebene. Denkbar ist beispielsweise das Auftreten von Sicherheitslücken in Computersystemen, aber auch der wiederholte Verstoß gegen vertragliche Verhaltensge-/verbote. Die Annahme von dolus eventualis und nicht nur von Fahrlässigkeit liegt insbesondere dann nahe, wenn die Sicherheitslücken offensichtlich sind und sich der Verantwortliche hinsichtlich des Auftretens solcher Sicherheitslücken leicht über öffentlich zugängliche Quellen unterrichten kann. Hinsichtlich personellen Fehlverhaltens gilt, dass dolus eventualis nahe liegt, wenn der Verantwortliche von wiederholtem Fehlverhalten hört, aber den Vorkommnissen nicht nachgeht.

Schließlich ist denkbar, dass die Wahl der Schutzmaßnahmen die Annahme von dolus eventualis nahe legt. Dies kann dann der Fall sein, wenn der Outsourcer beispielsweise aus Kostengründen auf technische Schutzmaßnahmen, die unmittelbar an der Datenebene ansetzen, verzichtet und stattdessen vertragliche Verbote einsetzt. Sind Daten digitalisiert und werden diese Daten zwischen Outsourcer und IT-Dienstleister ausgetauscht, kann ein Versagen oder ein Fehler in der Technik dazu führen, dass Daten für Dritte zugänglich werden. Der Vorteil des Einsatzes digitaler Technik korreliert mit möglichen neuen Gefahren durch die Technik.

---

[321] Tröndle/Fischer, StGB, § 15 Rn. 10a.
[322] Zum Audit umfassend Weichert, MedR 2003, S. 674ff.

Vertragliche Abreden, die für einen Schutz auf personeller Ebene sorgen, können Schwächen in der technischen Konzeption nicht ausgleichen, da sie nicht auf der Ebene ansetzen, auf der die Gefahr veranlasst worden ist. Erst wenn auf technischer Ebene ein wirksames Schutzniveau aufgebaut ist, können vertragliche Absprachen dieses Schutzniveau absichern. Kann der Outsourcer damit rechnen, dass das technische Schutzkonzept keinen wirksamen Schutz bietet und ergreift er dennoch nur personelle Schutzvorkehrungen, dann ist dies ein Gesichtspunkt, der für dolus eventualis spricht.

Im Umkehrschluss wird dolus eventualis regelmäßig zu verneinen sein, wenn der Outsourcer in Kooperation mit dem IT-Dienstleister ein wirksames technisches Schutzkonzept einsetzt und dieses durch arbeitsrechtliche Verbote sowie eine Belehrung der Mitarbeiter über die rechtlichen Konsequenzen ergänzt wird. Die Belehrung der Mitarbeiter über die Schweigepflicht sollte klar und konkret auf die Funktion des Mitarbeiters im Verarbeitungszusammenhang bezogen sein, damit der Mitarbeiter sich über Bedeutung und Tragweite der Schweigepflicht bewusst wird. Nach einer solchen zweckmäßigerweise schriftlichen Belehrung darf der Outsourcer regelmäßig davon ausgehen, dass der Mitarbeiter keine sensible Daten unbefugt an Außenstehende weitergibt. Mit der Möglichkeit, dass ein Mitarbeiter sich dennoch bewusst über ein Verbot hinwegsetzt und das Risiko einer Sanktion eingeht, muss der Outsourcer ohne besondere Anhaltspunkte nicht ernsthaft rechnen.

Schwierig ist die Frage zu beantworten, wann der Outsourcer davon ausgehen darf, dass ein wirksamer Schutz nach der Konzeption des Outsourcingvorhabens gegeben ist. Dies lässt sich nicht allgemein beantworten, sondern ist im Einzelfall für das jeweilige Outsourcingvorhaben anhand der konkreten technischen, organisatorischen und personellen Schutzmaßnahmen zu bestimmen. Generell kann aber festgehalten werden, dass je intensiver die Schutzmaßnahmen gestaltet werden, desto eher wird man davon ausgehen können, dass ein wirksamer Schutz gegeben ist.

Dabei ist eine Orientierung an anerkannten IT-Sicherheitsregeln sowie an Richtlinien und Empfehlungen zum Datenschutz und zur Datensicherheit regelmäßig geeignet, dem Vorwurf vorsätzlichen Handelns zu begegnen. Bei einer Ausgestal-

tung des Outsourcings als Datenverarbeitung im Auftrag sind die Sicherheits- und Kontrollmaßnahmen nach § 11 Abs. 5 BDSG zu beachten. Hier wird ein wissentliches Außerachtlassen den Vorwurf bedingt vorsätzlichen Handelns begründen können. Außerhalb von § 11 Abs. 5 BDSG bedeutet aber die Entscheidung für oder gegen bestimmte Schutz- oder Sicherheitsrichtlinien/-empfehlungen bzw. -standards nicht zwangsläufig, dass von einem unwirksamen Schutz sensibler Daten ausgegangen werden muss. Dies ist nur dann anzunehmen, wenn infolge der Versäumnisse mit einem Zugriff Dritter zu rechnen ist. Nicht erforderlich ist, das technisch optimale Schutzkonzept zu verwenden. Ausreichend ist, wenn aus objektiver Sicht die Wahl für ein Schutz- und Sicherheitskonzept einen wirksamen Schutz gegen unbefugte Zugriffe Dritter erwarten lässt. Ist dies offensichtlich und für den Outsourcer erkennbar nicht der Fall, wird man regelmäßig dolus eventualis annehmen können.

VIII. Befugnis zum Offenbaren

Bedeutet ein Outsourcingvorhaben ein „Offenbaren“ i.S.v. § 203 StGB, ist von Interesse, welche weiteren Voraussetzungen für eine Strafbarkeit vorliegen müssen. § 203 StGB stellt nicht jedes Offenbaren unter Strafe, sondern nur ein unbefugtes Offenbaren. Vor dem Hintergrund, dass ein Outsourcer zur Kostenreduktion durch das Outsourcing möglichst eine Organisationsentlastung verbunden mit einer möglichst weitgehenden Aufgabenerledigung durch den IT-Dienstleister, erzielen will stellt sich die Frage, wann ein Offenbaren unbefugt ist. Unbefugt ist das Offenbaren, wenn es nicht durch Offenbarungsrechte oder -pflichten oder durch den Willen des Betroffenen gedeckt ist[323].

Umstritten ist die Einordnung des Deliktmerkmals „unbefugt“ im Deliktsaufbau[324]. Nach wohl h.M. schließt eine Befugnis zum Offenbaren die Rechtswidrigkeit aus[325]. Begründet wird dies damit, dass das in § 203 StGB vertypte Unrecht nicht durch das Merkmal „unbefugt“ beeinflusst wird. Das Offenbaren sensibler Tatsachen bedeutet für sich einen erheblichen Interessensverlust und reicht zur

[323] Vgl. Lenckner, in: Schönke/Schröder, StGB, § 203 Rn. 21.
[324] Eingehend zum Deliktsmerkmal „unbefugt“ Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, S. 20 ff.
[325] Tröndle/Fischer, StGB, § 203 Rn. 31; a.A. wohl Lackner/Kühl, StGB, § 203 Rn. 18, Vor § 201 Rn. 2; für eine „Doppelfunktion“ Lenckner, in: Schönke/Schröder, StGB, § 203 Rn. 21.

Unrechtsbegründung aus[326]. Danach hat das Merkmal „unbefugt“, wie auch in den §§ 201, 202a, 204, 206 StGB, nur die Funktion, auf Vorschriften besonders hinzuweisen, die ausnahmsweise das Verhalten rechtfertigen und damit als befugt erscheinen lassen können. Nach a.A. hat das Merkmal „unbefugt“ tatbestandsbegrenzende Wirkung[327]. Hiernach scheitert eine Strafbarkeit nach § 203 StGB im Fall von bestehenden Offenbarungsbefugnissen bereits am fehlenden Tatbestand. Schließlich nimmt eine weitere Ansicht an, dass das Merkmal „unbefugt“ eine Doppelfunktion hat, also sowohl den Tatbestand begrenzt als auch ein allgemeines Rechtswidrigkeitsmerkmal darstellt[328]. In den Fällen einer Zustimmung des Betroffenen zum Offenbaren soll bereits der Tatbestand entfallen, während andere Offenbarungsrechte/-pflichten die Rechtswidrigkeit entfallen lassen. Hier wird also die Einordnung des Merkmals „unbefugt“ mit der Einordnung der Zustimmung durch den Betroffenen verknüpft. Das Merkmal „unbefugt“ verweist in diesen Fällen auf das Fehlen eines tatbestandsausschließenden Einverständnisses.

Begründet wird dies zum einen mit dem durch § 203 StGB geschützten Rechtsgut. Da bei § 203 StGB der Wille des Anvertrauenden konstitutiv für die Existenz des Rechtsguts ist, fehlt es bereits an einem rechtsgutverletzenden Akt[329]. Dem entspricht eine Einordnung des Merkmals „unbefugt“ als Tatbestandsmerkmal am Besten. Für diese Ansicht wird auch die Fassung des § 18 Abs. 2 HS 1 BNotO angeführt, wonach die Pflicht zur Verschwiegenheit entfällt, wenn die Beteiligten Befreiung hiervon erteilen[330]. Als weiteres Argument wird insbesondere von *Jähnke* angeführt, dass der Geheimhaltungswille konstituierendes Element des Geheimnisbegriffs ist[331]. Eine Zustimmung würde eine ganze oder teilweise Aufgabe des Willens zur Geheimhaltung bedeuten. Dadurch wird die Ebene des Tatbestandes betroffen. Gibt die willensgetragene Zustimmung eine Befugnis zum Offenbaren, muss auch die Einordnung des Merkmals „unbefugt“ auf der Ebene des Tatbestandes erfolgen[332]. Dieser Auffassung wird zum Teil zugestimmt, aber mit der Einschränkung, dass eine Zustimmung nur dann den Tatbestand aus-

[326] Rogall, NStZ 83, S. 16; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 119.
[327] Lackner/Kühl, StGB, Vor § 201 Rn. 2.
[328] Cierniak, in: Münchener Kommentar StGB § 203 Rn. 53; Lenckner, in: Schönke/Schröder StGB, § 203 Rn. 21; Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, S. 40.
[329] Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, S. 40.
[330] Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 54.
[331] Jähnke, in: Leipziger Kommentar StGB, 10. Auflage, § 203 Rn. 70.
[332] Jähnke, in: Leipziger Kommentar StGB, 10. Auflage, § 203 Rn. 56.

schließt, wenn der Betroffene mit der Einwilligung auf die Geheimhaltung insgesamt verzichtet[333].

Dieser rechtsdogmatische Streit hat in der Mehrzahl der Fälle keinen Einfluss auf das Ergebnis der strafrechtlichen Beurteilung des in Frage stehenden Verhaltens. Praktische Bedeutung kann die Frage aber vor allem dann haben, wenn der Täter irrtümlich von einer Zustimmung ausgeht. Dabei kann noch die Frage der Anstifterstrafbarkeit hinzutreten, wenn der Haupttäter irrtümlich von einer vorgespiegelten Zustimmung ausgeht.

Fehlvorstellungen über Merkmale „rechtswidrig", „unbefugt" etc., die zum Tatbestand zu zählen sind, wie etwa bei den §§ 242, 253, 263 StGB, führen regelmäßig zu einem Tatbestandsirrtum nach § 16 StGB, können aber auch einen Verbotsirrtum nach § 17 StGB darstellen. Wird das Merkmal „unbefugt" als Tatbestandsmerkmal angesehen, so wäre daher bei einer irrigen Annahme eines tatbestandlichen Einverständnisses ein Tatbestandsirrtum anzunehmen, da der Täter in der Regel tatsächliche Umstände annimmt, die ihm die Erfassung des rechtlich-sozialen Bedeutungsgehalts des Tatumstandes verschließen[334]. Er kann dann nicht erkennen, dass er „unbefugt" i. S. v. § 203 StGB handelt. Lediglich wenn bei richtig erkannten sachlichen Grundlagen eine irrige Bewertung durch den Täter erfolgt, kann ein Verbotsirrtum i. S. v. § 17 StGB angenommen werden, für den es auf die Frage der Vermeidbarkeit ankommt. In Konsequenz dazu wird regelmäßig eine Strafbarkeit nach § 203 StGB ausscheiden. Für einen Teilnehmer würde das nach dem Akzessorietätsgrundsatz des § 26 StGB ebenfalls Straffreiheit bedeuten, da keine beteiligungsfähige rechtswidrige Haupttat vorhanden ist.

Wird hingegen die Voraussetzung „unbefugt" als Merkmal der Rechtswidrigkeit angesehen, ist zwischen einem Erlaubnistatbestandsirrtum und einem Verbotsirrtum nach § 17 StGB zu differenzieren. Ein Erlaubnistatbestandsirrtum ist anzunehmen, wenn der Täter irrig Tatumstände annimmt, die, wenn sie tatsächlich vorliegen würden, das Verhalten gerechtfertigt wäre. Hier irrt der Täter über die sachlichen Voraussetzungen eines anerkannten Rechtfertigungsgrundes[335]. Hinge-

[333] So Tröndle/Fischer, StGB, § 203 Rn. 31.
[334] Wessels/Beulke, Strafrecht AT Rn. 455.
[335] Wessels/Beulke, Strafrecht AT Rn. 467; vgl. zu einem möglichen Irrtum eines Arztes über seine Befugnis zum Offenbaren von Patientengeheimnissen OLG Koblenz vom 28. April 1994,

gen handelt es sich um einen Verbotsirrtum, wenn der Täter die für die Tat maßgebliche Verbotsnorm nicht kennt oder falsch deutet und deshalb sein Verhalten für rechtlich erlaubt hält. Ebenfalls zu einem Verbotsirrtum führt das auf einem Irrtum beruhende Fehlen der Unrechtseinsicht.

Bei einem Erlaubnistatbestandsirrtum ist nach der überwiegenden und zutreffenden Meinung in der Literatur analog § 16 StGB der Schuldvorsatz ausgeschlossen, so dass nur eine Bestrafung wegen fahrlässiger Begehung in Frage kommt[336]. Bezogen auf § 203 StGB würde dies bedeuten, dass ein Täter straflos bleiben würde, da bei § 203 StGB nur vorsätzliches Handeln unter Strafe gestellt ist. Allerdings käme eine Strafbarkeit des Teilnehmers in Betracht, da trotz des Erlaubnistatbestandirrtums eine vorsätzliche und rechtswidrige Tat vorliegt. Lediglich der Schuldvorwurf würde entfallen.

Liegt hingegen ein Verbotsirrtum vor, kommt es nach § 17 StGB darauf an, ob der Irrtum vermieden werden konnte. Bei Vermeidbarkeit kann eine Strafmilderung nach § 49 Abs. 1 StGB erfolgen. Ein solcher Irrtum wird auf der Ebene der Strafzumessung berücksichtigt. Unterliegt der Täter gleichzeitig einem Erlaubnistatbestandsirrtum und einem Verbotsirrtum, wird dieser Sachverhalt insgesamt nach § 17 StGB, also nach den Regeln zum Verbotsirrtum, behandelt. Ein solcher doppelter Irrtum kann vorliegen, wenn der Täter über die sachlichen Voraussetzungen eines Rechtfertigungsgrundes irrt und zusätzlich die Reichweite des irrig angenommenen Rechtfertigungsgrundes verkennt[337].

Nach dem Ausgeführten zeigt sich, dass von der Einordnung des Merkmals „unbefugt“ hinsichtlich des Outsourcings medizinischer Daten durchaus die Frage der Strafbarkeit abhängen kann. Für eine Entscheidung muss eine Auseinandersetzung mit den Ansichten hinsichtlich ihrer Überzeugungskraft erfolgen. Auf den ersten Blick überzeugend ist das Argument von *Jähnke*, wonach der Geheimhal-

---

Az: 1 Ws 95/94. Hier ging das Gericht davon aus, dass das Merkmal unbefugt auf der Rechtfertigungsebene Bedeutung erlangt.

[336] Tröndle/Fischer, StGB, § 16 Rn. 19; zu dem gleichen Ergebnis gelangt die Rechtsprechung, Wessels/Beulke, Strafrecht AT Rn. 470; wegen der Konsequenz der Straffreiheit für den Teilnehmer sind Lösungen, die nicht auf der Schuldebene bleiben, abzulehnen, vgl. zu den unterschiedlichen Meinungen innerhalb der Schuldtheorie Wessels/Beulke, Strafrecht AT Rn. 427ff.

[337] Mit einem solchen Irrtum beim externen Archivieren von medizinischen Daten hatte sich das OLG Düsseldorf u.a. zu befassen, OLG Düsseldorf CR 1997, S. 536. Dabei hat das OLG die vermeintliche Zustimmung und das Merkmal unbefugt als Rechtfertigungsproblem angesehen.

tungswille konstituierendes Element des Geheimnisbegriffs ist. Dies ist anzuerkennen. Dazu ist es konsequent, anzunehmen, dass auch ein mutmaßlicher Geheimhaltungswille ausreicht.

Diese Erkenntnis zwingt aber bei näherer Betrachtung nicht zu der Annahme, dass das Merkmal „unbefugt“ zum Tatbestand zu zählen ist. Eine glatte Implementierung der Zustimmung in den Tatbestand des § 203 StGB gelingt nicht. Schwierigkeiten bereitet schon der Fall, in dem der Betroffene nicht insgesamt auf die Geheimhaltung verzichtet, sondern nur für bestimmte Situationen, unter besonderen Voraussetzungen oder mit begrenzter Reichweite. Soll das Geheimnis dann als nur teilweise geheim angesehen werden?.

Weiterhin ist fraglich, wie sich Willensmängel beim Verzichtenden auswirken. Sieht man das Einverständnis als tatbestandsausschließende Befugnisgrundlage an, muss man maßgeblich auf die Freiwilligkeit abstellen und zu einer Befugnis zum Offenbaren auch bei Willensmängeln kommen. Angesichts des hohen Ranges des durch § 203 StGB geschützten Rechts auf informationelle Selbstbestimmung begegnet diese Konsequenz Bedenken und erscheint nicht sachgerecht. Ein Ausweg dazu besteht darin, das tatbestandliche Einverständnis weitgehend denselben Wirksamkeitsvoraussetzungen zu unterwerfen wie die rechtfertigende Einwilligung[338]. Damit rückt man aber von der tatbestandlichen Verknüpfung von Wille und Handlung ab und nähert sich der Bedeutung der Zustimmung als Preisgabe zur Disposition stehender Individualrechtsgüter. Weiterhin ergeben sich Reibungen mit der tatbestandsausschließenden Wirkung eines Einverständnisses, wenn mutmaßlich kein Geheimhaltungswille besteht. Soll dann ein mutmaßliches Einverständnis[339] angenommen werden oder sind diese Fälle durch eine mutmaßliche Einwilligung gerechtfertigt?

Dies deutet darauf hin, dass der Geheimhaltungswille besser unabhängig vom Merkmal „unbefugt“ zu verstehen ist. Die willensgetragene Einräumung einer

[338] In diese Richtung kann die Entscheidung des OLG Karlsruhe verstanden werden, nach der ein „wirksames Einverständnis i.S.v. § 203 Abs. 1 Nr. 1 StGB“ voraussetzt, dass der Einwilligende eine im Wesentlichen zutreffende Vorstellung davon hat, worin er einwilligt und die Bedeutung und Tragweite seiner Entscheidung zu überblicken vermag, vgl. OLG Karlsruhe NJW 1998, S. 832.

[339] Näher zu dem Begriff des mutmaßlichen Einverständnisses Ludwig/Lange, JuS 2000, S. 446.

Befugnis[340] durch den Geheimnisträger kann durchaus vom Geheimhaltungswillen unterschieden werden. Der Geheimhaltungswille muss nicht darauf bezogen sein, einer anderen Person eine Dispositionsbefugnis einzuräumen. Vielmehr erschöpft sich der Geheimhaltungswille grundsätzlich dem Inhalt nach darin, eine Information der geschützten Privatsphäre zuzuordnen. Nur insoweit ist er als konstitutiv für das Tatbestandsmerkmal „Geheimnis“ in § 203 StGB anzusehen. Wenn ein Geheimnisträger seine Geheimnisse nach außen trägt und damit zu erkennen gibt, dass er sie nicht seinem Privatbereich zuordnet, dann kann begrifflich schon nicht von Geheimnissen gesprochen werden. Eine Befugnis, über die personenbezogene Information zu verfügen, ist damit nicht erteilt.

Erst wenn beim Geheimnisträger der weitergehende Wille hinzutritt, im Bewusstsein seines grundsätzlich geschützten Privatgeheimnisses anderen in bestimmten Situationen unter grundsätzlicher Weitergeltung des Selbstbestimmungsrechts das Recht, über bestimmte personenbezogene Informationen zu verfügen, einzuräumen, ist die Ebene der Befugnis betroffen. Dann steht aber nicht so sehr die Freiwilligkeit im Vordergrund, sondern eine selbstverantwortete Einschränkung des Dispositionsrechts nach einer individuellen Abwägung. Dies ist vorzugswürdig und sachgerecht auf der Stufe der Rechtswidrigkeit einzuordnen. Es geht nicht um bloße Mitteilung, sondern um Ermächtigung zur Verfügung. Einen solchen interpersonalen Aspekt hat der informationsbezogene und damit objektbezogene Geheimhaltungswille nicht. Insofern spricht der Geheimhaltungswille als Bestandteil des Geheimnisbegriffs nicht dafür, das Merkmal „unbefugt“ als Tatbestandsmerkmal zu betrachten, sondern erschöpft sich in der Gestaltung des Geheimnisbegriffs.

Als Zwischenergebnis bleibt festzuhalten, dass die Befugnis aufgrund einer Zustimmung mit den übrigen gesetzlichen Offenbarungsbefugnissen als Rechtfertigungsgrund zu begreifen ist und das Merkmal unbefugt insgesamt der Rechtswidrigkeitsebene zuzuordnen ist.

[340] Zur Verfügungsberechtigung, die nach h.M. allein beim Geheimnisträger liegt, vgl. Lenckner, in: Schönke/Schröder, StGB, § 203 Rn. 23.

1. Einzelne Offenbarungsbefugnisse

Einzelne Offenbarungsbefugnisse können sich aus Gesetz oder Gewohnheitsrecht ergeben[341]. Als Offenbarungsbefugnisse, die für das Outsourcing medizinischer Daten in Betracht zu ziehen sind, kommen Bestimmungen aus dem allgemeinen Datenschutzrecht, dem bereichsspezifischen Datenschutzrecht, dem Informations- und Kommunikationsrecht und dem Sozialrecht in Betracht. Weiterhin ist an den rechtfertigenden Notstand nach § 34 StGB, an die Grundsätze über die Abwägung widerstreitender Pflichten und Interessen sowie die Wahrnehmung berechtigter Interessen nach § 193 StGB zu denken. Schließlich kommt eine Befugnis kraft Zustimmung in Betracht. Im Folgenden soll untersucht werden, ob einzelne Offenbarungsbefugnisse einen tauglichen strafrechtlichen Erlaubnissatz hinsichtlich des Outsourcings medizinischer Daten darstellen. Eine mögliche Erlaubnis kraft Zustimmung soll erst nach den einzelnen anderen möglichen Rechtfertigungsgründen geprüft werden.

2. Bundesdatenschutzgesetz

Mögliche Rechtfertigungsgründe könnten im Bundesdatenschutzgesetz enthalten sein. Rechtfertigungsgründe sind nicht beschränkt auf das Strafgesetzbuch, sondern sind grundsätzlich der gesamten Rechtsordnung zu entnehmen[342]. Dies ergibt sich aus dem Grundsatz der Einheit der Rechtsordnung und dem sich daraus ableitenden Verbot der Widersprüchlichkeit der Rechtsordnung[343]. Hiernach darf ein außerhalb des Strafrechts als rechtmäßig bezeichnetes Verhalten nicht innerhalb des Strafrechts als rechtswidrig gelten, außer zwingende sachliche Unterschiede der Rechtsgebiete rechtfertigen eine unterschiedliche Bewertung. Auch gilt der Grundsatz der Einheit der Rechtsordnung nur, soweit gleiche Sachverhalte geregelt sind.

Eindeutig ist die Qualifizierung als strafrechtlicher Rechtfertigungsgrund, wenn in Normen des Strafrechts explizit geregelt ist, dass unter bestimmten Voraussetzun-

---

[341] Vgl. zu den Rechtsquellen Baumann/Weber/Mitsch, Strafrecht AT, S. 322ff.; Maurach/Zipf, Strafrecht AT, S. 343ff.
[342] Tröndle/Fischer, StGB, Vor § 32 Rn. 2.
[343] Lenckner, in: Schönke/Schröder, StGB, Vorb. §§ 32 Rn. 27; Roxin, Strafrecht AT 1, § 14 Rn. 30ff.; Maurach/Zipf, Strafrecht AT, S. 344.

gen ein Verhalten, das den Tatbestand eines Strafgesetzes erfüllt, nicht rechtswidrig ist. Beispielsweise spricht § 32 StGB davon, dass derjenige, der eine Tat begeht, die durch Notwehr geboten ist, nicht rechtswidrig handelt. Denkbar ist aber auch, dass eine Norm nicht ausdrücklich davon spricht, dass ein Verhalten gerechtfertigt ist, eine Auslegung aber die rechtfertigende Wirkung ergibt[344]. Dies könnte bei den §§ 11, 16, 28 BDSG der Fall sein.

§ 11 BDSG enthält eine Regelung zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. Mittelbar kann § 11 BDSG Bedeutung für den Gehilfenstatus und das Merkmal Offenbaren erlangen. In § 16 BDSG ist für den Bereich der Datenverarbeitung der öffentlichen Stellen die Zulässigkeit einer Datenübermittlung an nicht-öffentliche Stellen geregelt. Für den Bereich der Datenverarbeitung der nicht-öffentlichen Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen enthält § 28 BDSG Regelungen zur Zulässigkeit einer Datenübermittlung an Dritte.

a) Anwendungsbereich

Eine Rechtfertigung nach Vorschriften des Bundesdatenschutzgesetzes kommt nur in Betracht, soweit das BDSG anwendbar ist. Durch Gesetz vom 18.05.2001 ist der persönliche Anwendungsbereich auf Private ausgedehnt worden. Die entsprechende Regelung findet sich in § 1 Abs. 2 Nr. 3 BDSG. Daneben gilt das Bundesdatenschutzgesetz für öffentliche Stellen des Bundes und der Länder, § 1 Abs. 2 Nr. 1 und 2 BDSG. Für öffentliche Stellen der Länder gilt dies aber nur, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt, § 1 Abs. 2 Nr. 2 lit. a und b BDSG. Somit werden unmittelbar vom BDSG niedergelassene Ärzte, Krankenhäuser in privater Trägerschaft, Krankenhäuser, die dem Bund zugeordnet werden und Unternehmen der privaten Kranken-, Unfall-, Lebensversicherung oder privatärztliche Verrechnungsstellen erfasst. Hinsichtlich der durch die Länder oder Kommunen betriebenen Krankenhäuser oder öffentlich-rechtlichen Versicherungen ist wegen § 2 Abs. 4 BDSG in der Regel nicht das BDSG anwendbar, da zu-

[344] BSG NJW 1986, S. 1574.

meist eigene Regelungen in dem allgemeinen Datenschutzrecht der Länder bzw. im bereichsspezifischen Datenschutzrecht der Länder vorhanden sind.

Eine weitere Einschränkung enthält § 1 Abs. 3 S. 1 BDSG, wonach andere auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwendende Rechtsvorschriften des Bundes dem BDSG vorgehen. Nach § 1 Abs. 3 S. 2 BDSG bleibt die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt. Schließlich ist das Bundesdatenschutzgesetz nur bei personenbezogenen Daten anwendbar. Ist der Personenbezug aufgehoben, entfällt die sachliche Anwendbarkeit des Bundesdatenschutzgesetzes.

b) Geltung datenschutzrechtlicher Erlaubnissätze für § 203 StGB

Ist damit der Anwendungsbereich des BDSG umrissen, stellt sich die Frage, ob Normen des Bundesdatenschutzgesetzes, die datenschutzrechtlich Befugnisse verleihen, Rechtfertigungsgründe für das Strafrecht sein können. Grundsätzlich haben Strafrecht und Datenschutzrecht hinsichtlich des Geheimnisschutzes unterschiedliche Voraussetzungen und Strukturen, so dass von einer Parallelgeltung ausgegangen werden kann. Eine solche Parallelgeltung wird auch in weiten Teilen der Literatur angenommen[345]. Damit ist aber nicht gesagt, dass sich die beiden Bereiche nicht im Einzelfall beeinflussen. Erst recht steht nicht fest, in welcher Richtung ein Einfluss stattfinden kann. Andererseits wird auch ein grundsätzlicher Vorrang des § 203 StGB vor dem Datenschutzrecht vertreten[346].

Das Verhältnis von BDSG und § 203 StGB bedarf daher einer näheren Untersuchung. Zum Teil wird in der Literatur vertreten, dass das Bundesdatenschutzgesetz ebenso wie die Datenschutzgesetze der Länder nicht zur strafrechtlichen Rechtfertigung herangezogen werden können[347]. Begründet wird dies mit den Unterschieden zwischen dem Schutz des Datengeheimnisses nach § 5 BDSG und

[345] Sog. „Zwei-Schranken-Prinzip“ Mand, MedR 2003, S. 395.
[346] Schlund, in: Laufs/Uhlenbruck, Handbuch des Arztrechts, S. 586f.; Schneider, Handbuch des EDV- Rechts, S. 140; Kühne, Berufsrecht für Psychologen, S. 139; Lippert, in: Ratzel/Lippert, MBOÄ; § 9 Rn. 59.
[347] Eichelbrönner, Die Grenzen der Schweigepflicht des Arztes, S. 163.

dem Geheimnisschutz nach § 203 StGB[348]. Hierbei wird insbesondere auf die unterschiedlichen Schutzobjekte hingewiesen. Das Datenschutzrecht schützt personenbezogene Daten jeder Art, während § 203 StGB nur fremde Geheimnisse schützt. Für das Datenschutzrecht ist es irrelevant, ob die Information aus einer spezifischen Vertrauensbeziehung stammt. Damit erfasst das Datenschutzrecht einen weit größeren Daten- bzw. Informationsbestand als § 203 StGB. Dementsprechend zielt das Datenschutzrecht darauf ab, den Umgang mit diesen Daten zu regeln und einen Ausgleich zwischen den Interessen des Einzelnen an einer selbst bestimmten Verfügung über seine Daten und der Notwendigkeit einer im Allgemeininteresse liegenden Datenverarbeitung herbeizuführen.

Tatsächlich bestehen in der Schutzrichtung Unterschiede zwischen Datenschutzrecht und § 203 StGB. Der Privatgeheimnisschutz in § 203 StGB ist konzeptionell vorwiegend an Interessen des Einzelnen ausgerichtet, dient aber richtigerweise auch Allgemeininteressen. Der Schutz von Allgemeininteressen ist bezogen auf die Vertrauensbeziehung zwischen schweigepflichtigen Personen und betroffenen Geheimnisträgern[349]. Demgegenüber dient das Datenschutzrecht nicht dem Schutz von Allgemeininteressen, sondern dem „Grundrecht“ auf informationelle Selbstbestimmung und lässt im Gegensatz zu § 203 StGB weitgehend Durchbrechungen dieses Schutzes aufgrund von Interessen von allgemeiner Bedeutung zu[350].

Nach anderer Ansicht ist eine Rechtfertigung bei § 203 StGB durch Erlaubnissätze des Datenschutzrechts nicht grundsätzlich aufgrund der strukturellen Unterschiede zwischen dem Datenschutzrecht und § 203 StGB ausgeschlossen. Zur Begründung wird angeführt, dass personenbezogene Daten gleichzeitig auch „Geheimnisse“ i.S.v. § 203 StGB sein können. Daher müssen auch datenschutzrechtliche Offenbarungsbefugnisse einen strafrechtlichen Rechtfertigungsgrund bilden können[351]. Auch wenn § 203 StGB nur Individualinteressen schützt, ist dies unbeachtlich für die Qualifizierung datenschutzrechtlicher Erlaubnissätze.

Weiterhin wird angeführt, dass der Wortlaut des § 1 Abs. 3 S. 2 BDSG, nach dem die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder Be-

[348] Rogall, NStZ 1983, S. 7.
[349] Auf den personalen Charakter des § 203 StGB wurde bereits hingewiesen, vgl. S. 41.
[350] Vgl. Heyers/Heyers, MDR 2001, S. 1212; Eichelbrönner, Die Grenzen der Schweigepflicht des Arztes, S. 161.
[351] Lenckner, in: Schönke/Schröder, StGB § 203 Rn. 53c.

rufs- oder besonderer Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen, unberührt bleibt, keinen Vorrang der Schweigepflicht begründet. Vielmehr muss im Einzelfall durch Auslegung untersucht werden, ob eine Rechtfertigung durch eine Erlaubnisnorm des Datenschutzrechts möglich ist[352]. Schließlich wird mit Blick auf § 1 Abs. 3 S. 2 BDSG (§ 1 Abs. 4 S. 2 BDSG a.F.) argumentiert, dass diese Kollisionsnorm, entgegen der Begründung des Gesetzgebers, nicht einen allgemeinen Vorrang der strafrechtlichen Schweigepflicht bezweckt. Insoweit wird in der Formulierung „unberührt" ein sachlicher Unterschied zu der ausdrücklichen Vorrangregel des § 1 Abs. 3 S. 1 BDSG gesehen[353]. Nur wenn andere, hinsichtlich des strafrechtlichen Geheimnisumgangs gegenläufige, Vorschriften bestünden, sei ein Rückriff auf das Datenschutzrecht gesperrt. Ist dies nicht der Fall, besteht schon keine Konkurrenz zwischen Schweigepflicht nach § 203 StGB und dem Datenschutzrecht. Eine Rechtfertigung durch datenschutzrechtliche Vorschriften ist deshalb grundsätzlich möglich[354].

Im Ergebnis ist letztgenannte Auffassung vorzugswürdig. Ein genereller Vorrang des § 203 StGB vor dem Datenschutzrecht überzeugt nicht. Zunächst kann der Wortlaut des § 1 Abs. 1 S. 2 BDSG nicht übergangen werden, der so neutral gehalten ist, dass es konstruiert wirkt, ein generelles Spezialitätsverhältnis daraus ableiten zu wollen. Die Formulierung „unberührt" legt eher nahe, dass sowohl § 203 StGB als auch das Bundesdatenschutzgesetz nebeneinander gelten und damit die Voraussetzungen des Bundesdatenschutzgesetzes und des Strafrechts kumulativ zu erfüllen sind (sog. Zwei-Schranken-Modell)[355]. Dafür sprechen auch die erwähnten strukturellen Unterschiede zwischen dem Strafrecht und der Querschnittsmaterie Datenschutzrecht[356].

Gewichtiger erscheint das Argument, dass die Gesetzesmaterialien für eine Spezialität des strafrechtlichen Privatgeheimnisses gegenüber dem Datengeheimnis sprechen[357]. Dieses Argument ist aber letztlich nicht durchschlagend. Schon zu der alten Regelung des § 45 S. 3 BDSG, die ebenfalls die Differenzierung zwi-

[352] Vgl. Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 86f.
[353] Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 89, 90.
[354] Vgl. Eichelbrönner, Die Grenzen der Schweigepflicht des Arztes, S. 161, 162.
[355] Mand, MedR 2003, S. 395; Bieber, Datenschutz und ärztliche Schweigepflicht, S. 62; vgl. auch Meier, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, S. 31.
[356] Zu dieser Bezeichnung Bieber, Datenschutz und ärztliche Schweigepflicht, S. 50.
[357] Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 89, 90.

schen „geht vor“ und „bleibt unberührt“ enthielt, wurde überwiegend angenommen, dass der Gesetzesbegründung nur deklaratorische Wirkung zukommt[358]. Damit soll klargestellt werden, dass die verhältnismäßig jungen datenschutzrechtlichen Normen nicht eine Lockerung des strafrechtlichen Schutzniveaus bewirken können[359]. Schließlich weist Meier zu Recht darauf hin, dass andernfalls die §§ 13 Abs. 2 Nr. 7 BDSG und 28 Abs. 7 S. 2 BDSG überflüssig wären[360]. In der Tat muss man sich die Frage stellen, warum der nationale Gesetzgeber in Umsetzung europäischer Vorgaben aufgrund der Datenschutzrichtlinie Regelungen zum Schutz von Patientendaten geschaffen hat, wenn solche Patientendaten regelmäßig Geheimnisse im Sinne des § 203 StGB sind und § 203 StGB dem BDSG vorgeht.

Letzterer Ansicht ist daher im Ergebnis zu folgen. Dabei ist aber der Regelungsinhalt der Datenschutznormen zu beachten. Die Problemstellung ist nicht maßgeblich auf den generellen Vorrang oder die Parallelgeltung von Strafrecht und Datenschutzrecht auszurichten, sondern auf den inhaltlichen Bezug der beiden Rechtsgebiete. Bleibt eine datenschutzrechtliche Erlaubnisnorm dem Regelungsinhalt nach innerhalb des Kreises des Datenschutzrechts verhaftet, dann kann sie auch keine Bedeutung für das Strafrecht haben, weder durch die Festsetzung verschärfender Vorraussetzungen hinsichtlich des strafrechtlichen Geheimnisschutzes noch durch die Lockerung von Voraussetzungen mit Wirkung für den strafrechtlichen Geheimnisschutz. Nimmt die datenschutzrechtliche Erlaubnisnorm allerdings ausdrücklich oder dem Sinn und Zweck nach Bezug auf den strafrechtlichen Privatgeheimnisschutz, dann ist eine Wirkung auch für das Strafrecht, die über das bloße Berücksichtigen von datenschutzrechtlichen Bestimmungen zur Auslegung von Rechtfertigungsgründen des StGB reicht, denkbar[361].

Denn der Bundesgesetzgeber kann außerhalb des StGB Rechtfertigungsgründe regeln. Weder gibt es einen numerus clausus der Rechtfertigungsgründe[362], noch hat die Regelung eines Rechtfertigungsgrundes zwingend im StGB zu erfolgen,

---

[358] Bieber, Datenschutz und ärztliche Schweigepflicht, S. 62.
[359] Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 89, 90; Bieber, Datenschutz und ärztliche Schweigepflicht, S. 62.
[360] So Meier, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, S. 31.
[361] Anders Eichelbrönner, Die Grenzen der Schweigepflicht des Arztes, S. 164; Mahlein, Das Krankenhaus, S. 108; anders auch Otto, wistra 99, S. 205, der Wertungen datenschutzrechtlicher Erlaubnisnormen bei einer Rechtfertigung nach § 34 StGB einfließen lässt.
[362] Lenckner, in: Schönke/Schröder, StGB, Vorb. §§ 32 ff. Rn. 28.

um einen strafrechtlichen Rechtfertigungsgrund zu bilden[363]. Erforderlich für einen Rechtfertigungsgrund ist nach allgemeinen Regeln und entsprechend der Systematik der im StGB aufgeführten ausdrücklichen Rechtfertigungsgründen, dass gesetzlich hinreichend bestimmt sein muss, ob und wann eine strafrechtlich relevante Handlung gerechtfertigt ist.

Allerdings bleibt das Privatgeheimnis wegen § 1 Abs. 3 S. 2 BDSG weiterhin beachtlich, wenn es im Schutzniveau höhere Anforderungen als das Bundesdatenschutzgesetz stellt [364]. Denn dann würde es an dem maßgeblichen Bezug zu § 203 StGB fehlen, weil der durch § 203 StGB bezweckte Rechtsgüterschutz nicht hinreichend beachtet wird. Insoweit kann eine datenschutzrechtliche Erlaubnisnorm den strafrechtlichen Schutz von Privatgeheimnissen nicht berühren. Dies muss auch wegen des Gebots der Einheit der Rechtsordnung gelten. Zwar ist dieses Gebot und insbesondere dessen Reichweite nicht unumstritten[365], im Grundsatz ist aber anzuerkennen, dass ohne zwingende sachliche Gründe nicht das gleiche Verhalten außerhalb des StGB erlaubt sein kann, während es das Strafrecht verbietet.

Daher überzeugt es, die Formulierung in § 1 Abs. 3 S. 2 StGB dahingehend zu lesen, dass dann, wenn das Strafgesetzbuch selbst Rechtfertigungsregelungen aufstellt und eine Kollision mit dem Datenschutzrecht auftritt, die strafrechtliche Rechtfertigungsregelung eine solche des Bundesdatenschutzgesetzes verdrängt. § 203 StGB regelt aber keine Erlaubnis zum Offenbaren von Geheimnissen, weshalb auch keine echte Kollision besteht[366]. Dieses Ergebnis wird außerdem dadurch gestützt, dass der Gesetzgeber in § 1 Abs. 3 S. 2 BDSG eine andere Formulierung gewählt hat als in § 1 Abs. 3 S. 1 BDSG. Darin eine sprachliche Variation aus stilistischen Gründen zu sehen erscheint zutreffend wenig plausibel[367]. Grundsätzlich kommt daher eine Rechtfertigung durch Normen des Bundesdatenschutz-

[363] Vgl. Jescheck/Weigend, Lehrbuch des Strafrechts, § 31 III 1, mit dem begründenden Hinweis auf das Prinzip der Einheit der Rechtsordnung; Kühl, Strafrecht AT, § 3 Rn. 3, S. 128.
[364] Walz, in: Simitis, BDSG, § 11 Rn. 31, i.V.m. § 1 Rn. 174 mit dem Hinweis, dass das BDSG eine zweite, zusätzliche und im Hinblick auf das Recht auf informationelle Selbstbestimmung erforderliche Schutzebene darstellt.
[365] Maurach/Zipf, Strafrecht AT, § 25 IV Rn. 12ff., S. 344.
[366] Vgl. Bieber, Datenschutz und ärztliche Schweigepflicht, S. 61, 62.
[367] Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 90.

gesetzes in Betracht[368]. Es bedarf einer Untersuchung der jeweils in Frage kommenden Normen, ob sie als Rechtfertigungsgründe für § 203 StGB eingreifen können.

c) § 11 BDSG als strafrechtlicher Erlaubnissatz

Zunächst ist auf § 11 BDSG einzugehen. § 11 Abs. 1 BDSG ermöglicht, im Anwendungsbereich des BDSG personenbezogene Daten im Auftrag durch andere Stellen erheben, verarbeiten oder nutzen zu lassen. Die Norm lässt das unselbständige Erledigen von Aufgaben durch externe IT- Dienstleistungsunternehmen zu und kann als Rechtsgrundlage für Outsourcingprojekte herangezogen werden. Dabei ist die andere Stelle nicht Externer, sondern bildet mit dem Auftraggeber eine rechtliche Einheit, weshalb keine „Datenübermittlung" i.S. des Bundesdatenschutzgesetzes vorliegt[369]. Dies gilt wegen der grundsätzlichen Parallelgeltung von Datenschutzrecht und § 203 StGB nicht für den Bereich des Privatgeheimnisses. Trotz einer Ausgestaltung als Auftragsdatenverarbeitung kann nach h.M. ein „Offenbaren" i.S.v. § 203 StGB vorliegen[370].

Zu prüfen ist, ob das strafrechtlich geschützte „Privatgeheimnis" nach § 203 StGB einem Outsourcing medizinischer Daten in der Gestalt der „Auftragsdatenverarbeitung" nach § 11 BDSG entgegensteht[371], oder anders ausgedrückt, ob § 11 BDSG einen strafrechtlichen Rechtfertigungsgrund in Bezug auf § 203 StGB darstellt. Zum Teil wird in der Literatur in § 11 BDSG ein strafrechtlicher Rechtfertigungsgrund gesehen[372]. Diese Ansicht ist abzulehnen[373].

Das Argument von *Rogall*, dass Normen des BDSG schon deshalb keine Rechtfertigung liefern können, weil sie nur das Übermitteln von Daten (ohne Geheimnischarakter) gestatten, überzeugt zur Begründung allerdings wenig. Die Schnittmenge von personenbezogenen Daten und Geheimnissen ist groß und bereits oben wurde ausgeführt, dass Geheimnisse als personenbezogene Information bezeich-

---

[368] Im Ergebnis ebenso Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 87f.; Lenckner, in: Schönke/Schröder, StGB, § 203 Rn. 53 c.
[369] Gola/Schomerus, BDSG, § 11 Rn. 4.
[370] Walz, in: Simitis, BDSG, § 11 Rn. 31; Schneider, Handbuch des EDV-Rechts, S.140.
[371] Eine ähnliche Problematik stellt sich bei der Auslagerung von Bankdienstleistungen, vgl. Steding/Meyer, BB 2001, S. 1693.
[372] Vgl. Rogall, NStZ 1983, S. 7 mit Fußnote 129.
[373] Ebenso Walz, in: Simitis, BDSG, § 11 Rn. 31.

net werden können. Auch wenn das BDSG nur auf personenbezogene Daten abzielt, werden im Fall des Vorliegens personenbezogener Daten tatsächlich fast immer auch „Geheimnisse“ i.S.v. § 203 StGB vorliegen, sofern eine Beziehung zwischen einem Schweigpflichtigen und einem Geheimnisträger betroffen ist.

Bezogen auf den Aspekt des Rechtsgutschutzes liegt zudem kein gravierender Unterschied zwischen BDSG und § 203 StGB vor, da in beiden Fällen überwiegend der Schutz von Individualinteressen bezweckt ist. Es ist also durchaus denkbar, dass Normen des BDSG über personenbezogene Daten die Ebene des Datenschutzrechts verlassen können und auf das strafrechtlich geschützte Privatgeheimnis übergreifen. Dem steht auch nicht § 1 Abs. 3 S. 2 BDSG entgegen[374]. Denn mit einer grundsätzlichen Parallelgeltung von (Bundes-) Datenschutzrecht und § 203 StGB ist nicht ausgesagt, dass das Datenschutzrecht in bestimmten Bereichen nicht Einfluss auf die Schweigepflicht nehmen kann. Schon oben wurde dargelegt, dass es für die Frage der Rechtfertigung nicht maßgeblich auf einen pauschalen Vorrang oder eine pauschale Parallelgeltung ankommen kann, sondern auf den hergestellten Bezug in den fraglichen Normen. Daher ist nicht allgemein auf die unterschiedlichen Gegenstände, also Geheimnisse bei § 203 StGB und personenbezogene Daten im BDSG, abzustellen, sondern es muss die einzelne Norm, also in diesem Fall § 11 BDSG, interpretiert werden.

Der Wortlaut des § 11 BDSG deutet darauf hin, dass allein auf das Datenschutzrecht Bezug genommen wird. Die Formulierung in § 11 Abs. 1 BDSG, „ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich“, knüpft an eine erfolgte Erhebung, Verarbeitung oder Nutzung von personenbezogene Daten im Auftrag durch andere Stellen an. Bezug genommen wird also lediglich auf eine datenschutzrechtliche Möglichkeit einer Datenverarbeitung im Rahmen des § 11 BDSG und nicht auf den strafrechtlichen Schutz eines Geheimnisses im Sinne von § 203 StGB.

Auch dem Sinn und Zweck nach ist § 11 Abs. 1 BDSG als Befugnisnorm abzulehnen. § 11 Abs. 1 BDSG will verhindern, dass Schutzmechanismen des BDSG

[374] Anders Meier, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, S. 187. Aus § 1 Abs. 3 S. 2 BDSG folgt, dass das BDSG keine Befugnisnormen für § 203 StGB enthält. Dies gilt auch für die Landesdatenschutzgesetze, da § 1 Abs. 3 S. 2 BDSG einen allgemeinen Grundsatz enthält.

umgangen werden, indem der Umgang mit personenbezogenen Daten an Dritte delegiert wird[375]. Der Auftraggeber soll sich nicht von seiner Verantwortung „freikaufen“ können. Allerdings hat § 11 Abs. 1 BDSG nicht primär eine strafrechtliche Verantwortung im Auge. Das BDSG enthält zwar in § 44 BDSG eine Strafvorschrift. Der strafrechtliche Schutz ist aber an enge Voraussetzungen geknüpft. Nur vorsätzliche Handlungen, die gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, ausgeführt werden, sind strafbar. In allen anderen Fällen von Verstößen gegen die in § 43 BDSG erwähnten datenschutzrechtlichen Bestimmungen ist das Verhalten nicht mit Strafe bewehrt, sondern mit einem Bußgeld bewehrt. In der Mehrzahl der Fälle soll also der Konzeption nach keine strafrechtliche Sanktion für einen fehlerhaften Umgang mit personenbezogenen Daten erfolgen.

Neben der Sanktion durch ein Bußgeld für bestimmte in § 43 BDSG genannte Handlungen ist in § 7 BDSG allgemein bei einer nach dem BDSG oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten eine Schadensersatzpflicht bestimmt, sofern ein Schaden für den Betroffenen entstanden ist. Weiterhin sind im BDSG Auskunftsrechte für den Betroffenen sowie Kontrollrechte durch die Aufsichtsbehörden vorgesehen, um den sachgerechten Umgang mit personenbezogenen Daten zu schützen. Diesen Vorschriften soll sich der Auftraggeber nach § 11 Abs. 1 BDSG nicht einfach entziehen können. Insofern ist in § 11 Abs. 1 BDSG primär auf außerstrafrechtliche Verantwortung für den Schutz personenbezogener Daten, und damit des Rechtes auf informationelle Selbstbestimmung, abgestellt worden, wie auch § 11 Abs. 1 Satz 2 BDSG zeigt, nach dem die in §§ 6, 7 und 8 genannten Rechte dem Auftraggeber gegenüber geltend zu machen sind.

Dass § 11 Abs. 1 BDSG keine strafrechtliche Befugnisnorm ist, zeigt schließlich auch § 39 Abs. 1 BDSG. Adressat des § 39 Abs. 1 BDSG ist derjenige, der personenbezogene Daten von dem Schweigepflichtigen in Ausübung seiner Berufs- oder Amtspflicht zur Verfügung gestellt bekommen hat. Die durch § 39 BDSG verlängerte, das Datenschutzrecht prägende Zweckbindung, setzt eine mit dem Berufsgeheimnis vereinbare Zurverfügungstellung personenbezogener Daten vor-

[375] Vgl. Schaffland/Wiltfang, BDSG, § 11 Rn. 1; Bergmann/Möhrle/Herb, BDSG, § 11 Rn. 26; zu den Funktionen des § 11 BDSG umfassend Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 402f.

aus. Erst wenn eine solche nach dem Berufs- oder Amtsgeheimnis zulässige Zurverfügungstellung vorliegt, greift die durch § 39 BDSG fortgeschriebene Zweckbindung[376]. Mit dieser Betonung des Berufs- oder Amtsgeheimnisses in § 39 BDSG ist es nicht vereinbar, in § 11 BDSG eine strafrechtliche Befugnisnorm zu sehen, da § 11 BDSG weder ausdrücklich, noch dem Sinn und Zweck nach auf den Schutz von „Geheimnissen" i.S.v. § 203 StGB Rücksicht nimmt.

Damit ist nicht gesagt, dass § 11 BDSG keinerlei strafrechtliche Bedeutung erlangen kann. Aus dem Dargelegten folgt lediglich, dass § 11 BDSG kein tauglicher strafrechtlicher Rechtfertigungsgrund ist. Denkbar ist, dass Wertungen des § 11 BDSG bei § 203 StGB innerhalb von strafrechtlichen Rechtfertigungsgründen berücksichtigt werden, beispielsweise im Rahmen einer Rechtfertigung nach § 34 StGB[377]. Aber auch ein Einfluss auf der Seite des Tatbestandes ist denkbar[378].

d) § 16 BDSG als strafrechtlicher Erlaubnissatz

Außer § 11 BDSG, der die Datenverarbeitung im Auftrag regelt, könnte § 16 BDSG als Erlaubnisnorm in Betracht kommen. § 16 BDSG findet auf die Datenverarbeitung der öffentlichen Stellen Anwendung und erlaubt unter bestimmten Voraussetzungen die Datenübermittlung an nicht-öffentliche Stellen, wenn keine Datenverarbeitung im Auftrag vorliegt. Eine Qualifizierung des § 16 BDSG als strafrechtlichen Rechtfertigungsgrund scheitert aber aus den gleichen Gründen wie bei § 11 BDSG. Auch bei § 16 BDSG findet sich kein gezielter Bezug auf den strafrechtlichen Geheimnisschutz nach § 203 StGB. Vielmehr verweist § 16 Abs. 1 Nr. 1 BDSG pauschal auf § 14 BDSG . Nach § 14 Abs. 5 BDSG richtet sich die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten nach den Voraussetzungen in § 13 Abs. 2 Nr. 1-6 oder 9 unabhängig davon, ob eine strafrechtliche Geheimhaltungspflicht besteht. Nur für die in § 13 Abs. 2 Nr. 7 BDSG genannten Verarbeitungszwecke bestimmt § 14 Abs. 5 BDSG, dass sich die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten nach den für die in § 13 Abs. 2 Nr. 7 ge-

[376] Ähnliche Regelungen finden sich in den Landesdatenschutzgesetzen, vgl. Art. 22 Bayerisches Datenschutzgesetz.
[377] Otto, wistra 1999, S. 207.
[378] So bei der Erfüllung des Tatbestandes durch Unterlassen, vgl. Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 52.

nannten Personen geltenden Geheimhaltungspflichten. Für den Bereich der medizinischen Daten, die sich weitgehend mit den in § 3 Abs. 9 BDSG genannten Daten überschneiden, wird damit vorausgesetzt, dass § 203 StGB eingehalten ist. § 203 StGB wird nicht im Sinne einer Rechtfertigung durchbrochen.

Gegen einen strafrechtlichen Rechtfertigungsgrund spricht zudem, dass in § 16 BDSG, anders als in § 11 BDSG, eine Datenübermittlung geregelt ist. Nach der Übermittlung ist die empfangende Stelle verantwortlich für den Umgang mit den Daten. Dies folgt aus § 16 Abs. 2 BDSG, nach dem die übermittelnde Stelle nur die Verantwortung für die Zulässigkeit der Übermittlung trägt. Wäre somit § 16 BDSG ein Rechtfertigungsgrund für ein Offenbaren von „Geheimnissen" i.S.v. § 203 StGB, dann könnte eine Delegation strafrechtlicher Verantwortung erfolgen, ohne dass der personale Charakter der Schweigepflicht nach § 203 StGB berücksichtigt und ohne dass der Übermittelnde Verantwortung für die Schutzvorkehrung des Empfängers behält. Das kann nicht überzeugen.

e) § 28 BDSG als strafrechtlicher Erlaubnissatz

Eine weitere potenzielle strafrechtliche Erlaubnisnorm findet sich in § 28 BDSG. Hier erfassen die durch Gesetz vom 18.05.2001 angefügten Absätze 6-8 besondere Arten von personenbezogenen Daten. Darunter fallen Angaben über die Gesundheit nach § 3 Abs. 9 BDSG. Da in einem weiten Bereich medizinische Daten, die personenbezogen und zugleich Geheimnisse i.S.v. § 203 StGB sind, unter diesen Begriff fallen, ist § 28 Abs. 6-8 BDSG einschlägig.

§ 28 Abs. 8 BDSG ermöglicht eine Datenübermittlung an Dritte aus anderen als in Abs. 6 und 7 genannten Zwecken, wenn die Voraussetzungen des § 28 Abs. 6 Nr. 1-4 oder Abs. 7 Satz 1 eingehalten werden. § 28 Abs. 7 BDSG lässt das Erheben von besonderen personenbezogenen Daten zu bestimmten Gesundheitszwecken zu, wenn die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Norm bezieht sich also auf den strafrechtlichen Schutz von Geheimnissen durch § 203 StGB, indem sie fordert, dass die am Umgang mit besonderen Arten personenbezogener Daten Beteiligten einer entsprechenden Geheimhaltungspflicht unterliegen müssen und Angehörige eines anderen als in § 203 Abs. 1

und 3 des Strafgesetzbuches genannten Berufes nur unter den Voraussetzungen besondere Arten personenbezogener Daten verarbeiten dürfen, unter denen auch ein Arzt dazu befugt wäre.

Hieraus wird teilweise der Schluss gezogen, dass unter Durchbrechung des „Privatgeheimnisses“ i.S.v. § 203 StGB eine Übermittlung an Dritte, die ebenfalls der Schweigepflicht nach § 203 StGB unterliegen, im Rahmen eines Outsourcings strafrechtlich erlaubt sein soll[379]. Für die genannte Schlussfolgerung spricht, dass sie die Weitergabe an enge Voraussetzungen bindet bzw. die Übermittlung der Daten an andere schweigepflichtige Personen nur dann zulässt, wenn sie nach Abwägung der Interessen an einer Übermittlung im Vergleich zu den Interessen des Betroffen am Schutz seiner Daten erforderlich ist. Insofern wird dem Privatgeheimnisschutz nach § 203 StGB in einem starken Maße Rechnung getragen. Die fehlende Spezifizierung im Adressatenkreis fällt dagegen weniger ins Gewicht. Man könnte daher annehmen, dass eine Aushöhlung der strafrechtlichen Schweigepflicht nicht droht.

Bedenken hiergegen bestehen, weil sich § 28 Abs. 6 und 7 BDSG nicht direkt an Geheimnisverpflichtete richtet. Zugeschnitten ist § 28 Abs. 6-8 BDSG generell auf nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen. Hinsichtlich des Normadressaten ist daher fraglich, ob § 28 BDSG dem personalen Charakter des strafrechtlichen Geheimnisschutzes gerecht wird. Außerdem ist bereits zum Tatbestand des § 203 StGB festgestellt worden, dass ein Offenbaren auch bei Schweigepflichtigen untereinander anzunehmen ist[380]. Dies soll dem Wortlaut nach durch § 28 BDSG nicht verändert werden[381], da nach § 28 Abs. 7 BDSG die Voraussetzungen der beruflichen Geheimhaltungspflicht für die Zulässigkeit der Datenverarbeitung maßgeblich sein sollen. Insofern erscheint es zweifelhaft, in § 28 BDSG einen strafrechtlichen Rechtfertigungsgrund zu sehen. Man mag annehmen, dass aus kriminalpolitischen Erwägungen kein Bedürfnis für eine Strafbarkeit besteht, da dem Schutz des informationellen Selbstbestimmungs-

[379] So Köpke, Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für Private Krankenversicherer, S. 167, 174.
[380] Vgl. oben S. 71; hinsichtlich einer Befugnis vgl. Lenckner, in: Schönke/Schröder, StGB, § 203 Rn. 21.
[381] Aus ähnlichen Erwägungen wurde § 49b Abs. 4 S. 1 BRAO von den Instanzgerichten nicht als Offenbarungsbefugnis gesehen, vgl. LG München I NJW 2004, S. 451, entgegen AG Regensburg NJW 2004, S. 1879; anders mittlerweile der BGH, der die zwischen den Instanzgerichten lange umstrittene Rechtsfrage entschieden hat, vgl. BGH Urteil vom 01.03.2007, Az.: IX ZR 189/05.

rechts hinreichend im Datenschutz Rechnung getragen wird. Allerdings ist einer solchen Argumentation nicht zu folgen, da sie die eigenständige strafrechtliche Wertung überspielen würde. Sofern eine Strafbarkeit hinsichtlich § 203 StGB entfallen soll, bedarf es auch einer entsprechenden auf das Strafrecht bezogenen Regelung durch den Gesetzgeber. Ein solcher Bezug ist aber weder ausdrücklich gewollt, noch ergibt er sich aus dem Sinn und Zweck des Datenschutzrechts. Denn der Schutz des Datengeheimnisses weist, wie bereits aufgezeigt wurde, erhebliche Unterschiede zum Geheimnisschutz nach § 203 StGB auf. Überzeugender ist es daher, § 28 BDSG auch nach seiner Änderung als rein datenschutzrechtliche Erlaubnisnorm anzusehen[382].

Von der Qualifizierung als strafrechtliche Erlaubnisnorm abgesehen**,** kann die rechtfertigende Wirkung bei § 28 Abs. 8 i.V.m. Abs. 7 Satz 1 nur bei einer Übermittlung an selbst schweigepflichtige Personen erfolgen. Daher scheidet diese Norm für das Outsourcing medizinischer Daten an private IT-Dienstleistungsunternehmen zumeist aus, da diese regelmäßig nicht zu dem nach § 203 StGB schweigepflichtigen Personenkreis gehören. Die verbleibende Möglichkeit über § 28 Abs. 8 BDSG i.V.m. Abs. 6 Nr. 1-4 BDSG würde daran scheitern, dass die tatbestandlichen Voraussetzungen der Nr. 1-4 nicht erfüllt wären.

Ein Outsourcing medizinischer Daten, das vornehmlich einer Kosten-Nutzen-Analyse entspringt, dient nicht dem Schutz lebenswichtiger Interessen, Nr. 1, auch sind nicht Daten betroffen, die der Betroffene offenkundig öffentlich gemacht hat, Nr. 2. Schließlich ist es weder zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche, Nr. 3, noch zur Durchführung wissenschaftlicher Forschung erforderlich. Die Bedeutung des § 28 BDSG ist somit für Outsourcingvorhaben beschränkt. Allenfalls als Auffangtatbestand bei einer Kooperation zwischen Schweigepflichtigen untereinander könnte § 28 BDSG herangezogen werden, sofern keine vorrangigen Sonderregelungen bestehen[383].

---

[382] So auch Duhr/Naujok/Danker/Seiffert, DuD 2003, S. 11; a.A. wohl OLG Nürnberg vom 7. Dezember 2000, Az: 8 U 1307/00, das aber nicht begründet, warum § 28 BDSG strafrechtliche Erlaubnisnorm sein soll; auch Köpke nimmt wohl eine Rechtfertigungsmöglichkeit nach § 28 BDSG an, vgl. Köpke, Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für Private Krankenversicherer, S. 234f.

[383] So enthält Art. 27 BayKrG eine für den Krankenhausbereich vorrangige spezifische Sonderregelung, die ein Outsourcing von Patientendaten nur dann zulässt, wenn ein anderes Krankenhaus Outsourcingpartner ist.

3. Regelungen des Telekommunikationsgesetzes

Denkbar ist, dass Regelungen des Telekommunikationsgesetzes, TKG, dem Outsourcer das Heranziehen externer Dienstleistungsanbieter ermöglicht. Vorschriften zum Datenschutz finden sich in den §§ 91 ff. TKG. Nach § 91 Abs. 1 TKG wird durch die §§ 91 ff TKG. der Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken, geregelt. Beim Outsourcing medizinischer Daten nehmen die betroffenen Geheimnisträger nicht an einer Telekommunikation teil. Dass der Outsourcer sich eventuell im Verhältnis zum externen Dienstleistungsanbieter der Telekommunikation bedient, ändert nichts daran, dass der Outsourcer die medizinischen Daten des Betroffenen nicht zu Telekommunikationszwecken erhalten hat. Dadurch könnte höchstens der Outsourcer zum Nutzer werden. Es geht nicht um den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation. Daher sind die §§ 91 ff. TKG nicht anwendbar. Ein Erlaubnistatbestand nach dem TKG scheidet somit aus[384]. Aus den gleichen Erwägungen scheiden Regelungen des TMG als Erlaubnistatbestände aus[385].

4. Sozialrechtliche Offenbarungsbefugnisse

Befugnisnormen, die für eine Rechtfertigung hinsichtlich § 203 StGB in Betracht zu ziehen sind, finden sich weiterhin im Sozialrecht. Dabei ist zwischen Regelungen des allgemeinen Sozialdatenschutzes und speziellen Regelungen zu unterscheiden. In § 35 Abs. 1 SGB I ist als Eingangsregelung das Sozialgeheimnis normiert. Hiernach hat jeder „Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 1 SGB X) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden“. Zu den Leistungsträgern zählen, soweit hier von Interesse, Ärzte, Krankenhäuser und Krankenkassen im System der gesetzlichen Krankenversicherung einschließlich ihrer im Sozialgesetzbuch genannten Zu-

[384] Ausführlich Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 160.
[385] So auch Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 160 f., zum Vorrang des alten TDDSG gegenüber dem BDSG Schrey/Schmitz, in: Wissmann, Telekommunikationsrecht, S. 857.

sammenschlüsse. In § 78 SGB X wird die Verpflichtung zum Schutz der Sozialdaten auf Dritte erweitert.

Davon ausgehend wird der allgemeine Sozialdatenschutz in § 35 Abs. 2 SGB I und den Vorschriften des zweiten Kapitels des zehnten Buches geregelt. Die Regelungen des Sozialdatenschutzes gehen wegen § 1 Abs. 3 S. 2 1. Alt. BDSG und vergleichbarer Regelungen in den Landesdatenschutzgesetzen dem allgemeinen Datenschutzrecht vor. Spezielle Regelungen finden sich in den einzelnen Büchern des SGB, für den Bereich medizinischer Daten vorwiegend in den §§ 284 ff. SGB V und in § 310 SGB V. Nach Maßgabe des § 37 S. 1 SGB X gehen diese speziellen Regelungen, soweit sie den Umgang mit Daten abweichend regeln, den allgemeinen Vorschriften zum Sozialdatenschutz vor.

a) Spezielle Regelungen im SGB V

Die speziellen Regelungen im SGB V regeln lediglich die Datenerhebung, -verarbeitung, -nutzung und -übermittlung zwischen den Beteiligten im System der Gesetzlichen Krankenversicherung. Sie können nicht für die Einschaltung privater IT- Dienstleistungsunternehmen zu Outsourcingzwecken herangezogen werden. Dafür sind die Vorschriften nicht konzipiert, da sie allein das Innenverhältnis der Beteiligten in der Gesetzlichen Krankenversicherung betreffen. Eine Aufgabenverlagerung zu privaten IT- Dienstleistungsunternehmen zur kostengünstigeren Erfüllung eigener Aufgaben, die das durch § 203 StGB geschützte Verhältnis zwischen Schweigepflichtigen und Geheimnisträger durchbricht, ist nicht geregelt.

Dies gilt auch für § 291 a SGB V, durch den die Einführung der elektronischen Gesundheitskarte als Erweiterung der bisherigen Krankenversichertenkarte zum 1. Januar 2006 festgelegt worden ist. Denn § 291a Abs. 8 SGB V zeigt, dass ein Zugriff von privaten Dienstleistungserbringern außerhalb des Systems der GKV nicht vorgesehen ist. Eine Durchbrechung des § 203 StGB unter Heranziehung privater Dienstleistungsanbieter ist dadurch nicht gedeckt. Gedeckt ist hingegen die Ausgabe der elektronischen Gesundheitskarte durch die gesetzlichen Krankenkassen in Absprache mit den weiteren Beteiligten der Selbstverwaltung und der damit verbundene Zugriff durch die in § 291a SGB V genannten Personen. Hier wird insofern eine Befugnis zum Offenbaren eingeräumt, als durch § 291a

Abs. 4 SGB V die Weitergabe von Daten zwischen nach § 203 StGB schweigepflichtigen Personen ermöglicht wird. Die Weitergabe von Daten kann aber nicht an jeden beliebigen Schweigepflichtigen erfolgen. § 291a Abs. 4 SGB V schränkt dies insoweit ein, als er einen Zugriff bestimmter schweigepflichtiger Personen nur zulässt, soweit es zur Versorgung der Versicherten erforderlich ist.

Vor dem Hintergrund des Rechts auf informationelle Selbstbestimmung ist § 291a Abs. 4 SGB V so zu verstehen, dass nur solchen Personen Geheimnisse offenbart werden dürfen, die in die Behandlung eingeschaltet sind. In solchen Fällen ist regelmäßig davon auszugehen, dass auch eine konkludente Einwilligung des Patienten vorliegt, die eine Befugnis zum Offenbaren verleiht. Für bestimmte besonders sensible Daten nach § 291a Abs. 3 SGB V stellt § 291a Abs. 5 SGB V sicher, dass ein Erheben, Verarbeiten und Nutzen dieser Daten mittels der elektronischen Gesundheitskarte nur mit dem Einverständnis der Versicherten erfolgen kann. Somit wird für den Bereich der medizinischen Daten die Selbstbestimmung gewahrt und die inhaltliche Erweiterung der bisherigen Krankenversicherungskarte zur elektronischen Gesundheitskarte überwiegend an dem Prinzip der Freiwilligkeit orientiert. Damit wird dem Recht auf informationelle Selbstbestimmung Genüge getan.

Zugleich folgt daraus, dass § 291a SGB V über den dargestellten Rahmen hinaus keine Befugnisnorm für Outsourcingvorhaben, beispielsweise für das Einrichten zentraler Datenpools**,** sein kann. Dies gilt auch dann, wenn die Personen, die mit den Daten in Kontakt kommen, ebenfalls einer Schweigepflicht unterliegen. Demgegenüber findet sich in § 96 SGB XI eine Vorschrift, die die Einrichtung eines gemeinsamen Datenpools begrenzt ermöglicht[386]. Ein Heranziehen privater IT-Dienstleistungsunternehmen ist in § 96 SGB XI nicht vorgesehen. § 96 SGB XI betrifft ausschließlich das Verhältnis zwischen Krankenkasse und Pflegekasse. Eine Außenbefugnis im Verhältnis zu den Betroffenen wird nicht erteilt.

[386] Verfassungsrechtliche Bedenken gegenüber § 96 SGB XI äußern Krahmer/Stähler, NZS 2003, S. 193ff.

b) Allgemeine Regelungen im SGB X

Zahlreiche Befugnisse finden sich im zweiten Abschnitt des zweiten Kapitels SGB X. Diese Vorschriften sind bereichsspezifisches Datenschutzrecht. Sie betreffen den Schutz von Sozialdaten. Der Begriff „Sozialdaten“ ist in § 67 SGB X legal definiert. Es handelt sich um personenbezogene Daten, die von einer in § 35 Abs. I SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt werden. Solche Daten müssen nicht wie bei § 203 StGB Geheimnisse im materiellen Sinne sein[387]. Der Begriff „Sozialdaten“ wird nicht maßgeblich durch die in den Daten enthaltene Information bestimmt, sondern indem die Daten einem Aufgabenbereich einer in § 35 SGB I genannten Stelle zugeordnet werden können und in deren räumlichen Verarbeitungsbereich gelangen. Hierdurch erhalten Sozialdaten einen fachlichen Bezug[388].

Typischerweise unterliegen diese in § 35 SGB I genannten Stellen entweder einer Schweigepflicht nach § 203 Abs. 1 und 3 StGB oder nach § 203 Abs. 2 StGB. Zum Teil wird hieraus gefolgert, dass die in den §§ 67 ff. SGB X enthaltenen Befugnisse auch ein „Offenbaren“ i.S.v. § 203 StGB rechtfertigen[389].

Dieser Auffassung kann nicht gefolgt werden. Nach § 67d SGB X ist eine Übermittlung von Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift des SGB X vorliegt. Eine allgemein gehaltene Übermittlungsbefugnis von großer praktischer Relevanz enthält § 69 SGB X, durch den die Übermittlung von Sozialdaten zur Erfüllung sozialer Aufgaben ermöglicht wird. Unabhängig etwaiger Bedenken hinsichtlich einer hinreichenden Bestimmtheit[390] zeigt die Norm, worauf die gesetzlichen Übermittlungsbefugnisse der §§ 68 bis 77 SGB X hauptsächlich zugeschnitten sind. Ermöglicht werden soll der Informationsfluss innerhalb der Sozialverwaltung[391]. Integrierender Anknüpfungspunkt ist die Erfüllung ge-

[387] Mrozynski, SGB I, § 35 Rn. 8; Krahmer, in: Krahmer, Sozialgesetzbuch Allgemeiner Teil, § 35 Rn. 6.
[388] Vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 113; Seewald, in: Kassler Kommentar Sozialversicherungsrecht, § 35 SGB I Rn. 5; Rombach, in: Hauck/Haines, SGB X/1, 2, K, § 67 Rn. 11f.
[389] Meier, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, S. 188.
[390] Dazu Schott, Die Geheimnispflicht der Sozialversicherungsträger, S. 160 ff.
[391] Binne, in: von Maydell/Ruland, Sozialrechtshandbuch, S. 498 f.; Giese/Krahmer, Sozialgesetzbuch, I § 35 Rn. 5.4, 5.5.

setzlicher Aufgaben. Dieser Bereich lässt sich höchstens mit dem durch § 203 Abs. 2 StGB geschützten Bereich vergleichen.

Auf den Geheimnisschutz nach § 203 Abs. 1 StGB sind die sozialrechtliche Übermittlungsbefugnisse des zweiten Kapitels des zehnten Buches nicht abgestimmt. Sie knüpfen an § 35 SGB I an, dem ein eher institutionelles Verständnis zu Grunde liegt[392]. Schon aus diesem Grund sind sie nicht allgemein als strafrechtliche Befugnisnormen zu werten. Untermauert wird diese Auffassung durch § 76 SGB X. § 76 SGB X schränkt die Übermittlung „besonderer personenbezogener Daten" i.S.v. § 67 Abs. 12 SGB X, zu denen auch medizinische Daten gehören, ein. Sind Sozialdaten einer Stelle nach § 35 SGB I durch einen nach § 203 Abs. 1 oder Abs. 3 StGB Schweigepflichtigen anvertraut worden, so ist eine Zweitübermittlung dieser Daten nur unter den Voraussetzungen zulässig, unter denen der nach § 203 Abs. 1 oder Abs. 3 StGB Schweigepflichtige selbst übermittlungsbefugt wäre. Damit können, soll § 76 SGB X Sinn machen, sozialrechtliche Übermittlungsbefugnisse nach den §§ 68 bis 77 SGB X nicht für § 203 Abs. 1 oder 3 StGB maßgeblich sein. Vielmehr ist umgekehrt fraglich, inwiefern die Rechtfertigungsregeln für § 203 StGB die sozialrechtlichen Übermittlungsbefugnisse beeinflussen können.

Schließlich stellt auch § 97 Abs. 1 SGB X keinen Rechtfertigungsgrund dar. Nach seinem eindeutigen Wortlaut setzt § 97 Abs. 1 SGB X eine Ermächtigungsnorm voraus, stellt aber selbst keine Ermächtigungsnorm zum Heranziehen Dritter dar[393]. Auch § 88 SGB X ermöglicht seinem eindeutigen Wortlaut nach nicht das Heranziehen privater Dritter, sondern nur das Heranziehen weiterer Leistungsträger oder ihrer Verbände. § 88 SGB X bleibt also im Innenbereich der Sozialverwaltung verhaftet und eignet sich nicht als Erlaubnisnorm für das Outsourcing medizinischer Daten[394].

Denkbar erscheint, dass die §§ 67 ff. SGB X wenigstens im Hinblick auf § 203 Abs. 2 StGB Rechtfertigungsgründe darstellen. Schließlich bezieht sich die Einschränkung des § 76 SGB X nur auf § 203 Abs. 1 und 3 StGB. Letztlich überzeugt

[392] Mrozynski, SGB I, § 35 Rn. 5.
[393] Breitkreuz, in: Diering/Timme/Waschull, Sozialgesetzbuch X, § 97 Rn. 1; Dortants/ Hansemann, NZS 1999, S. 543.
[394] Vgl. auch Dortants/Hansemann, NZS 1999, S. 544, die zutreffend auch die Möglichkeit einer analogen Anwendung des § 88 SGB X verneinen.

dies nicht. Rechtfertigungsgründe hinsichtlich § 203 StGB sind dann anzunehmen, wenn dem Schweigepflichtigen aufgrund einer gesetzlich vorweggenommenen Interessenabwägung Mitteilungspflichten auferlegt werden. Sofern diese Mitteilungspflichten mit dem Recht auf informationelle Selbstbestimmung vereinbar sind, erlauben sie zwangsläufig ein Offenbaren auch von „Geheimnissen" i.S.v. § 203 StGB. Daran knüpft § 71 SGB X an, der eine Übermittlung von Sozialdaten dann für zulässig erachtet, wenn sie zur Erfüllung der gesetzlichen Mitteilungsverpflichtungen erforderlich sind. Daran zeigt sich, dass die §§ 68 bis 77 SGB X nicht eine Durchbrechung des § 203 StGB ermöglichen, sondern an eine zulässige Offenbarung nach § 203 StGB anknüpfen, unabhängig davon, ob § 203 Abs. 1, 3 StGB oder § 203 Abs. 2 StGB betroffen sind. Dafür spricht auch der personale Charakter des § 203 StGB. § 203 Abs. 2 StGB nimmt wie § 203 Abs. 1 StGB auf Geheimnisse Bezug. Nur ergänzend wird in § 203 Abs. 2 S. 2 StGB auf Einzelangaben eingegangen, für die § 203 Abs. 2 S. 2 HS. 2 StGB eine Ausnahme von S. 1 schafft[395]. Daher kann auch § 203 Abs. 2 StGB nicht wie § 35 SGB I im Bereich des Sozialdatenschutz institutionell interpretiert werden. Die §§ 67 ff SGB X stellen somit insgesamt für § 203 StGB keine Rechtfertigungsgründe dar[396].

Im dritten Abschnitt des SGB X regelt § 80 SGB X die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag. Die Norm ähnelt § 11 BDSG, enthält aber eine gewichtige Einschränkung im Vergleich zu § 11 BDSG. Nach § 80 Abs. 5 SGB X ist eine Auftragsdatenverarbeitung durch nicht-öffentliche Stellen nur zulässig, wenn beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst.

Unabhängig der Probleme, die § 80 Abs. 5 SGB X im Tatbestand aufweist, nämlich festzulegen, was unter „erheblich kostengünstiger" oder „überwiegende Teil der Speicherung des gesamten Datenbestandes" zu verstehen ist, stellt sich die Frage, ob § 80 SGB X eine strafrechtliche Befugnis zum Offenbaren verleiht. Dies kann deswegen in Betracht gezogen werden, weil § 80 SGB X in der Regel Personen betreffen wird, die einer Schweigepflicht aus § 203 StGB unterliegen.

[395] Dabei wird zum Teil die eigenständige Bedeutung des S. 2 bezweifelt, vgl. Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 48.
[396] Im Ergebnis wohl ebenso Mrozynski, SGB I, § 35 Rn. 5, 6.

Zudem lässt § 80 SGB X die Auftragsdatenverarbeitung durch nicht-öffentliche Stellen nur unter erschwerten Bedingungen zu.

Eine strafrechtliche Befugnis ist trotzdem abzulehnen. Schon die systematische Stellung im dritten Abschnitt des SGB X spricht gegen eine strafrechtliche Befugnis. Der dritte Abschnitt des SGB X ist überschrieben mit „Organisatorische Vorkehrungen zum Schutz der Sozialdaten, besondere Datenverarbeitungsarten". Dies spricht dafür, dass in § 80 SGB X lediglich eine besondere Erscheinungsform der Datenverarbeitung geregelt wird, die eine Befugnis im Innenbereich der Datenverarbeitung enthält, ohne zusätzliche Befugnisse im Außenverhältnis zum Betroffenen festzusetzen. Darauf deutet auch der Wortlaut des § 80 Abs. 1 SGB X hin. Der Formulierung, „Werden Sozialdaten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt…", lässt sich entnehmen, dass eine grundsätzlich zulässige Auftragsdatenverarbeitung als besondere Organisationsform vorausgesetzt wird, die dann durch § 80 SGB X ausgestaltet und an bestimmte Voraussetzungen für das Heranziehen eines Auftragnehmers geknüpft wird. Passend zu dieser Sichtweise wird überwiegend und entsprechend zu § 11 BDSG angenommen, dass bei einer Datenweitergabe an den Auftragnehmer keine Übermittlung vorliegt[397]. Der Auftragnehmer ist nicht Dritter im datenschutzrechtlichen Sinne.

Ein „Offenbaren" i.S.v. § 203 StGB wird deswegen aber nicht ausgeschlossen. Denn § 80 SGB X verlangt in Abs. 1 nur, dass der Auftraggeber für die Einhaltung der sozialrechtlichen Datenschutzbestimmungen und anderer Vorschriften über den Datenschutz verantwortlich bleibt. Auf den Privatgeheimnisschutz wird nicht Bezug genommen. Auch sinngemäß ist eine Bezugnahme auszuschließen, da die den Datenschutz sichernden Regelungen auf den Informationsfluss innerhalb der Sozialverwaltung abgestimmt sind, nicht aber auf den personalen Charakter des § 203 StGB. So orientiert sich § 80 SGB X an den Übermittlungsbefugnissen der §§ 68 bis 70 SGB X sowie an den speziellen Übermittlungsbefugnissen in den anderen Büchern des SGB und integriert die Datenverarbeitung im Auftrag als besondere Erscheinungsform in das System des Informationsflusses. Die Einschränkungen des § 76 SGB X für besondere Sozialdaten gelten auch im

[397] Seidel, in: Diering/Timme/Waschull, Sozialgesetzbuch X, § 80 Rn. 3; Kessler, DuD 2004, S. 42.

Rahmen der Auftragsdatenverarbeitung[398]. Vor diesem Hintergrund sind den Datenschutz sichernde Anforderungen in § 80 SGB X zu verstehen. Sie beziehen sich auf die Anforderungen im Datenschutzrecht, nicht auf die Erfordernisse des strafrechtlichen Privatgeheimnisschutzes. Festzuhalten ist somit, dass bei § 80 SGB X keine „Übermittlung" im datenschutzrechtlichen Sinne, wohl aber ein „Offenbaren" i.S.v. § 203 StGB vorliegen kann. Die Regelung des § 80 SGB X ist keine strafrechtliche Befugnisnorm.

5. Landesrecht als bundesrechtlicher Rechtfertigungsgrund

Ob Landesrecht Handlungen, die den bundesrechtlichen Straftatbestand des § 203 StGB erfüllen, rechtfertigen kann, erscheint auf den ersten Blick fraglich. In einer Entscheidung zu § 7 GDSG NW hat das OLG Düsseldorf diese Frage verneint[399]. § 7 GDSG NW ermöglicht die Beauftragung eines privaten Dritten unter der Voraussetzung, dass „beim Auftragnehmer die Wahrung der ärztlichen Schweigpflicht sichergestellt" sein muss. In dieser Regelung ist auf § 203 StGB Bezug genommen. Das OLG Düsseldorf hat es jedoch abgelehnt, in dieser Regelung einen strafrechtlichen Rechtfertigungsgrund zu sehen, weil Landesrecht als solches keinen Rechtfertigungsgrund für den bundesgesetzlichen § 203 StGB darstellen kann.

Allerdings findet sich diese Aussage nicht in den tragenden Entscheidungsgründen, sondern wird als obiter dictum festgestellt. Das obiter dictum überrascht, wenn man bedenkt, dass die h.M. in der strafrechtlichen Literatur davon ausgeht, dass auch Landesrecht einen Rechtfertigungsgrund für bundesrechtliche Tatbestände darstellen kann, wenn die Rechtsmaterie, der der landesrechtliche Rechtfertigungsgrund entstammt, in die Gesetzgebungskompetenz der Länder fällt[400]. Dementsprechend ist die Entscheidung des OLG Düsseldorf in diesem Punkt kritisiert worden[401]. Die Aussage des OLG Düsseldorf ist im Verhältnis zur h.M. auf ihre Tragfähigkeit zu untersuchen.

---

[398] Seidel, in: Diering/Timme/Waschull, Sozialgesetzbuch X, § 80 Rn. 6.
[399] OLG Düsseldorf, CR 1997, S. 536 ff.
[400] Lenckner, in: Schönke/Schröder, StGB, Vorb. §§ 32 ff. Rn. 27; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 13.
[401] Vgl. die Anmerkung des Bayerischen Datenschutzbeauftragten in CR 1997, S. 539.

Betrachtet man die These der h.M., dass bei entsprechender Gesetzgebungskompetenz der Länder auch Landesrecht einen Rechtfertigungsgrund für einen bundesgesetzlichen Tatbestand darstellen kann, könnte in Konsequenz dazu das Outsourcing medizinischer Daten in einem Bundesland erlaubt, in einem anderen Land strafbar sein. Insofern wäre eine Strafbarkeit von landesrechtlichen Vorschriften abhängig. Diese Konsequenz mag auf den ersten Blick merkwürdig erscheinen, weil unter Umständen „Strafbarkeitsinseln" entstehen könnten.

Dies könnte letztlich aber nur konsequente Folge des im Grundgesetz in Art. 20 Abs. 1 GG statuierten Bundesstaatsprinzips sein, nach dem die Bundesländer eigene Staatsqualität besitzen. Die Staatsqualität ergibt sich daraus, dass die Länder ein eigenständiges Staatsgebiet, ein eigenes Staatsvolk und eine eigenständige Staatsgewalt haben. Innerhalb des Rahmens und nach Maßgabe des föderativen Systems des Grundgesetzes können die Länder ihre Verhältnisse souverän ordnen. Sofern dies das Grundgesetz kompetenzrechtlich zulässt, ist es konsequent, den Ländern die Möglichkeit zuzusprechen, Rechtfertigungsgründe für das Strafrecht aufzustellen.

Die Frage ist dahingehend zu stellen, ob die Kompetenzregelungen des Grundgesetzes eine Rechtfertigung von Handlungen, die den Tatbestand des § 203 StGB erfüllen, auf Landesebene zulassen. Nach Art. 74 Abs. 1 Nr. 1 GG ist das Strafrecht Gegenstand der konkurrierenden Gesetzgebung. Die Länder dürfen in diesem Bereich nach Art. 72 Abs. 1 GG tätig werden, „solange und soweit der Bund von seiner Gesetzgebungszuständigkeit nicht durch Gesetz Gebrauch gemacht hat". Für den Bereich des Strafrechts sind die Länder daher, soweit bundesgesetzliche Straftatbestände bestehen, hinsichtlich eigener Straftatbestände gesperrt. Damit ist nicht gesagt, dass die Länder auch an dem Erschaffen neuer Rechtfertigungsgründe gehindert sind. Man könnte sich auf den Standpunkt stellen, dass dort, wo der Bund keine Rechtfertigungsgründe vorgesehen hat, die Länder berechtigt sind, bei entsprechender Gesetzgebungskompetenz tätig zu werden[402]. In diesem Sinne hat die Rechtsprechung für den den Ländern zugeordneten Bereich

[402] Vgl. Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 13; nach h. M. ist auch Art. 74 Abs. 1 Nr. 1 GG kein Hinderungsgrund, weil zum Strafrecht im Sinne dieser Norm nur die Regelung staatlicher Reaktion auf Straftaten gehören sollen, die an die Straftat anknüpfen, ausschließlich für Straftäter gelten und ihre sachliche Rechtfertigung auch aus der Anlasstat beziehen, vgl. BVerfG vom 10.02.2004, Az.: 2 BvR 834/02.

des Schulwesens entschieden[403]. In Frage stand die Rechtfertigung einer Körperverletzung nach § 223 StGB durch das Züchtigungsrecht des Lehrers.

Die Argumentationslinie der Rechtsprechung ist nicht bedenkenfrei. Allerdings bestand die Besonderheit, dass der Rechtfertigungsgrund des Züchtigungsrechts als gewohnheitsrechtlich anerkannt angesehen wurde. Auch wenn das Züchtigungsecht aus dem dienstlichen Erziehungsauftrag, der in den Bereich der Landeszuständigkeit fällt, abgeleitet wird, besteht über die Anerkennung als Gewohnheitsrecht ein übergeordneter, das Landesrecht überschreitender Bezug.

Gewichtiger erscheinen jedoch Bedenken, die sich aus dem Aspekt der Garantiefunktion des Tatbestandes und dem Grundsatz „Bundesrecht bricht Landesrecht", Art. 31 GG, ergeben[404]. Von der in § 1 StGB abgegebenen, verfassungsrechtlich durch Art. 103 Abs. 2 GG abgesicherten Garantie wird der so genannte „Garantietatbestand" erfasst[405]. Dieser beinhaltet alle Voraussetzungen strafbaren Verhaltens, also auch die Rechtswidrigkeit. Die Frage der Rechtfertigung kann daher auch bei bestehender Gesetzgebungskompetenz der Länder, bezogen auf die Materie, aus der der Erlaubnissatz stammt, z.B. Schul- oder Pressewesen, nicht einfach getrennt behandelt werden. Der landesrechtliche Erlaubnissatz bezieht sich auf das bundesgesetzlich geregelte strafbewehrte Verhalten und hat mittelbar Einfluss auf die Strafbarkeit, auch wenn er auf dem Boden der herrschenden Tatbestandslehre nicht das den Unrechtsgehalt prägende Verhalten beschreibt[406]. Den Länder darf auch bei gegebener Gesetzgebungszuständigkeit hinsichtlich der Materie des Erlaubnissatzes kein allgemeines „Rechtfertigungsfindungsrecht" zustehen. Das Argument, dass sich Erlaubnissätze zugunsten des Täters auswirken und daher kein Konflikt mit § 103 Abs. 2 GG droht, ist nur teilweise zutreffend. Ist beispielsweise in einem Land ein Verhalten aufgrund landesrechtlicher Vorschriften erlaubt, während es in einem anderen Bundesland strafbar ist, bedeutet dies eine Einschränkung von Rechtfertigungsmöglichkeiten[407].

---

[403] BGHSt 6, 276 und 11, 244.
[404] Vgl. Kühne, in: Frommann/Mörsberger/Schellhorn, Sozialdatenschutz, S. 157.
[405] Vgl. Lenckner, in: Schönke/Schröder, StGB, Vorb. §§ 13 ff. Rn. 43 f.; Wessels/Beulke, Strafrecht AT Rn. 44, 117.
[406] Zum Unrechtstatbestand vgl. Wessels/Beulke, Strafrecht AT Rn. 117 ff., vgl.
[407] Anders die h.M., vgl. Eser in Schönke/Schröder, StGB, § 1 Rn. 14; Rönnau, in: Leipziger Kommentar StGB, Vor § 32 Rn. 68.

Neben der kompetenzrechtlichen Zulässigkeit ist für das Verhältnis von landesrechtlicher Rechtfertigungsregelung und bundesgesetzlichem Deliktstatbestand Art. 31 GG zu beachten[408]. Hiernach darf das Landesrecht nicht im Widerspruch zum Bundesrecht stehen. In Kollisionsfällen geht das Bundesrecht vor. Die nähere Ausgestaltung des in Art. 31 GG dargelegten Grundsatzes hinsichtlich des Strafrechts ist in den §§ 1 ff. EGStGB erfolgt[409]. Nach Art. 4 Abs. 2 EGStGB sind dem Landesgesetzgeber alle Materien verschlossen, die bereits im StGB abschließend geregelt sind. Daher kann nur dann eine landesrechtliche Rechtfertigung möglich sein, wenn diese in dem bundesgesetzlichen Tatbestand angelegt ist und der Regelungsbereich, aus dem der Rechtfertigungsgrund stammt, der ausschließlichen oder konkurrierenden Gesetzgebungszuständigkeit der Länder zugeordnet ist.

Zwar geht es nicht um die Schaffung eigener oder ergänzender landesgesetzlicher Straftatbestände, sondern um Rechtfertigungsgründe. Diese können aber ebenso unmittelbar zur Strafbarkeit führen, selbst wenn man die Rechtfertigungsgründe mit der h.M. im strafrechtlichen Schrifttum nicht als negative Tatbestandsmerkmale auffasst[410]. Somit liegt es in den Händen der Länder, unmittelbar auf die Strafbarkeit Einfluss zu nehmen, indem sie in den Bereichen, in denen sie die Gesetzgebungszuständigkeit haben, Erlaubnissätze aufstellen. Dies darf unter dem Gesichtspunkt des Art. 31 GG und des § 4 Abs. 2 EGStGB nur dann der Fall sein, wenn dies in dem bundesgesetzlichen Tatbestand angelegt ist und damit eine abschließende Regelung nicht gegeben ist.

Angelegt ist eine landesrechtliche Rechtfertigung beispielsweise in den verwaltungsakzessorischen Straftatbeständen der §§ 324 ff. StGB, aber auch in § 284 StGB, der das unerlaubte Veranstalten eines Glückspiels zum Gegenstand hat. Gerade an letzter Norm, die in jüngster Zeit aktuell geworden ist, kann das Ausgeführte verdeutlicht werden[411]. Sofern man die in § 284 StGB genannte behördliche

---

[408] Nach Kühne scheitert eine bundesgesetzliche Regelung an Art. 31 GG, vgl. Kühne, Berufsrecht für Psychologen, S. 132; a.A. die h.M., vgl. Bruns, Die Schweigepflicht der Sozialen Dienste der Justiz, S. 133.

[409] Vgl. dazu Tröndle/Fischer, StGB, Einleitung Rn. 2; Eser, in: Schönke/Schröder, StGB, Vorb. zu § 1 Rn. 43 ff.

[410] Vgl. Wessels/Beulke, Strafrecht AT Rn. 124, eingehend zur der Lehre von den negativen Tatbestandsmerkmalen Rönnau, in: Leipziger Kommentar StGB, Vor § 32 Rn. 11ff.

[411] Vgl. nur die Entscheidung des Bayerischen Verwaltungsgerichtshofs vom 29. September 2004, Az: 24 BV 03.3162; in dieser Entscheidung ging es zum einen um den Begriff „Glücksspiel“ i.S.v. § 284 StGB, zum anderen um die Frage der Reichweite einer Erlaubnis nach dem Recht der ehemaligen DDR.

Erlaubnis als Rechtfertigungsgrund auffasst, wird auch auf landesrechtliche Rechtfertigungsgründe verwiesen. Dies ergibt sich daraus, dass bestimmte Bereiche des Glücksspiels, beispielsweise Lotterien und Wetten, nur aufgrund landesrechtlicher Gesetze erlaubt werden können, da hierfür die Gesetzgebungszuständigkeit bei den Ländern liegt[412]. Insofern wird eine bundeseinheitliche Strafbarkeit gewährleistet, obwohl die Erlaubnisvoraussetzungen in den Bundesländern unterschiedlich geregelt werden können[413]. Solch ein Verweis auf landesrechtliche Vorschriften, der über eine zulässige Blankettnorm eröffnet wird[414], begegnet unter dem Gesichtspunkt des Art. 31 GG oder dem Gebot der Einheit der Rechtsordnung kaum Bedenken.

Für den Bereich des § 203 StGB ist diese Beurteilung nicht so leicht möglich. Zwar wird auch § 203 StGB als Blankettstrafgesetz bezeichnet, eine Vereinbarkeit mit Art. 31 GG kann aber aus diesem Grund nicht einfach unterstellt werden. Sicherlich bedarf das Merkmal „unbefugt“ der Ausfüllung[415]. Dennoch ist fraglich, ob eine bundeseinheitliche Strafbarkeit gewährleistet ist. Denn im Vergleich beispielsweise zu § 284 StGB bestehen Unterschiede. Bei § 284 StGB ist dem Normadressaten deutlich vor Augen geführt, dass nur bei einer behördlichen Erlaubnis eine Straflosigkeit in Betracht kommt. Das Landesrecht beschränkt sich darauf, die Erlaubnisvoraussetzungen aufzustellen. Es steht für jeden Normadressaten fest, dass ohne eine behördliche Erlaubnis das in § 284 StGB tatbestandlich beschriebene Verhalten zur Strafbarkeit führt. Dies gilt unabhängig davon, in welchem Bundesland die Handlung ausgeführt wird.

Um die behördliche Erlaubnis zu erlangen, muss der Betroffene die öffentlich-rechtlichen Vorschriften beachten, die allein für die Erteilung der Erlaubnis maßgeblich sind. In der Regel sind Erlaubnispflichtigkeit und Erlaubnisfähigkeit zu prüfen. Die öffentlich-rechtlichen Vorschriften, nach denen gegebenenfalls eine Erlaubnis beantragt und erteilt werden muss, greift § 284 StGB pauschal über das Erfordernis einer behördlichen Erlaubnis auf. Allein an das Ergebnis, also das

---

[412] Zutreffend der Beschluss des OVG Lüneburg vom 4. März 2003, Az.: 11 ME 420/02.
[413] So BayVGH vom 29. September 2004, Az.: BV 03.3162; zu weiteren Konsequenzen einer fehlenden landesrechtlichen Erlaubnis vgl. OLG Celle vom 01.02.2007, Az.: 13 U 195/06.
[414] Ein Verstoß gegen das Bestimmtheitsgebot, nulla poena sine lege certa, aus Art. 103 Abs. 2 GG wird bei § 284 StGB abgelehnt, vgl. nur die Entscheidung des Bayerischen Verwaltungsgerichtshofs vom 29. September 2004, Az.: 24 BV 03.3162; allgemein zu Blankettstrafvorschriften und ihrer Zulässigkeit Eser, in: Schönke/Schröder StGB, § 1 Rn. 18a.
[415] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 13.

Vorliegen einer Erlaubnis, knüpft § 284 StGB an. Die Bereiche der bundesrechtlichen Strafbarkeitsvoraussetzungen und eventuelle landesrechtliche Vorschriften, die die Erlaubnis regeln, haben ihre eigenständige Bedeutung. Sie sind hintereinander geschaltet und geraten nicht in Kollision. Die landesrechtlichen Erlaubnisvoraussetzungen verfolgen keine Strafzwecke. Daher kann zutreffend von bundeseinheitlichen Strafbarkeitsvoraussetzungen bei § 284 StGB ausgegangen werden.

Dies gilt auch, wenn nach Landesrecht keine Möglichkeit für eine Erlaubnis besteht, da eine landesrechtliche Entscheidung für oder gegen eine Erlaubnismöglichkeit nicht unmittelbar auf bundesrechtliche Strafbarkeitsvoraussetzungen übergreift. Ob eine Erlaubnis nicht erteilt wird, weil die landesrechtlich festgesetzten Voraussetzungen nicht vorliegen oder eine Erlaubnis gar nicht vorgesehen ist, macht unter dem Gesichtspunkt der Gewährung einer bundeseinheitlichen Strafbarkeit keinen Unterschied.

Ähnlich verhält es sich bei den Straftatbeständen der §§ 242, 293 StGB bezüglich des normativen Tatbestandmerkmals „fremd“ in 242 StGB[416], bzw. „fremdes Fischereirecht“ in § 293 StGB[417]. Auch hier ist als Vorfrage zu beantworten, was „fremd“ im Sinne der Norm bedeutet. Die Festlegung kann je nach Kompetenz durch Bundes- oder durch Landesrecht erfolgen. Erst wenn dies durch die Rechtsordnung festgelegt worden ist, kann sinnvollerweise der Straftatbestand „zum Zuge kommen“. Die Festlegung dessen, was „fremd“ ist bedarf keiner strafrechtlichen Betrachtung. Vielmehr muss durch die Rechtsordnung insgesamt eine strafrechtsunspezifische Zuordnung erfolgen, an die dann das Strafrecht anknüpft.

§ 203 StGB stellt demgegenüber ein unbefugtes Offenbaren unter Strafe. Unterschiedliche landesrechtliche Befugnisse können unmittelbar zu unterschiedlicher Strafbarkeit des gleichen Verhaltens führen. Bei § 203 StGB wird der Systematik nach über das Merkmal „unbefugt“ nicht wie bei § 284 StGB auf einen vorgeschalteten verwaltungsrechtlichen Akt, der sich getrennt und nach einem anderen Rechtsgebiet beurteilt, verwiesen. Befugnisnormen können in jedem Rechtsgebiet geregelt sein, also auch im Landesrecht. Die Verweisung in § 203 StGB ist zwar

[416] Auch Landesrecht kann maßgeblich sein, vgl. Tröndle/Fischer, StGB, § 242 Rn. 9.
[417] Eser/Heine, in: Schönke/Schröder, StGB, § 293 Rn. 9.

offen, enthält aber nicht die Aussage, dass landesrechtliche Befugnisse und Bundesstrafrecht nicht kollidieren könnten. Es stellt sich zwangsläufig die Frage, ob diese außerstrafrechtlichen, landesrechtlichen Befugnisnormen nicht nur innerhalb des Rechts- und Hoheitsgebietes, dem sie entstammen, sondern auch für den bundesgesetzlichen Straftatbestand Bedeutung beanspruchen können. Eine Kollision erscheint nicht schon wegen der Notwendigkeit einer Ausfüllung des Merkmals „unbefugt“ ausgeschlossen.

Andererseits werden in § 203 StGB selbst keine näheren Vorgaben gemacht, wann eine Befugnis zum Offenbaren vorliegt. Eine Kollision ist daher dann abzulehnen, wenn die Befugnisnorm speziell auf die Besonderheiten der Rechtsmaterie, aus der sie stammt, zugeschnitten ist und einen eigenständigen Anwendungsbereich beansprucht. Dies passt zu den Forderungen des Bundesverfassungsgerichts nach bereichsspezifischen Regelungen für den Umgang mit personenbezogenen Daten, die gesetzliche Ermächtigungsgrundlagen für den Eingriff in das Recht auf informationelle Selbstbestimmung beinhalten. Die Gefahr von „Strafbarkeitsinseln“ relativiert sich, wenn man bedenkt, dass die landesrechtlichen Regelungen mit dem höherrangigen Recht auf informationelle Selbstbestimmung vereinbar sein müssen. Im Kern wird das Recht auf informationelle Selbstbestimmung ebenfalls durch § 203 StGB geschützt, wenn auch mit Divergenzen zum Datenschutzrecht. Insofern gewährt die Klammer des informationellen Selbstbestimmungsrechts eine gewisse Rechtseinheit, die der Bildung von „Strafbarkeitsinseln“ ausreichend entgegenwirkt.

Die Regelung der Befugnis im Landesrecht darf aber nicht über den Umweg der Landeskompetenz auf eine Schwächung des Strafrechtsschutzes durch § 203 StGB abzielen[418]. Unter dieser Voraussetzung ist im Ergebnis davon auszugehen, dass auch im Landesrecht ein Erlaubnissatz hinsichtlich § 203 StGB geregelt sein kann. Es ist eine andere Frage, ob die landesrechtliche Regelung mit höherrangigem Recht, in diesem Zusammenhang ist vor allem das Recht auf informationelle Selbstbestimmung von Bedeutung, vereinbar ist, oder ob eine nicht ausdrücklich als Rechtfertigung formulierte Regelung aufgrund einer Gesetzesauslegung als

[418] Vgl. zu dem umgekehrten Fall, dass der Bundesgesetzgeber nicht über den Vorwand des Strafrechts eine Materie an sich ziehen darf, die tatsächlich aufgrund bestehender Landeskompetenzen sachnäher durch die Länder geregelt werden müsste, BVerfG vom 16.03.2004, Az.:1 BvR 1778/01.

strafrechtlicher Erlaubnissatz zu lesen ist. Zu prüfen ist im Folgenden, ob das Landesrecht solche Offenbarungsbefugnisse enthält, die das Outsourcing medizinischer Daten betreffen.

6. Sektorspezifische Regelungen im Landesrecht

Außerhalb des allgemeinen Datenschutzrechts der Länder finden sich im Gesundheitswesen spezielle sektorspezifische Regelungen der Länder, die in unterschiedlichem Ausmaß das Heranziehen privater Dritter ermöglichen[419]. Sektorspezifische Regelungen finden sich insbesondere im Krankenhausbereich. Sie betreffen den Umgang mit personenbezogenen Daten in bestimmten Bereichen des Gesundheitswesens. Vielfach findet sich dabei das Institut der Auftragsdatenverarbeitung wieder. Allerdings sind die Länderregelungen speziell auf das Gesundheitswesen bezogen, berücksichtigen die Schutzbedürftigkeit und Schutzwürdigkeit von Patientendaten, richten sich an die schweigepflichtigen Berufsausübenden und beziehen auch den Datenempfänger im Rahmen der Auftragsdatenverarbeitung ein. Insofern kann nicht auf die Argumentation zu den Regelungen der Auftragsdatenverarbeitung in § 11 BDSG verwiesen werden. Vielmehr muss eine Rechtfertigungswirkung hinsichtlich § 203 StGB näher untersucht werden.

Als mögliche strafrechtliche Erlaubnisnorm ist § 7 Gesundheitsdatenschutzgesetz Nordrhein-Westfalen, GDSG NW, diskutiert worden. Das GDSG NW findet insbesondere auf in Nordrhein-Westfalen nach dem SGB V zugelassene Krankenhäuser Anwendung, betrifft hinsichtlich des Outsourcings medizinischer Daten also öffentliche Stellen der Leistungserbringung im System der gesetzlichen Krankenversicherung**,** die einer Schweigepflicht nach § 203 StGB Abs. 1 Nr. 1 StGB unterliegen. § 7 Abs. 2 GDSG NW formuliert wie folgt: „eine Verarbeitung im Auftrag ist nur nach Maßgabe der Absätze 2 bis 4 zulässig“. § 7 Abs. 3 i.V.m. Abs. 4 GDSG NW erlaubt unter bestimmten Voraussetzungen die Auftragsvergabe auch an private Unternehmen. In einer zu § 7 GDSG NW ergangenen Entscheidung des OLG Düsseldorf wurde § 7 GDSG NW als strafrechtlicher Erlaub-

[419] Vgl. Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 192-194.

nissatz aus verschiedenen Erwägungen abgelehnt. Im Ergebnis ist diese Entscheidung auf Zustimmung in der Literatur gestoßen[420].

Nach der hier vertretenen Auffassung kann entgegen dem OLG Düsseldorf auch eine landesrechtliche Vorschrift eine Befugnis im Sinne des § 203 StGB darstellen. In dem dargelegten Rahmen ist es dem Landesgesetzgeber möglich, strafrechtliche Befugnisnormen zu schaffen. Es ist nicht ersichtlich, dass § 7 GDSG NW gezielt den strafrechtlichen Geheimnisschutz nach § 203 StGB unterlaufen will. Vielmehr will § 7 Abs. 3 GDSG NW im Zusammenhang mit der Regelung des Umgangs mit besonderen personenbezogenen Daten die Wahrung der ärztlichen Schweigepflicht sichergestellt wissen. Auch fällt die Regelung des Krankenhausbereiches, soweit nicht die wirtschaftliche Sicherung und die Regelung der Krankenhauspflegesätze betroffen sind, Art. 74 Abs. 1 Nr. 19a GG, in die ausschließliche Gesetzgebungskompetenz der Länder. Diese Gesetzgebungskompetenz wird auch nicht dadurch beeinträchtigt, dass im GDSG NW Regelungen zum Schutz personenbezogener Daten getroffen werden, da § 1 Abs. 2 Nr. 2 BDSG den Vorrang der Länderregelungen für den Bereich der öffentlichen Stellen sicherstellt. Die rechtfertigende Wirkung kann also nicht pauschal mit dem Hinweis auf Landesrecht abgelehnt werden.

Auch das OLG Düsseldorf stützt seine Ablehnung maßgeblich auf andere Erwägungen. Das Gericht stellt auf § 7 Abs. 3 GDSG NW ab, der verlangt, dass „beim Auftragnehmer die Wahrung der Datenschutzbestimmungen dieses Gesetztes und der ärztlichen Schweigepflicht sichergestellt ist“. Bei Auftragnehmern, die nicht zu dem in § 203 StGB aufgezählten Personenkreis zählen, könne die Wahrung der ärztlichen Schweigepflicht denknotwendig nicht eingehalten werden, denn diese Auftragnehmer könnten, weil sie § 203 StGB nicht unterlägen, die ärztliche Schweigepflicht auch nicht brechen[421]. Das Gericht erkennt, dass bei einer derart engen Auslegung der Norm diese inhaltsleer erscheint. Selbstverständlich kann nur ein Schweigepflichtiger die Schweigepflicht nach § 203 StGB verletzen. Es ist daher in der Tat fraglich, ob die „ärztliche Schweigepflicht“ in § 7 Abs. 3 GDSG NW rechtstechnisch zu verstehen ist.

---

[420] Ehmann, in einer Anmerkung zum Urteil des OLG Düsseldorf C ,1997, S. 538.
[421] OLG Düsseldorf CR 1997, S. 538.

Das Gericht geht auf die Möglichkeit einer anderen Lesart ein, nämlich dahingehend, dass mit der „ärztlichen Schweigepflicht eine Umschreibung einer auf die Patientendaten bezogenen Verschwiegenheit“ gemeint ist. Aber auch dann ist keine Offenbarungsbefugnis anzunehmen. Denn eine Befugnis zum Offenbaren folgt nicht schon daraus, dass auch der Empfänger schweigepflichtig ist. Anderenfalls müsste jede Weitergabe von Patientendaten durch einen Arzt an einen Dritten „unter dem Siegel der Verschwiegenheit“ als gerechtfertigt anzusehen sein. Auf das Erfordernis einer Patienteneinwilligung kann nicht verzichtet werden[422].

In einer Stellungnahme zu diesem Urteil stimmt Ehmann den Ausführungen des OLG Düsseldorf zur Frage der Rechtfertigung durch § 7 GDSG NW im Wesentlichen zu. Dem Wortlaut nach hat der nordrhein-westfälische Gesetzgeber § 7 GDSG NW eindeutig nicht als strafrechtlichen Erlaubnissatz ausgestaltet[423]. Zutreffend ist die Einschätzung, dass bei einem „gewöhnlichen“ Outsourcing-Unternehmen, also bei einem Unternehmen, das nicht ein Krankenhaus ist, das Privileg der Beschlagnahmefreiheit gemäß § 97 Abs. 2 StPO nicht gegeben ist, bei einem Krankenhaus dagegen sehr wohl[424]. Verwiesen wird schließlich darauf, dass nach der Rechtsprechung des Bundesgerichtshofs wirtschaftliche Erwägungen keinesfalls die Verletzung der ärztlichen Schweigepflicht rechtfertigen können, wenn man auf der anderen Seite die potenziell schädliche Wirkung eines Bekanntwerdens sensibler Informationen über die Gesundheit für den Betroffenen in seinem sozialen Umfeld berücksichtigt[425].

In der Bewertung erscheinen die Argumente, die gegen § 7 GDSG NW als strafrechtliche Erlaubnis sprechen, gewichtig. In der Tat will § 7 GDSG NW die Datenverarbeitung im Auftrag für Teilvorgänge der automatischen Datenverarbeitung unter dem Gesichtspunkt der Kostenreduzierung ermöglichen. Die Einstellung dieses Aspekts spricht vor dem Hintergrund der Rechtsprechung des Bundesgerichtshofes gegen eine Rechtfertigung mit strafrechtlicher Wirkung und für eine rein datenschutzrechtliche, spezielle Erlaubnisnorm. Zutreffend ist auch, dass allein aus dem Umstand einer Schweigepflicht des Empfängers nicht auf eine

---

[422] OLG Düsseldorf CR 1997, S. 538 unter Hinweis auf Körner-Dammann, NJW 1992, S. 729f. und König, NJW 1991, S. 755f.
[423] Ehmann, CR 1997, S. 539.
[424] Ehmann, CR 1997, S. 539 mit dem Hinweis auf die Entscheidungen des Bayerischen Verfassungsgerichtshofs CR 1989, S. 530 und des Bundesverfassungsgerichts CR 1991, S. 296.
[425] BGH NJW 1991, S. 2955, 2957.

strafrechtliche Befugnis geschlossen werden kann und insofern eine gemeinsame Schweigepflicht nur bedingt zur Begründung eines strafrechtlichen Erlaubnissatzes herangezogen werden kann[426].

Auf der anderen Seite finden sich Einwände gegen die Argumentation des OLG Düsseldorf, insbesondere hinsichtlich der Argumentation zu § 97 Abs. 2 StPO. § 7 Abs. 3 GDSG NW, nach dem die Wahrung der ärztlichen Schweigepflicht sichergestellt sein muss, kann auch in dem Sinne verstanden werden, dass der Auftraggeber die Datenverarbeitung so zu organisieren hat, dass auch das Beschlagnahmeverbot des § 97 StPO greift. Der Umstand, dass in der Regel bei einem privaten Unternehmer, der nicht zum Täterkreis des § 203 StGB zählt, keine Beschlagnahmefreiheit vorliegt, zwingt nicht zu der Annahme, dass die ärztliche Schweigepflicht hinsichtlich des Aspekts der Beschlagnahmefreiheit nicht sichergestellt werden kann. Es mag regelmäßig so sein, dass § 97 StPO bei einem selbständigen Auftragnehmer nicht eingreift. Daraus kann aber nicht geschlossen werden, dass durch bestimmte organisatorische und technische Maßnahmen der externe Auftragnehmer nicht so eingebunden werden kann, dass sich das Beschlagnahmeverbot auch auf ihn erstreckt.

Dafür spricht auch folgende Überlegung. Wäre der Auftragnehmer selbst schweigepflichtig, wäre eine Sicherstellung der ärztlichen Schweigepflicht nicht überflüssig. Denn diese gilt wie dargestellt grundsätzlich auch zwischen zwei Schweigepflichtigen. Folglich macht es Sinn, wenn der Auftragnehmer seine Schweigepflicht, im Sinne seiner Verantwortung für die Einhaltung dieser Schweigepflicht, sicherstellt, unabhängig davon, ob der Auftragnehmer einer eigenen Schweigpflicht unterliegt. Bei einer derartigen Interpretation könnte § 7 GDSG NW eine Rechtfertigung bieten, wenn durch organisatorische und technische Sicherheitsmaßnahmen der Auftragnehmer derart eingebunden ist, dass er eine einem Gehilfen vergleichbare Stellung hat. Eine solche Interpretation könnte auch im Hinblick auf Art. 12 GG angezeigt sein, da sie dem Auftraggeber ein hohes Maß an Organisationshoheit in dem Bereich der Berufsausübung belässt.

[426] Auch die (Muster)-Berufsordnung der Ärzte geht davon aus. Denn in § 9 Abs. 4 MBO-Ä ist geregelt, dass zwischen Ärzten eine Weitergabe von Geheimnissen nur dann erfolgen darf, wenn ein Einverständnis des Patienten vorliegt oder anzunehmen ist.

Im Ergebnis ist der Auffassung, dass § 7 GDSG NW eine strafrechtliche Befugnis darstellt, dennoch nicht zu folgen. Die Forderung, in § 7 Abs. 3 GDSG NW die Wahrung der ärztlichen Schweigepflicht sicherzustellen, bleibt als Anknüpfungspunkt zu unbestimmt, um darin überzeugend die Grundlage für eine Durchbrechung der ärztlichen Schweigepflicht zu sehen. § 7 Abs. 3 GDSG NW gibt keine Hinweise darauf, wie die Wahrung der Schweigepflicht sicherzustellen ist. Es ist nicht erkennbar, dass der Gesetzgeber nach einer Abwägung der Interessen mit § 7 GDSG NW eine Durchbrechung der ärztlichen Schweigepflicht wollte, ohne das Schutzniveau des § 203 StGB zu gefährden. Vielmehr deutet die Formulierung in § 7 Abs. 3 GDSG NW darauf hin, dass eine Zulässigkeit der Datenverarbeitung nach § 203 StGB vorausgesetzt wird und § 7 Abs. 3 GDSG NW daran anknüpfend datenschutzrechtliche Aspekte sektorspezifisch regelt.

Auch der Gesichtspunkt der Berufsfreiheit vermag darüber nicht hinwegzuhelfen, denn betroffen ist auf der Seite des Berufsträgers ein Randbereich der Berufsausübung, während auf der anderen Seite des Geheimnisträgers ein Eingriff in den Kernbereich des Rechts auf informationelle Selbstbestimmung steht. Allenfalls dann, wenn mit der Frage der Organisation der Berufsausübung die Existenz des Berufsausübenden zusammenhängt, also faktisch ein Berufshindernis errichtet würde, könnte Art. 12 GG bzw. Art. 14 GG, von dem auch das Recht auf den eingerichteten und ausgeübten Gewerbebetrieb erfasst wird[427], durchschlagen. Dass die Existenz eines Unternehmens durch Outsourcing-Entscheidungen im Bereich medizinischer Daten betroffen ist, wird kaum der Fall sein.

Hinzu kommt, dass über die Möglichkeit der Einwilligung ein Outsourcing unabhängig von einer gesetzlichen Befugnisnorm als Möglichkeit verbleibt. Art. 12 GG bzw. Art. 14 GG zwingen daher nicht dazu, in § 7 GDSG NW eine strafrechtliche Befugnisnorm zu sehen. Damit ist nicht gesagt, dass nicht innerhalb einer bestehenden allgemeinen strafrechtlichen Rechtfertigungsnorm, die eine Interessenabwägung erfordert, Art. 12 GG bzw. Art. 14 GG in die Abwägung eingestellt werden können. Darauf wird im Rahmen der allgemeinen strafrechtlichen Recht-

[427] Nach zutreffender Ansicht ist das Recht am eingerichteten und ausgeübten Gewerbebetrieb Eigentum im Sinne des Art. 14 GG, vgl. Papier, in: Maunz/Dürig, GG, Art. 14 Rn. 95. Der Gewerbebetrieb ist nicht an der Gewerbeordnung auszurichten, sondern erfasst jedes auf Erwerb ausgerichtete Unternehmen, mithin auch freiberufliche Tätigkeit, soweit sie mit personellen und sachlichen Mitteln, also betrieblich, organisiert ist, beispielsweise in einer Arzt oder Anwaltspraxis, Papier, in: Maunz/Dürig, GG, Art. 14 Rn. 98; BGH NJW 1986, S. 2499, 2500.

fertigungsgründe noch einzugehen sein. Im Ergebnis zu § 7 GDSG NW bleibt festzuhalten, dass keine strafrechtliche Befugnis hinsichtlich § 203 StGB gegeben ist.

Außer im GDSG NW finden sich in vielen Landeskrankenhausgesetzen Regelungen, die ein Heranziehen privater Dritter zur Patientendatenverarbeitung ermöglichen. Diese Regelungen gehen aber nicht über die Regelungen des § 7 GDSG NW hinaus. So verlangen die Normen entweder, dass eine § 203 StGB entsprechende Schweigepflicht beim Auftragnehmer sichergestellt wird[428], oder dass dem Auftragnehmer eine § 203 StGB entsprechende Schweigepflicht auferlegt wird[429]. Dies gilt letztlich auch für § 49 Krankenhausgesetz Baden-Württemberg**,** der ausdrücklich bestimmt, dass auch ein nach § 203 StGB Schweigepflichtiger befugt Patientendaten weitergeben darf. Allerdings stellt § 48 Abs. 2 Krankenhausgesetz Baden-Württemberg klar, dass Patientendaten im Auftrag des Krankenhauses nur dann verarbeitet werden dürfen, wenn dem Auftragnehmer eine § 203 StGB entsprechende Schweigepflicht auferlegt worden ist. Die Norm setzt ebenfalls eine nach § 203 StGB zulässige Datenverarbeitung voraus und regelt daran anknüpfend die datenschutzrechtliche Zulässigkeit im Krankenhaussektor.

Schließlich kann auch nicht in § 9 Abs. 1 Hamburgisches Krankenhausgesetz eine strafrechtliche Befugnisnorm gesehen werden. Der Wortlaut spricht, anders als von *Ehmann* vermutet[430], nicht für einen strafrechtlichen Erlaubnissatz. Denn nach § 9 Abs. 1 Hamburgisches Krankenhausgesetz darf das Krankenhaus „die Speicherung und die weitere Verarbeitung von Patientendaten einem Auftragnehmer übertragen, wenn dieser sich verpflichtet, die für das Krankenhaus geltenden Datenschutzbestimmungen einzuhalten“. Die Norm bezieht sich nicht auf die ärztliche Schweigepflicht und bleibt sogar hinter den Anforderungen des § 11 BDSG zurück. Daher ist die Formulierung „darf“ zwar vom Wortlaut als Erlaubnisnorm ausgestaltet, beschränkt sich aber allein auf das (Patienten-) Datenschutzrecht im Krankenhausbereich.

---

[428] Vgl. § 36 Abs. 9 S. 1 Landeskrankenhausgesetz Rheinland-Pfalz, § 29 Abs. 6 S. 5 Saarländisches Krankenhausgesetz, § 33 Abs. 10 Sächsisches Krankenhausgesetz.
[429] Vgl. § 6 Abs. 3 S. 2 Bayerisches Krankenhausgesetz.
[430] Ehmann, CR 1997, S. 539.

7. Landesdatenschutzgesetze

Nach § 1 Abs. 2 Nr. 2 BDSG gehen bei öffentlichen Stellen der Länder Landesgesetze zum Datenschutz dem BDSG vor[431]. Insofern kommen als Erlaubnistatbestände Normen der Landesdatenschutzgesetze in Betracht. Die Landesgesetze enthalten für den Bereich der Datenverarbeitung im Auftrag Regelungen, die weitgehend dem § 11 BDSG entsprechen[432]. Aus denselben Gründen, die bei § 11 BDSG angeführt wurden, scheidet daher eine Qualifizierung als strafrechtliche Erlaubnisnorm aus.

8. Allgemeine strafrechtliche Rechtfertigungsgründe

Befugnisse zum Offenbaren von Geheimnissen können sich schließlich unmittelbar aus dem StGB oder aus anerkannten strafrechtlichen Rechtfertigungsgrundsätzen ergeben. Zu prüfen ist im Folgenden, inwieweit solche strafrechtlichen Rechtfertigungsgründe als Grundlage für das Outsourcing medizinischer Daten dienen können. In Betracht zu ziehen sind die Wahrnehmung berechtigter Interessen, § 193 StGB, die Grundsätze über die Abwägung widerstreitender Pflichten oder Interessen sowie der rechtfertigende Notstand, § 34 StGB.

a) Wahrnehmung berechtigter Interessen

Die Wahrnehmung berechtigter Interessen ist in § 193 StGB geregelt. § 193 StGB enthält für die Beleidigungstatbestände besondere Rechtfertigungsgründe[433]. Denkbar wäre, dass im Outsourcing medizinischer Daten eine Wahrnehmung berechtigter Interessen liegt. Sofern § 193 StGB auf § 203 StGB übertragbar ist, wäre zu überlegen, ob sich daraus eine Befugnis zum Offenbaren ergibt, die ein Outsourcing medizinischer Daten ermöglicht.

---

[431] Für den Krankenhausbereich sind sektorspezifische Datenschutzregelungen zur Auftragsdatenverarbeitung zu beachten, vgl. zum Überblick Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 192- 194.

[432] Vgl. nur Art. 6 BayDSG.

[433] Tröndle/Fischer, StGB, § 193 Rn. 1; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 131.

Der Anwendungsbereich des § 193 StGB außerhalb der Beleidigungstatbestände im StGB ist umstritten. Die h.M. lehnt eine Anwendung auf andere strafbare Handlungen ab[434]. Sieht man allgemein in § 193 StGB einen Anwendungsfall einer Interessenabwägung[435], erscheint die Auffassung zweifelhaft. Man könnte, wie von einem Teil der Literatur vertreten, annehmen, dass in § 193 StGB ein allgemeiner Grundsatz enthalten ist, der sich auf andere Straftatbestände übertragen lässt[436].

Eine analoge Anwendung des § 193 StGB ist jedoch abzulehnen[437]. Zwar mag es sein, dass § 193 StGB eine aktive Komponente enthält und sich damit gegenüber den meisten anderen Rechtfertigungsgründen, die defensiv ausgerichtet sind, unterscheidet. Jedoch spricht gerade diese Besonderheit gegen eine analoge Anwendung. Denn der Rechtfertigungsgrund der Wahrnehmung berechtigter Interessen ist bewusst im Zusammenhang mit den Beleidigungstatbeständen ausgestaltet worden. Er setzt eine Beleidigung nach der äußeren und inneren Tatseite voraus[438], die unter bestimmten in § 193 StGB genannten Fallgruppen gerechtfertigt ist, sofern nicht zugleich eine Formalbeleidigung gegeben ist. Somit wird allein der Inhalt einer Äußerung geschützt.

Berücksichtigt man weiter, dass die Fallgruppen in § 193 StGB sich überwiegend als Konkretisierung des Rechtfertigungsgrundes der Wahrnehmung berechtigter Interessen darstellen, zeigt sich, dass § 193 StGB mit seiner aktiven Dimension speziell für Situationen der Ehrverletzung geschaffen worden ist. Eine Meinungsäußerung, die aus einer anerkannten Berechtigung einem anderen gegenüber erfolgt, greift zwangsläufig aktiv in ein fremdes Rechtsgut ein. Insofern hat § 193 StGB vor dem Hintergrund des Art. 5 Abs. 1 GG eine kommunikationssichernde

---

[434] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 131; Joecks, Studienkommentar StGB, § 193 Rn. 4; Hoyer, in: Systematischer Kommentar StGB, § 193 Rn. 89; Schmitz, JA 1996, S. 954; a.A. Jähnke, in: Leipziger Kommentar StGB (10. Auflage), § 203 Rn. 82; Eser, Wahrnehmung berechtigter Interessen S. 12, 48 ff.; Rogall, NStZ 1983, S. 6.

[435] BGHSt 18, 184; Herdegen, in: Leipziger Kommentar StGB, § 193 Rn. 1 ff.

[436] Vgl. Eser, Wahrnehmung berechtigter Interessen, S. 12, 48 ff., der in § 193 StGB eine verallgemeinerbare Befugnis zu aktiven Eingriffen in fremde Rechtgüter sieht; so wohl auch Meier, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, S. 201f., der aber eine Verortung des Instituts der Wahrnehmung berechtigter Interessen offen lässt.

[437] Im Ergebnis ebenso Hoyer, in: Systematischer Kommentar StGB, § 203 Rn. 89; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 131; Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 75f.; Lenckner, in: Schönke/Schröder, StGB § 203 Rn. 30.

[438] Tröndle/Fischer, StGB, § 193 Rn. 2.

Wirkung. Eine Übertragung auf andere Bereiche ist weder notwendig noch zulässig. Eine planwidrige Regelungslücke ist aus diesem Grund nicht anzunehmen.

Schließlich sprechen noch weitere gewichtige Gründe gegen eine analoge Anwendung des § 193 StGB. Im öffentlichen Bereich bedürfen nach dem Grundsatz des Vorbehalts des Gesetzes, dessen Rechtsgrundlage überwiegend in Art. 20 Abs. 3 GG gesehen wird[439], jedenfalls im Bereich der Eingriffsverwaltung alle belastenden Maßnahmen einer gesetzlichen Grundlage. Auch das BVerfG hat im Volkszählungsurteil auf diesen Aspekt abgestellt und eine ausreichende gesetzliche Grundlage für Eingriffe in das grundrechtlich verankerte Recht auf informationelle Selbstbestimmung verlangt. Das Erfordernis einer gesetzlichen Eingriffsgrundlage hat disziplinierende Funktion und bedingt, dass sich Inhalt, Zweck und Ausmaß des Eingriffs im Wesentlichen unmittelbar aus einer gesetzlichen Regelung ergeben. In Umsetzung dieser Vorgaben sind eine Reihe bereichsspezifischer Regelungen ergangen.

Bei einer Übertragung des Rechtfertigungsgrundes der Wahrnehmung berechtigter Interessen auf § 203 StGB, der weitgehend das informationelle Selbstbestimmungsrecht schützt, würde man dem Gesetzesvorbehalt und dessen Umsetzung im Bereich des informationellen Selbstbestimmungsrechts nicht gerecht werden[440]. Denn die Rechtfertigung eines Eingriffs in das Recht auf informationelle Selbstbestimmung bedeutet eine Eingriffslegitimierung, die faktisch wie eine Eingriffsermächtigung wirkt. Hätte der Gesetzgeber eine Legitimierung im Bereich des informationellen Selbstbestimmungsrechts mit einer „aktiven“ Komponente, vergleichbar § 193 StGB, gewollt, dann hätte er dies gesetzlich ausdrücken können und müssen. Die bewusst fehlende gesetzgeberische Entscheidung darf nicht durch eine analoge Anwendung des § 193 StGB überspielt werden[441].

Im privaten Bereich kann nicht unmittelbar auf den Grundsatz des Gesetzesvorbehalts abgestellt werden. Aus in der Sache ähnlichen Erwägungen ist aber auch in diesem Bereich eine analoge Anwendung abzulehnen. Denn die Übertragung eines postulierten allgemeinen, aus § 193 StGB abgeleiteten Abwägungsgrundsat-

[439] BVerfGE 40, 237, (248); 49, 89, (126); zweifelnd Maurer, Allgemeines Verwaltungsrecht, § 6 Rn. 4.
[440] Hoyer, in: Systematischer Kommentar StGB, § 203 Rn. 89.
[441] Im Ergebnis ebenso Tröndle/Fischer, StGB, § 203 Rn. 42.

zes ist nicht mit dem Bestimmtheitsgebot als Teil des Rechtsstaatsprinzips vereinbar. Die Legitimierung würde ihrem Inhalt und Umfang nach nahezu konturenlos sein. Hinzu kommt, dass in § 34 StGB bzw. in den Grundsätzen über die Abwägung widerstreitender Pflichten oder Interessen ein Abwägungsrahmen bereits vorhanden ist, in den die Wahrnehmung berechtigter Interessen eingestellt werden kann. Dieser in § 34 StGB gesetzlich bereits vorgegebene bzw. durch Rechtsprechung und Literatur nach den Grundsätzen der Abwägung widerstreitender Pflichten oder Interessen herausgearbeitete Abwägungsrahmen, der nach der Konzeption im StGB auf alle Straftatbestände Anwendung findet, ist im Rechtfertigungsgefüge einer Verallgemeinerung der Besonderheit in § 193 StGB unter dem Gesichtspunkt der Bestimmtheit vorzuziehen[442].

Dafür spricht im Übrigen auch ein Blick auf datenschutzrechtliche Erlaubnistatbestände. Nach hier vertretener Auffassung sind diese nicht für § 203 StGB maßgeblich. Bestimmte Wertungen, die sich auf den Gedanken des Schutzes des Rechts auf informationelle Selbstbestimmung zurückführen lassen, können indes wegen den Überschneidungen im Schutzgut im Rahmen des § 203 StGB beachtet werden. Betrachtet man den Erlaubnistatbestand des § 28 BDSG im Bereich der Datenverarbeitung der nicht öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen, zeigt sich, dass die Wahrnehmung berechtigter Interessen nicht als allgemeiner Rechtfertigungsgrund eingreifen kann.

In § 28 Abs. 1 Nr. 2 BDSG ist die Wahrnehmung berechtigter Interessen nur ein zu berücksichtigender Aspekt, der in die Interessenabwägung einzustellen ist. Die Interessen der verantwortlichen Stelle müssen das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen. Ähnliche Einschränkungen in der Wahrnehmung berechtigter Interessen finden sich in § 16 BDSG für die Datenverarbeitung im öffentlichen Bereich. Das Datenschutzrecht greift also den Aspekt der Wahrnehmung berechtigter Interessen nicht als eigenständiges aktives Prinzip auf. Es ist nicht überzeugend, wenn man bei § 203 StGB ein solches allgemeines Prinzip anerkennt.

---

[442] Ähnlich Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 131, der aber darauf abstellt, dass keine Notwendigkeit für eine analoge Anwendung des § 193 StGB besteht.

Neben einer analogen Anwendung des § 193 StGB wird in der Literatur zum Teil vertreten, dass der Rechtsgedanke des § 30 Abs. 4 Nr. 5 AO jedenfalls auf § 203 Abs. 2 StGB übertragbar wäre und zu einer Rechtfertigung führen könne[443]. Diese Auffassung ist aus den gleichen Gründen, die schon gegen eine analoge Anwendung des § 193 StGB angeführt wurden, abzulehnen. Die Besonderheiten in der Steuerverwaltung sind nicht auf § 203 StGB übertragbar[444].

b) Rechtfertigender Notstand, § 34 StGB

Mit der Ablehnung einer analogen Anwendung des § 193 StGB bzw. des § 30 Abs. 4 Nr. 5 AO stellt sich die Frage, ob eine Offenbarung von Geheimnissen im Rahmen von Outsourcingvorhaben medizinischer Daten durch § 34 StGB gerechtfertigt sein kann. Die Frage ist von erheblicher praktischer Bedeutung. Denn eine Rechtfertigung nach § 34 StGB könnte unabhängig von der Einordnung als Gehilfe die strafrechtliche Zulässigkeit beabsichtigter Outsourcingvorhaben bedeuten.

Diese Frage ist in Literatur und Rechtsprechung bisher nur für bestimmte Teilbereiche des Outsourcings behandelt worden. Für den Bereich des Outsourcings von Versicherungsdaten behandelt *Hilgendorf* das Problem einer Rechtfertigung nach § 34 StGB[445]. Weiterhin geht *Wolf* für den Bereich des externen Honorareinzugs auf eine mögliche Rechtfertigung nach § 34 StGB ein und ordnet dabei die Wahrnehmung berechtigter Interessen als einen Aspekt innerhalb der Interessenabwägung bei § 34 StGB ein[446].

Anerkannt ist die Anwendung des § 34 StGB, wenn der Arzt selbst abrechnet und seine Forderung einzieht. Muss er dabei einen Rechtsanwalt einschalten, um die Forderung gerichtlich einzutreiben, ist ein Offenbaren der zur Geltendmachung erforderlichen Daten in der Regel durch § 34 StGB gerechtfertigt[447]. Dies ist beim

---

[443] So insbesondere Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, S. 91.
[444] Im Ergebnis ebenso Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 138.
[445] Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 106f.
[446] Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 78f.
[447] So weitgehend die strafrechtliche Literatur, vgl. Schünemann, in Leipziger Kommentar StGB, § 203 Rn. 133; Cierniak, in: Münchener Kommentar StGB, § 203 Rn. 86; so auch Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 410; anders Ulsenheimer, in: Laufs/Uhlenbruck, Handbuch des Arztrechts, § 72 Rn. 16, der diese Fallgestaltung über das Institut der Wahrnehmung berechtigter Interessen analog § 193 StGB löst; die zivilrechtliche Rechtsprechung vermeidet eine ausdrücklich Einordnung, wenn sie von der Wahrnehmung berechtigter Interessen spricht, vgl. BGH MedR 1991, S. 327, 328; BGH NJW 1996, S. 775, 776.

externen Honorareinzug fraglich. Beim externen Honorareinzug gibt der Arzt auch medizinische Daten des Patienten an eine Verrechnungsstelle weiter. Die Verrechnungsstelle übernimmt aufgrund vorheriger vertraglicher Vereinbarung die Abrechnung, meist einschließlich des Honorareinzugs, für den Arzt[448]. Diese Vorgehensweise kann unter den Begriff Outsourcing, so wie er hier verwendet wird, subsumiert werden, da private Dritte zur eigenen Aufgabenerfüllung herangezogen werden und in Kontakt mit fremden Daten gelangen. Hier ist die Anwendung des § 34 StGB zweifelhaft[449].

Außerhalb dieses Teilbereichs des Outsourcings medizinischer Daten ist eine Rechtfertigung nach § 34 StGB im Bereich des Outsourcings von Bankleistungen in der Literatur diskutiert worden. Insbesondere *Otto* bejaht die Möglichkeit einer Durchbrechung des Bankgeheimnisses nach § 34 StGB[450]. Die Wertungen des § 34 StGB liest *Otto* in die Vorschrift des § 203 Abs. 2 StGB hinein[451]. Durch diese mittelbare Beachtung des § 11 BDSG wird sichergestellt, dass letztlich ein Outsourcing nur dann gerechtfertigt ist, wenn ein auftragähnliches Verhältnis vorliegt und die Verantwortlichkeit des Auftraggebers durch die Vergabe nach außen nicht reduziert wird.

Die höchstrichterliche Rechtsprechung hat sich in diesem Zusammenhang nicht eindeutig geäußert. So geht die zivilrechtliche Rechtsprechung beim externen Honorareinzug auf den Aspekt der Wahrnehmung berechtigter Interessen innerhalb einer Interessenabwägung ein, bezieht aber nicht Stellung, ob sie die Interessenabwägung bei § 34 StGB verortet[452]. Eindeutig scheint jedenfalls die Feststellung der Rechtsprechung, dass wirtschaftliche Interessen des Arztes, aufgrund derer die planmäßige Außenvergabe der Abrechnung und der Einziehung von Honorarforderungen erfolgt, unter keinen Umständen ein Offenbaren von Geheimnissen rechtfertigen können[453].

---

[448] Zu den Gestaltungsmöglichkeiten des externen Honorareinzugs vgl. Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 11.
[449] Im Ergebnis lehnt Wolf eine Rechtfertigung nach § 34 StGB ab, vgl. Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 80, 82 .
[450] Otto, wistra 1999, S. 204f.
[451] Eine Strafbarkeit nach § 203 Abs. 2 StGB kommt bei Instituten in öffentlich-rechtlicher Trägerschaft in Betracht.
[452] BGH NJW 1996, S. 775; deutlich für eine Interessenabwägung innerhalb von § 34 StGB OLG Karlsruhe, RDV 2006, S. 265.
[453] BGH NJW 1991, S. 328.

Könnten wirtschaftliche Erwägungen tatsächlich unter keinen Umständen eine Offenbarung rechtfertigen, müsste § 34 StGB im Bereich des Outsourcings medizinischer Daten kaum näher geprüft werden, denn regelmäßig werden wirtschaftliche Erwägungen die wesentliche Motivation für das Outsourcing darstellen. Indes ist die Aussage der Rechtsprechung nicht zwingend als kategorischer Ausschluss zu verstehen[454]. Sie ist vielmehr auf den Kontext des Honorareinzugs begrenzt, ohne eine darüber hinaus determinierende Wirkung zu entfalten.

Dies ergibt sich, wenn man die Grundsatzentscheidung des BGH zum externen Honorareinzug genau betrachtet. Der BGH führt aus, dass „solche wirtschaftlichen Erwägungen, von denen die Durchsetzung des Honorareinzugs nicht abhängt“, eine Durchbrechung der ärztlichen Schweigepflicht nicht zu rechtfertigen vermögen. Damit sind zwei gewichtige Einschränkungen verbunden. Zum einen ist nur die ärztliche Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB angesprochen. Zum anderen zeigt der Passus „von denen die Durchsetzung des Honorareinzugs nicht abhängt“, dass die wirtschaftlichen Erwägungen auf eine bestimmte Aufgabe bezogen werden. Sie sind deshalb unbeachtlich, weil die Aufgabenerfüllung durch sie nicht gefährdet ist.

Damit ist nicht ausgesagt, dass in anderen Aufgabenbereichen wirtschaftliche Erwägungen im Rahmen von Outsourcingvorhaben nicht eingreifen könnten, insbesondere wenn solche Erwägungen die Aufgabenerfüllung sichern können[455]. Dafür spricht auch, dass dem Gesetzgeber wirtschaftliche Erwägungen bei personenbezogenen Informationen durchaus nicht fremd sind. So ist beispielsweise eine Auftragsdatenverarbeitung nach § 80 SGB X unter anderem gemäß § 80 Abs. 5 Nr. 2 SGB X nur dann zulässig, wenn die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können[456]. Insofern bedarf es eines näheren Eingehens auf § 34 StGB.

---

[454] Auch im Bereich der Umweltdelikte sind im Rahmen einer Interessenabwägung wirtschaftliche Erwägungen nur regelmäßig ausgeschlossen, vgl. Tröndle/Fischer, StGB, § 324 Rn. 7a.

[455] Zu berücksichtigen ist auch, dass das Gebot zu wirtschaftlichem Handeln Outsourcing motiviert, vgl. zum Wirtschaftlichkeitsgebot in der GKV die §§ 12 und 70 Abs. 1 SGB V sowie Krauskopf, in: Krauskopf, Soziale Krankenversicherung Pflegeversicherung, SGB V, § 70 Rn. 3ff., § 72 Rn. 6 sowie Käsling, in: Krauskopf, Soziale Krankenversicherung Pflegeversicherung, SGB V, § 12, Rn. 4ff.; vgl. zum Wirtschaftlichkeitsgebot auch Hartmann, Outsourcing in der Sozialverwaltung und Sozialdatenschutz, S. 42 und 72.

[456] Auch im Bereich der Umweltdelikte sind wirtschaftliche Erwägungen nur regelmäßig ausgeschlossen, vgl. Tröndle/Fischer, StGB, § 324 Rn. 7a.

§ 34 StGB regelt den rechtfertigenden Notstand und ermöglicht unter bestimmten Voraussetzungen die Beeinträchtigung fremder Rechtsgüter zur Abwehr von Gefahren, die den eigenen Rechtsgütern oder denen Dritter drohen. § 34 StGB setzt im Einzelnen voraus, dass eine Notstandslage, also eine gegenwärtige Gefahr für ein notstandsfähiges Rechtsgut, vorliegt. Weiterhin verlangt § 34 StGB eine erforderliche und angemessene Notstandshandlung. Eine solche kann nur vorliegen, wenn eine Interessenabwägung ergeben hat, dass das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Beim Outsourcing medizinischer Daten ist geschütztes Rechtsgut das Interesse an der Funktionstüchtigkeit der Datenverarbeitung, beeinträchtigtes Interesse das Interesse am Schutz der anvertrauten Geheimnisse[457].

Problematisch erscheint bezogen auf Outsourcingvorhaben das Vorliegen einer gegenwärtigen Gefahr. Zwar erfasst § 34 StGB auch sogenannte Dauergefahren, wenn nach menschlicher Erfahrung der Zustand bei natürlicher Weiterentwicklung jederzeit in einen Schaden umschlagen kann[458]. Das Outsourcing ist aber gerade nicht eine Reaktion auf ungewöhnliche, plötzliche Ereignisse. Kennzeichnend ist, dass planmäßig, regelmäßig und nach einer Kosten-Nutzen-Analyse Daten an Dritte weitergegeben werden bzw. Dritte mit diesen Daten in Kontakt gelangen. Dabei wird zwischen den Beteiligten zumeist ein Rahmenvertrag getroffen, in dem die einzelnen Leistungen und die jeweiligen Rechte und Pflichten aufgelistet werden. Solche Verträge werden sich zudem regelmäßig auf einen längeren Zeitraum erstrecken, allein um mögliche Einsparpotentiale realisieren zu können. Dazu passt es nicht, von einer Gefahr für die Datenverarbeitung zu sprechen. Daher wird das Vorliegen einer Gefahr bei Outsourcinghandlungen regelmäßig zu verneinen sein. Lediglich in außerplanmäßigen Einzelfällen im Datenverarbeitungsvorgang könnte eine Gefahr anzunehmen sein[459].

Bedenken ergeben sich auch hinsichtlich der Interessenabwägung nach § 34 StGB. Erforderlich ist eine Interessenabwägung im Einzelfall unter Berücksichtigung der konkreten Situation. Notwendig ist eine Gesamtwürdigung aller Um-

[457] Vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 106.
[458] Lackner/Kühl, StGB, § 34 Rn. 2; Tröndle/Fischer, StGB, § 34 Rn. 4.
[459] Ähnlich für Versicherungsdaten Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 106, der für Versicherungsdaten nur in außergewöhnlichen Fällen eine Rechtfertigung nach § 34 StGB für möglich hält: „Das Outsourcen von Versicherungsdaten als solches lässt sich nicht über § 34 StGB rechtfertigen.“.

stände und widerstreitenden Interessen. Die danach vorgenommene Interessenabwägung muss ergeben, dass das Interesse an der Funktionstüchtigkeit der Datenverarbeitung das Interesse des Betroffenen am Schutz seiner Geheimnisse wesentlich überwiegt[460].

Ein solches wesentliches Überwiegen ist zweifelhaft, angesichts des hohen Ranges des auf der Seite des Betroffenen geschützten Rechtsgutes. Ein offensichtlicher Rangunterschied zwischen den in die Abwägung einzustellenden widerstreitenden Rechtsgütern ist nicht erkennbar. Nach der hier vertretenen Auffassung sind wirtschaftliche Erwägungen nicht kategorisch ausgeschlossen. Allerdings könnten diese allenfalls dann zu einem wesentlichen Überwiegen führen, wenn von ihnen die Sicherung der Aufgabenerfüllung abhängt und auf der anderen Seite durch Beachtung von Sicherungs- und Schutzmaßnahmen das Risiko einer unkontrollierten Datenpreisgabe an weitere Dritte minimiert werden kann.

Dass die Personal- und Sachkosten für das Vorhalten eigener Datenverarbeitungsresourcen derart bedeutsam werden, dass nur durch ein Outsourcing die Aufgabenerfüllung gewährleistet werden kann, ist kaum denkbar. Möglich erscheint dies allenfalls, wenn in der Verwaltung von Daten eine Hauptaufgabe des Schweigepflichtigen liegt. Dies kann sowohl bei gesetzlichen Krankenkassen als auch bei privaten Krankenversicherungsunternehmen vertreten werden, wenn man auf die tatsächliche Bedeutung der Datenverwaltung und nicht auf die vertragliche oder gesetzlich vorgesehene Aufgabe abstellt. Die Datenverarbeitung nimmt rein tatsächlich bei diesen Institutionen einen wesentlichen Umfang im Arbeitsaufwand ein.

Für den Bereich der stationären und ambulanten Krankenversorgung kann dies nicht angenommen werden. Denn für die nach § 203 Abs. 1 Nr. 1 StGB Schweigepflichtigen dominiert die diagnostische und therapeutische Leistung. Auch wenn den Arzt eine Dokumentationspflicht trifft, wird man die Datenverwaltung nicht als Hauptaufgabe oder Hauptpflicht bezeichnen können, unabhängig davon, ob man in der Dokumentationspflicht eine Nebenpflicht des Behandlungsvertrags

[460] Zu Beispielen aus dem medizinischen Bereich Ulsenheimer, Arztstrafrecht in der Praxis, Rn. 376 und Schlund, DAR 1995, S. 54.

sieht oder sie als Teil der ärztlichen Behandlungspflicht begreift[461]. Tatsächlich kann man nicht behaupten, dass die Datenverwaltung eine Kernaufgabe des Arztes oder des Krankenhauses wäre.

Ist zumindest hinsichtlich der gesetzlichen Krankenkassen, die nach § 203 Abs. 2 StGB schweigepflichtig sind, und den privaten Krankenversicherungsunternehmen, die nach § 203 Abs. 1 Nr. 6 StGB schweigepflichtig sind, denkbar, dass im Einzelfall ein wesentliches Überwiegen der Rechtsgüter vorliegt, bleiben Bedenken hinsichtlich der Interessenabwägung. Erforderlich ist eine konkrete Interessenabwägung, bei der sämtliche für die Bewertung bedeutsamen Umstände zu würdigen sind[462].

Beim Outsourcing wird in der Regel nicht ein einmaliges Heranziehen privater Dritter als Reaktion auf konkrete Umstände erfolgen. Vielmehr ähnelt die Outsourcingentscheidung eher einer antizipierten, abstrakten Abwägung im Rahmen einer unternehmerischen oder organisatorischen Entscheidung, deren Leitlinie eine effektivere und kostengünstigere Aufgabenerfüllung ist. Dabei erfolgt eine strategische, auf einen längeren Zeitraum bezogene Kosten-Nutzen-Analyse. Der Eintritt der kalkulierten Effektivitätssteigerung und Kostensenkung ist in die Zukunft projiziert und kann durch andere Entwicklungen konterkariert werden. Schon von der Anlage her passt dieser Regelbefund nicht zu der nach § 34 StGB erforderlichen Interessenabwägung.

Darüber hinaus ergeben sich Spannungen bei einem „Hineinlesen“ des § 11 BDSG in die Interessenabwägung nach § 34 StGB. Denn § 11 BDSG enthält präventive Elemente und ist nicht auf eine konkrete Situation oder einen einmaligen, zeitlich eng begrenzten Vorfall zugeschnitten, sondern bildet den Rahmen für eine besondere Form der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag.

Die Beachtung der Wertung des § 11 BDSG bei § 34 StGB erscheint daher wenig überzeugend. Überzeugender ist, die Wertungen des § 11 BDSG bei der Feststellung eines Offenbarens im Rahmen der Einbindung von berufsmäßigen Gehilfen

[461] Zu den unterschiedlichen Meinungen vgl. Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 24f.
[462] Tröndle/Fischer, StGB, § 34 Rn. 8, 9.

zu beachten. Ausnahmsweise ist aber auch denkbar, dass ein einmaliges Outsourcing nach einer konkreten Interessenabwägung unter Berücksichtigung aller Einzelumstände erfolgt. In einer solchen, praktisch wohl selten vorkommenden Situation ist eine Anwendung des § 34 StGB möglich. Dann ist aber ein Rekurrieren auf § 11 BDSG erst recht weder passend noch notwendig.

Im Ergebnis kann festgehalten werden, dass regelmäßig beim Outsourcing von medizinischen Daten eine Rechtfertigung nach § 34 StGB ausscheidet. Eine verlässliche Planungsgrundlage für Outsourcingvorhaben ist § 34 StGB allemal nicht.

c) Abwägung widerstreitender Interessen oder Pflichten

Neben einer Rechtfertigung nach § 34 StGB wird in der Literatur und der Rechtsprechung eine Rechtfertigungsmöglichkeit nach den Grundsätzen über die Abwägung widerstreitender Interessen oder Pflichten vertreten[463]. Die Begründung dieser Meinung ist nicht sehr tiefgehend. Als Argument wird hauptsächlich angeführt, dass durch das Erfordernis des wesentlichen Überwiegens des geschützten Interesses in § 34 StGB der Bereich strafloser Offenbarungsmöglichkeiten zu weit eingeschränkt wird[464]. Zudem würden diese Abwägungsgrundsätze allgemein die Rechtsordnung beherrschen[465]. Hiergegen kann man einwenden, dass der Verzicht auf das Erfordernis eine Umgehung von § 34 StGB bedeutet[466]. Im öffentlichen Bereich würde die Anwendung der Grundsätze ähnlich wie bei einer analogen Anwendung von § 193 StGB in Konflikt mit dem Grundsatz des Vorbehalts des Gesetzes geraten. Im privaten Bereich besteht die Gefahr ausufernder Offenbarungsrechte.

Dennoch ist im Ergebnis eine Rechtfertigung nach den Grundsätzen der Abwägung widerstreitender Interessen oder Pflichten bei § 203 StGB anzuerkennen. Dafür spricht entscheidend das im Kern durch § 203 StGB geschützte Recht auf informationelle Selbstbestimmung. Einschränkungen dieses Rechts bedürfen zwar

[463] Vgl. OLG Köln NJW 2000, S. 3656; KG NJW 1994, S. 1817, 1823; Rogall, NStZ 1983, S. 1, 6; offen gelassen noch von Rein, VersR 1976, S. 122; a.A. Schmitz, JA 1996, S. 949 (953).
[464] OLG Köln, NJW 2000, S. 3657.
[465] OLG Köln, NJW 2000, S. 3657.
[466] Allgemein anerkannt ist eine Rechtfertigung nur im Unterlassungsbereich unter dem Gesichtspunkt der Pflichtenkollision, wenn mehrere Handlungspflichten nebeneinander Geltung beanspruchen, nicht dagegen, wenn eine Handlungspflicht mit einer Unterlassungspflicht bei dem Handelnden zusammentreffen, vgl. Beulke, Strafrecht AT Rn. 736.

einer gesetzlichen Grundlage, die gesetzgeberische Entscheidung stellt aber eine vorweggenommene und das Verhältnismäßigkeitsprinzip beachtende Interessenabwägung dar. Sind die gesetzlichen Entscheidungen unzureichend, dann muss nach einer individuellen Interessenabwägung unter Beachtung des Verhältnismäßigkeitsprinzips eine Rechtfertigung möglich sein, insbesondere wenn sich der Schweigepflichtige unvereinbaren Interessen oder Pflichten in seiner Person gegenübersieht. Die Auflösung eines solchen Spannungsverhältnisses muss durch eine Abwägung unter Beachtung des Verhältnismäßigkeitsprinzips möglich sein[467].

Dies gilt umso mehr, als dem Einzelnen, nach § 203 StGB Verpflichteten kein ähnlich weiter Spielraum in seiner Entscheidung zusteht wie dem Gesetzgeber. Das Erfordernis der Verhältnismäßigkeit führt im Abwägungsergebnis zu einer Annäherung an § 34 StGB, bei dem ein wesentliches Überwiegen des geschützten Rechtsgutes in § 34 StGB resultieren muss. Danach ist erforderlich, dass das geschützte Interesse jedenfalls höherrangig sein muss. Auch bei einem höherrangigem entgegenstehenden Interesse wäre eine Offenbarung aber nur dann erforderlich, wenn der Interessensgegensatz nicht auf andere Weise gelöst werden kann[468]. Unter diesen Schranken kann eine Rechtfertigung nach den Grundsätzen über die Abwägung widerstreitender Interessen oder Pflichten erfolgen, ohne dass eine Umgehen des § 34 StGB befürchtet werden muss.

Allerdings bleibt für die tatsächliche Anwendung dieser Grundsätze auf das Outsourcing medizinischer Daten wenig Spielraum. Denn die sachlichen Bedenken, die bei der Interessenabwägung im Rahmen des § 34 StGB dargestellt wurden, bleiben in ähnlicher Weise bei einer Abwägung widerstreitender Interessen oder Pflichten bestehen. In der Regel werden kaum konkrete Umstände eintreten, die ein höherrangiges entgegenstehendes Interesse begründen könnten, dem man nicht auf andere Weise gerecht werden könnte, als durch ein Outsourcing medizinischer Daten. Im Ergebnis wird eine Rechtfertigung nach den Grundsätzen über die Abwägung widerstreitender Interessen oder Pflichten regelmäßig für Outsourcingvorhaben ausscheiden.

---

[467] Ähnlich Deutsch/Spickhoff, Medizinrecht Rn. 479.
[468] Tröndle/Fischer, StGB, § 203 Rn. 45.

Nach dem gefundenen Ergebnis ist die Frage, ob § 34 StGB außerhalb des § 203 StGB eine Erlaubnisnorm im bereichsspezifischen Datenschutzrecht darstellt, von untergeordneter praktischer Bedeutung. Zum Teil wird im Sozialdatenschutz wegen § 76 SGB X vertreten, dass § 34 StGB keine Offenbarungsbefugnis liefert, wenn eine Stelle nach § 35 SGB I und nicht ein nach § 203 Abs. 1 StGB Schweigepflichtiger unter Wahrnehmung berechtigter Eigeninteressen Sozialdaten, die zugleich „Geheimnisse" i.S.v. § 203 StGB sind, weitergeben will[469]. Diese Auffassung überzeugt nicht. Zwar kann man einwenden, dass über § 34 StGB eine Ausweitung der sozialrechtlichen Einzelbefugnisse praeter legem droht. Dieser Einwand ist aber nicht stichhaltig. In § 85a SGB X, der nach dem Vorbild des § 44 BDSG geschaffen worden ist, werden i.V.m. § 85 SGB X bestimmte Verstöße gegen den Sozialdatenschutz sanktioniert. Dabei kann Täter jeder Mitarbeiter einer verantwortlichen Stelle sein. Im Bereich der Ordnungswidrigkeit nach § 85 SGB X ist über § 30 OWiG auch eine Sanktion gegenüber einer juristischen Person, also einem Sozialversicherungsträger, denkbar. Daher ist es nicht einzusehen, dass sich ein nach § 203 StGB Schweigepflichtiger auf § 34 StGB berufen kann, nicht aber ein Mitarbeiter einer verantwortlichen Stelle im Sozialdatenschutzrecht. Die allgemeinen Rechtfertigungsgründe des StGB gelten daher auch im Sozialdatenschutzrecht uneingeschränkt.

d) Einwilligung

Schließlich ist denkbar, dass ein unbefugtes Offenbaren im Rahmen des Outsourcings medizinischer Daten deshalb entfällt, weil der Betroffene vorher der Geheimnisoffenbarung zugestimmt hat. Unterschieden werden das Einverständnis, die ausdrückliche und die konkludente Einwilligung sowie die mutmaßliche Einwilligung. Liegt eine wirksame Zustimmung vor, kann ein Offenbaren von Geheimnissen nicht „unbefugt" i. S. v. § 203 StGB sein. Nach der hier vertretenen Auffassung ist das Merkmal „unbefugt" insgesamt der Rechtswidrigkeitsebene zuzuordnen mit der Konsequenz, dass eine Zustimmung als rechtfertigende Einwilligung und nicht als tatbestandsausschließendes Einverständnis zu begreifen ist[470]. Im Folgenden soll zunächst die konkludente und die mutmaßliche Einwilli-

[469] Vgl. Giese/Krahmer, Sozialgesetzbuch, § 76 Rn. 16; a.A. Seidel, in: Diering/Timme/Waschull, Sozialgesetzbuch X, § 76 Rn. 10.
[470] Vgl. oben unter S. 111 ff.; für ein tatbestandsausschließendes Einverständnis Vogel, Zum strafrechtlichen Schutz des Sozialgeheimnisses, S. 45; vgl. zur deliktssystematischen Einordnung der Einwilligung auch Kindhäuser, Strafrecht AT, S. 104 ff.

gung untersucht werden. Anschließend ist auf die ausdrückliche Einwilligung einzugehen.

aa) Konkludente Einwilligung

Bei der konkludenten oder stillschweigenden Einwilligung wird der Wille des Betroffenen nicht ausdrücklich erklärt, sondern folgt aus einer nach außen erkennbaren Handlung des betroffenen Rechtsgutsinhabers. Eine solche konkludente Einwilligung ist beispielsweise bei der Behandlung eines Patienten durch ein Krankenhausteam oder in einer Gemeinschaftspraxis anzunehmen[471]. Aus der Tatsache, dass der Patient sich in Behandlung begibt, wird zum Ausdruck gebracht, dass er mit einer Weitergabe von Geheimnissen an andere Schweigepflichtige, mit deren Einbeziehung in die Behandlung im Voraus gerechnet werden kann, einverstanden ist.

Bisweilen wird die Unterscheidung zwischen konkludenter und ausdrücklicher Einwilligung in Frage gestellt. In Teilen der Literatur wird angenommen, dass eine wirksame Einwilligung keine Erklärung voraussetzt[472]. Begründet wird die Auffassung damit, dass die Einwilligung kein Rechtsgeschäft ist, sondern schlichter Rechtsverzicht, bei dem es nicht erforderlich ist, dass ein Vertragspartner von der Erklärung Kenntnis nehmen muss[473].

Käme es nur auf den inneren Willen des Betroffenen an, würde sich in der Tat die Unterscheidung zwischen konkludenter und ausdrücklicher Einwilligung erübrigen. Indes ist dieser Auffassung nicht zu folgen. Es mag sein, dass das Erfordernis einer Erklärung als ein „Überbleibsel aus der Zeit, in der die Einwilligung als Rechtsgeschäft zwischen Täter und Opfer verstanden wurde“, angesehen werden kann[474]. Das zwingt aber nicht zu der Annahme, dass eine Erklärung abweichend von zivilrechtlichen Regeln entbehrlich ist[475]. Auch unter dem Gesichtspunkt des

[471] Vgl. Schlund, Handbuch des Arztrechts, S. 570.
[472] Joecks, Studienkommentar StGB, Vor § 32 Rn. 21; anders die h.M. vgl. Wessels/Beulke, Strafrecht AT Rn. 378.
[473] Joecks, Studienkommentar StGB, Vor § 32 Rn. 21.
[474] So Joecks, Studienkommentar StGB, Vor § 32 Rn. 21.
[475] Das bedeutet nicht, dass sich zivilrechtliche und strafrechtliche Anforderungen voll decken würden; zu dem Problem der Geschäftsfähigkeit und der Form, vgl. Jescheck/Weigend, Strafrecht AT, § 34 IV 1, 4; Wessels/Beulke, Strafrecht AT Rn. 374; Meier, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, S. 166, 169.

Rechtsgüterverzichts ist eine Erklärung zu verlangen. Denn ohne das Erfordernis einer Erklärung würden die Grenzen zur mutmaßlichen Einwilligung verwischt. Insbesondere bei einem Verzicht auf bedeutsame Rechtsgüter, wie z.B. auf das Selbstbestimmungsrecht, besteht das Bedürfnis nach einer nachweisbaren Erklärung. Nur ein solches Erfordernis wird dem Schutz des Betroffenen vor einer in ihn hineingelesenen Preisgabe seiner Rechtgüter gerecht und sichert eine auch im Strafrecht notwendige bewusste Entscheidung. Dies zeigt ein Blick auf den Bereich der privaten Krankenversicherung. Hier sind vorformulierte Klauseln oft der einzige Anhaltspunkt für die Annahme einer Einwilligung. Sie haben über das Zivilrecht auch Bedeutung für das Strafrecht[476]. Lässt sich keine Erklärung feststellen, dann kann eine Rechtfertigung nur noch nach den Regeln über die mutmaßliche Einwilligung erfolgen.

Ist somit an der grundsätzlichen Unterscheidung zwischen ausdrücklicher und konkludenter Einwilligung festzuhalten, stellt sich die Frage, ob eine konkludente Einwilligung beim Outsourcing medizinischer Daten angenommen werden kann. Denkbar wäre es, in der Inanspruchnahme von Leistungen durch den Patienten eine Einwilligung in die Offenbarung von Geheimnissen an Outsourcingpartner zu sehen. Eine solche Konstruktion ist abzulehnen. Sie entbehrt einer hinreichenden tatsächlichen Grundlage und erscheint fiktiv.

Die Einschaltung privater IT-Dienstleister unterscheidet sich gravierend von den anerkannten Fallgruppen der konkludenten Einwilligung. Der Patient mag noch absehen können, dass andere Ärzte an seiner Behandlung mitwirken. Er kann und muss aber nicht damit rechnen, dass die Geheimnisse an private IT- Dienstleister outgesourct werden[477]. Dies dennoch angesichts der komplexen und schwer zu beurteilenden Outsourcinggestaltungen zu verlangen, entspräche nicht der Wissensverteilung, würde Verantwortung unbillig verteilen und ist den betroffenen Patienten nicht zumutbar. Der Patient ist sich der Tragweite und Bedeutung solch einer Einwilligung nicht bewusst. Dies ist aber zwingende Voraussetzung für die Einwilligung[478]. Diese Voraussetzung würde unterlaufen werden. Der Einwilligung einen über die Mit-, Weiter-, und Nachbehandlung hinausgehenden weiteren

[476] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 104.
[477] Bereits oben wurde ausgeführt, dass das Outsourcing medizinischer Daten keinesfalls als sozial üblich bezeichnet werden kann, vgl. S. 104f.
[478] Vgl. Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 237.

Erklärungswert hinsichtlich des Outsourcings medizinischer Daten beizumessen, wäre willkürlich.

Dem entspricht es, dass die höchstrichterliche zivilrechtliche Rechtsprechung bei der Annahme einer konkludenten Einwilligung zurückhaltend ist. Zum Teil wurde angenommen, dass die Abtretung von ärztlichen Honorarforderungen an externe, private Verrechnungsstellen durch eine konkludente Einwilligung der Betroffenen gedeckt ist[479]. Zutreffend geht heute die Rechtsprechung seit der Grundsatzentscheidung des BGH vom 10.07.1991- VIII ZR 296/90 davon aus, dass eine stillschweigende Einwilligung grundsätzlich nicht angenommen werden kann, auch wenn der Arzt auf seine Vorgehensweise durch Aushänge hingewiesen hat[480]. Der BGH hat Tendenzen der Überantwortung der Einhaltung der ärztlichen Schweigepflicht auf den Patienten vorgebeugt, indem er ausgeführt hat, dass es nicht Sache des Patienten sei, der Weitergabe seiner Daten zu widersprechen, um den Eindruck des stillschweigenden Einverständnisses zu vermeiden[481].

Die Ansicht des BGH ist überzeugend. Die Richtigkeit dieser Grundüberlegung der Verantwortungszuordnung wird für medizinische Daten als besondere personenbezogene Daten durch § 4a Abs. 3 BDSG bestätigt. Nach § 4a Abs. 3 BDSG, der Art. 7a der Europäischen Datenschutzrichtlinie in nationales Recht umsetzt, ist eine ausdrückliche und eindeutige Einwilligung erforderlich. Nur eine solche Einwilligung wird dem Schutz des Rechts auf informationelle Selbstbestimmung, um den es im Kern auch bei § 203 StGB geht, gerecht. Aus diesem Grund stellen formularmäßige Klauseln, die bestehende Verträge dahingehend verändern, dass zukünftig Outsourcingmaßnahmen zur Effizienzsteigerung oder Kostensenkung zulässig sind, sofern der Betroffene nicht widerspricht, eine unangemessene Benachteiligung des Vertragspartners des Verwenders dar und sind nach § 307 BGB unwirksam[482].

Teilweise werden in der Literatur unter dem Einwand der Eigenständigkeit des Strafrechts die Anforderungen der zivilrechtlichen Rechtsprechung als überzogen

---

[479] Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 110; LG Kleve NJW 1991, S. 756; AG Grevenbroich NJW 1990, S. 1535.
[480] Vgl. BGH MedR 1991, S. 328.
[481] BGH MedR 1991, S. 328.
[482] Ähnliche Bedenken äußert Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 106.

kritisiert[483]. Aber der Einwand der Eigenständigkeit führt hier nicht weiter. Zwar ist richtig, dass Zivilrecht und Datenschutzrecht sich vom Strafrecht unterscheiden. Für die Frage der Beurteilung einer konkludenten Einwilligung bei § 203 StGB ist dieser Aspekt nicht entscheidend. Denn man versucht festzustellen, ob der Betroffene aufgrund eines bestimmten Verhaltens einen bestimmten Willen geäußert hat. Der Umgang mit medizinischen Daten ist dabei für den Betroffenen sehr bedeutsam. Beeinträchtigt ist regelmäßig ein Kernbereich des allgemeinen Persönlichkeitsrechts, das durch den Betroffenen eingeschränkt wird. Daher muss der Betroffene bewusst entscheiden, ob er einem bestimmten Umgang mit seinen Geheimnissen zustimmt. Einem Verhalten, das nicht eine ausdrückliche Einwilligung in einen bestimmten Umgang mit Geheimnissen beinhaltet, einen solchen Erklärungswert beizumessen kann allenfalls dann angenommen werden, wenn der Sachverhalt, in den eingewilligt wird, völlig üblich und so selbstverständlich ist, dass eine besondere, bewusste Willensbildung und Willensartikulierung nicht erforderlich ist. Davon kann beim Sachverhalt des Outsourcings medizinischer Daten nicht die Rede sein[484]. Andernfalls würde man annehmen, dass bei identischer Einsichtslage und demselben Anknüpfungspunkt zivilrechtlich gesehen sein Verhalten nicht für eine Einwilligung ausreicht, strafrechtlich aber als Einwilligung zählt. Der Betroffene weiß also hinsichtlich des Zivilrechts nicht was er macht, wohl aber hinsichtlich des Strafrechts. Dies ist nicht plausibel. Auch bei einer rein strafrechtlichen Betrachtung kann daher ein unterlassener Widerspruch bei entsprechenden formularmäßigen Klauseln nicht zu einer wirksamen Einwilligung in ein Outsourcing medizinischer Daten führen.

Im Bereich der gesetzlichen Krankenversicherung muss der Patient nur damit rechnen, dass die personenbezogenen Informationen, die die Krankenkassen nach Maßgabe gesetzlicher Vorschriften erhalten haben, von diesen selbst verwaltet werden. Vor diesem Hintergrund sind Mitteilungen des Patienten an die gesetzlichen Krankenkassen aufgrund bestehender Mitwirkungspflichten oder Mitteilungen der Leistungsträger an die gesetzlichen Krankenkassen nach Inanspruchnahme durch den Patienten zu verstehen. Daraus kann keine konkludente Einwilligung hinsichtlich des Outsourcings abgeleitet werden. Gleiches gilt hinsichtlich der privaten Krankenversicherung. Teilt der Patient hier auf vertraglicher Grund-

[483] Vgl. dazu Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19, Rn. 502.
[484] Vgl. dazu bereits die Ausführungen zur Sozialadäquanz S. 116 f.

lage Geheimnisse mit, bedeutet dies nicht konkluden, dass die Geheimnisse an dritte IT-Dienstleistungsunternehmen outgesourct werden dürfen.

bb) Mutmaßliche Einwilligung

Scheidet eine konkludente Einwilligung durch den Betroffenen aus, ist zu prüfen, ob eine Rechtfertigung nach den Regeln über die mutmaßliche Einwilligung eingreift. Nach zutreffender und ganz überwiegender Ansicht ist das gewohnheitsrechtlich anerkannte Rechtsinstitut der mutmaßlichen Einwilligung ein eigenständiger Rechtfertigungsgrund und stellt nicht lediglich einen Unterfall des rechtfertigenden Notstandes dar[485]. Maßgeblich für die mutmaßliche Einwilligung ist das subjektive Interesse des Betroffenen und nicht eine objektive Interessenabwägung[486]. Freilich dürfen zur Ermittlung dieses subjektiven Interesses objektive Umstände herangezogen werden.

Eine Rechtfertigung unter dem Gesichtspunkt der mutmaßlichen Einwilligung wird beim Outsourcing medizinischer Daten regelmäßig nicht eingreifen. Dies ergibt sich aus folgender Überlegung. Eine mutmaßliche Einwilligung kann grundsätzlich, wenn der Vorrang und Schutz des subjektiven Willens des Betroffenen gesichert werden soll, nur dann eingreifen, wenn der Betroffene vermutlich einwilligen würde, aber nicht rechtzeitig einwilligen kann[487]. Mutmaßungen bedarf es nur dann, wenn der Betroffene sich nicht rechtzeitig eindeutig äußern kann. Für den Regelfall des Outsourcings ist diese Grundvoraussetzung für die mutmaßliche Einwilligung nicht gegeben, da eine Einwilligung eingeholt werden kann. Das Einholen kann, insbesondere bei einer Vielzahl von Betroffenen, langwierig und kostenintensiv sein. Zudem wird vielleicht nicht jeder Betroffene einwilligen, wodurch die Effizienz eines solchen Vorgehens im Rahmen von Outsourcingmaßnahmen verloren gehen könnte. Dies ändert aber nichts daran, dass eine Einwilligung tatsächlich möglich ist. Besondere, plötzliche Umstände, die ein Erreichen des Betroffenen unmöglich oder unzumutbar erscheinen lassen, liegen bei längerer Zeit im Voraus und unter wirtschaftlichen Aspekten geplanten Outsourcingprojekten in der Regel nicht vor.

---

[485] Ulsenheimer, in: Handbuch des Arztrechts, S. 556; BVerfG NJW 2002, S. 2165.
[486] Tröndle/Fischer, StGB, Vor § 32 Rn. 4.
[487] BVerfG NJW 2002, S. 2165; Lackner/Kühl, StGB, Vor § 32 Rn. 21.

cc) Ausdrückliche Einwilligung

Schließlich ist zu untersuchen, ob eine Rechtfertigung des Outsourcings medizinischer Daten unter dem Gesichtspunkt der ausdrücklichen Einwilligung in Betracht kommt. Eine wirksame ausdrückliche Einwilligung setzt voraus, dass der Betroffene über das Rechtsgut verfügen darf und einwilligungsfähig ist. Einwilligungsfähigkeit ist dabei nach überwiegender und zutreffender Meinung nicht mit der zivilrechtlichen Geschäftsfähigkeit gleichzusetzen, sondern meint, dass der Betroffene nach seiner geistigen und sittlichen Reife fähig sein muss, Bedeutung, Umfang und Tragweite seiner Einwilligung zu erkennen und sachgerecht zu beurteilen[488]. Weiterhin wird vorausgesetzt, dass die Einwilligung nicht an wesentlichen Willensmängeln leidet[489]. Dazu ist erforderlich, dass dem Betroffenen die wesentlichen Informationen über das konkrete Vorgehen, in das der Betroffene einwilligen soll, zugänglich gemacht werden müssen[490].

Für eine wirksame strafrechtliche Einwilligung ist keine Schriftform erforderlich. Zwar können Normen außerhalb des StGB ein Schriftformerfordernis statuieren[491], allerdings ist dieses Formerfordernis ohne Bedeutung für die strafrechtliche Bewertung[492]. Dies folgt daraus, dass die strafrechtliche Einwilligung auf die natürliche Einsichtsfähigkeit abstellt. Der Schutzzweck der Schriftform außerhalb des Strafrechts in Spezialgesetzen vermag diesen Gesichtspunkt nicht zu beeinflussen. Eventuelle Formerfordernisse sind daher nur im Rahmen des jeweiligen Spezialgesetztes zu beachten. Im Verhältnis zum allgemeinen Datenschutzrecht ergibt sich das schon aus der erwähnten Parallelgeltung von Schweigepflicht und allgemeinem Datenschutzrecht.

Für das Outsourcing medizinischer Daten bedeutet dies, dass der Outsourcer den Betroffenen darüber unterrichtet, an wen, wann, unter welchen Voraussetzungen und zu welchem Zweck seine Geheimnisse outgesourct werden. Ein pauschaler Hinweis darauf, dass Daten an Outsourcingpartner zur effizienteren Datenverwal-

---

[488] Wessels/Beulke, Strafrecht AT Rn. 374; Tröndle/Fischer, StGB, § 203 Rn. 32.
[489] Näher Wessels/Beulke, Strafrecht AT Rn. 375.
[490] Vgl. zu den Anforderungen an ein wirksames Einverständnis zur Weitergabe von Behandlungsunterlagen im Rahmen einer Abtretung einer zahnärztlichen Honorarforderung OLG Karlsruhe NJW 1998, S. 831ff.
[491] Vgl. z.B. § 4a BDSG.
[492] Vgl. Tröndle/Fischer, StGB, § 203 Rn. 33; Schünemann, in: Leipziger Kommentar StGB, § 203 Rn. 106; ebenso zu § 4 Abs. 2 BDSG a.F. Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 523, 576.

tung weitergegeben werden, reicht nicht[493]. Werden die dargelegten Voraussetzungen der Einwilligung eingehalten, ermöglicht eine individuell eingeholte Einwilligung Outsourcingmaßnahmen, ohne dass § 203 StGB verletzt wird. Dieser prinzipiell gangbare Weg ist allerdings mit viel Aufwand verbunden und überdies hinsichtlich der Erfolgsrate unsicher.

Denkbar ist, dass solche Einwilligungen formularmäßig eingeholt werden. Möglich ist dies allerdings nur, soweit die Beziehung zwischen Outsourcer und betroffenem Geheimnisträger eine vertragliche Grundlage hat. Dies gilt für die ärztliche Behandlung im stationären und ambulanten Bereich sowie für die Beziehung zu privaten Krankenversicherungen. Die Beziehung zu den gesetzlichen Krankenkassen beruht nicht auf vertraglicher Grundlage, sondern auf einseitiger Beitrittserklärung. Hier ist nur eine gesonderte individuelle Einwilligung möglich, die freilich zusammen mit der Beitrittserklärung erfolgen kann. In den anderen Fällen könnte in Allgemeinen Geschäftsbedingungen oder in Allgemeinen Versicherungsbedingungen eine Klausel aufgenommen werden, nach der das Outsourcing aktuell wie zukünftig für zulässig erklärt wird. Nimmt der Betroffene diese Klauseln an, könnte darin eine wirksame Einwilligung liegen.

Gegen eine solche Vorgehensweise bestehen erhebliche Bedenken[494]. Solche Klauseln unterliegen der Inhaltskontrolle nach den §§ 307 ff. BGB. Sie sind an § 307 BGB zu messen. Nach § 307 BGB sind Bestimmungen in Allgemeinen Geschäftsbedingungen nur dann wirksam, wenn sie den Vertragspartner nicht entgegen des Gebots von Treu und Glauben unangemessen benachteiligen.

Bei der formularmäßigen Einwilligung in das Outsourcing von medizinischen Daten wird das Recht auf informationelle Selbstbestimmung eingeschränkt. Bei der Frage der unangemessenen Benachteiligung ist die Ausstrahlungswirkung von Art. 2 Abs. 1 und 1 Abs. 1 GG, aus denen das Recht auf informationelle Selbstbestimmung überwiegend abgeleitet wird, zu beachten. Hiernach wirkt das Recht auf informationelle Selbstbestimmung auch im Privatrecht. Die verwendete Klausel darf insbesondere das Recht auf informationelle Selbstbestimmung nicht un-

[493] Vgl. zu den strengen Anforderungen formularmäßiger Schweigepflichtentbindungserklärungen VG Stuttgart vom 27.12.2006, Az.: 17 K 1608/06 und BVerfG vom 23.10.2006, Az.: 1 BvR 2027/02.
[494] Vgl. Ulsenheimer, Arztstrafrecht in der Praxis, S. 366; Rieger, Lexikon des Arztrechts, Rn. 1641.

verhältnismäßig einschränken. Dies ist bei einer formularmäßigen Einwilligungseinholung zweifelhaft.

Zum einen ist fraglich, ob eine solche formularmäßige Einwilligung, angesichts der Machtstellung des Verwenders, freiwillig erfolgt. Schließlich geht es für den Vertragspartner des Verwenders um existenzielle Gesundheits-, Versorgungs- oder Vorsorgeleistungen. Faktisch bleibt dem Nachfragenden kaum eine Wahl. Dies spricht eher dafür, keine Freiwilligkeit in solchen Konstellationen anzunehmen.

Zum anderen ist zu berücksichtigen, dass Outsourcingsachverhalte für den betroffenen Einwilligenden schwer zu beurteilen sind. Wie soll sich der Patient einen Überblick darüber verschaffen, ob die Geheimnisse gegen unbefugten Zugriff Dritter geschützt sind? Hinzu kommt, dass sich die Rahmenbedingungen bei Outsourcingprojekten verändern können und sich dann nicht mehr mit der konkreten Situation decken, für die die Einwilligung erteilt worden ist. Der Einwilligende wird solche Vorgänge kaum beurteilen können. Daher sprechen insgesamt gewichtige Gründe dafür, dass durch solche formularmäßig eingeholte Klauseln, insbesondere bei allgemein gehaltenen Klauseln, die eine Einwilligung in Outsourcingmaßnahmen statuieren, der Betroffene unangemessen benachteiligt wird.

Die zivilrechtliche Unwirksamkeit wird i.d.R. auch für die strafrechtliche Beurteilung maßgeblich sein. Zwar wird in der Literatur mit guten Gründen eingewandt, dass aufgrund der Unterschiede zwischen Zivilrecht und Strafrecht nicht jeder zivilrechtliche Nichtigkeitsgrund für die strafrechtliche Beurteilung einer Einwilligung maßgeblich sein muss[495]. Bezogen auf § 203 StGB wird dieser Einwand aber häufig unerheblich bleiben[496]. Denn die zivilrechtliche Unwirksamkeit ergibt sich regelmäßig aus einer Verletzung des allgemeinen Persönlichkeitsrechts durch die zum Nachteil des Betroffenen verwendeten Klauseln. Die formularmäßigen Klauseln greifen in die Verfügungsbefugnis des Betroffen ein und beeinträchtigen allgemein die selbstbestimmte Willensbildung des Geheimnisträgers. In solchen Fällen würde eine Differenzierung zwischen einem „zivilrechtlichen Teil“ des allgemeinen Persönlichkeitsrechts und einem „strafrechtlichen Teil“ des allgemei-

[495] Vgl. zu diesem Problem Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 597ff.
[496] Vgl. auch die Ausführungen zur konkludenten Einwilligung S. 167.

nen Persönlichkeitsrechts allzu künstlich erscheinen. Es ist kaum vorstellbar, dass ein zivilrechtliches Recht auf informationelle Selbstbestimmung verletzt ist, der Geheimnisträger aber strafrechtlich gesehen Bedeutung, Umfang und Tragweite seiner Einwilligung erkennen und sachgerecht beurteilen kann. Dies gilt umso mehr als das Outsourcing medizinischer Daten vertraglich ausgestaltet wird und somit die vertragliche Gestaltung erst die strafrechtlich zu beurteilende Handlung ergibt.

Soll also eine Einwilligung wirksam eingeholt werden, wird dies, unter Beachtung der Wirksamkeitsvoraussetzungen für eine strafrechtliche Einwilligung, regelmäßig im Wege einer Individualvereinbarung zu erfolgen haben.

IX. Ergebnis zu § 203 StGB

Die bisherigen Untersuchungen haben gezeigt, dass de lege lata beim Outsourcing medizinischer Daten an private IT- Dienstleistungsunternehmen in der Regel eine Verletzung des § 203 StGB erfolgt. § 203 StGB erlaubt nicht ein Heranziehen Dritter zum eigenverantwortlichen Umgang mit medizinischen Daten, die zugleich „Geheimnisse“ i. S. v. § 203 StGB sind. Eine solche Delegation an private Dritte ist weder in § 203 StGB angelegt, noch ergibt sie sich aus anderen Regelungen. Mit § 203 StGB vereinbar ist es aber, Mitarbeiter privater IT- Dienstleistungsunternehmen in die Organisation des Outsourcers als Gehilfen einzubinden, wodurch eine tatbestandliche Verantwortungseinheit entstehen kann. Dies setzt voraus, dass der Outsourcer die Weisungsgebundenheit des in seinem Bereich tätigen Dienstleisters sicherstellt und zudem das Innenverhältnis zwischen Dienstleister und Outsourcer durch geeignete Maßnahmen des Datenschutzes und der Datensicherheit wirksam nach außen abschirmt. Dann kann von einer tatbestandlichen Verantwortungseinheit gesprochen werden innerhalb derer eine Weitergabe von Geheimnissen kein Offenbaren i.S.v. § 203 StGB darstellt. Ansonsten ist ein Outsourcing vor dem Hintergrund des § 203 StGB nur bei einer ausdrücklichen Einwilligung möglich, wenn der Betroffene die wesentlichen Informationen hinsichtlich der beabsichtigten Outsourcingmaßnahmen erhalten hat, so dass er sich der Bedeutung und Tragweite einer Einwilligung bewusst werden kann.

D. Outsourcing und strafrechtlicher Datenschutz

Nach der hier vertretenen Ansicht sind neben den strafrechtlichen Anforderungen des § 203 StGB zugleich die Anforderungen des allgemeinen und sektorspezifischen Datenschutzrechts zu beachten. Ist ein Outsourcingvorhaben datenschutzrechtlich nicht zulässig, drohen auch außerhalb des StGB Sanktionen. Neben § 203 StGB finden sich Regelungen, in den Datenschutzgesetzen des Bundes und der Länder, die bei datenschutzrechtlichen Verstößen strafrechtliche Sanktionen vorsehen[497]. Im Folgenden wird auf diese Regelungen eingegangen, wobei wegen der praktischen Bedeutung und des Sachzusammenhangs auch die bußgeldbewehrten Vorschriften angesprochen werden.

I. Strafbarkeit nach § 44 BDSG

Das Bundesdatenschutzgesetz enthält in § 44 BDSG eine Strafvorschrift. Hiernach wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer eine in § 43 Abs. 2 BDSG bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen. Im Zusammenhang mit dem Outsourcing medizinischer Daten ist bei § 43 Abs. 2 BDSG hauptsächlich die Nr. 1 von Bedeutung. § 43 Abs. 2 Nr. 1 BDSG nennt als Handlung das unbefugte Erheben oder Verarbeiten personenbezogener Daten, die nicht allgemein zugänglich sind.

Wie bei § 203 StGB ist das Merkmal „unbefugt“ der Rechtswidrigkeitsebene zuzuordnen[498]. Der gegenteiligen Meinung in der Literatur kann nicht zugestimmt werden. Zwar ist zuzugeben, dass der Vorgang des Übermittelns sich vom Offenbaren unterscheidet. Vor dem Hintergrund des Rechts auf informationelle Selbstbestimmung und der Rechtsprechung des Bundesverfassungsgerichts kann eine Übermittlung personenbezogener Daten durchaus als unrechtstypisch betrachtet werden. Hierfür bedarf es des Merkmals unbefugt nicht. Außerdem wäre es wi-

[497] Die Regelungen zum Datenschutzstrafrecht stehen, soweit nicht ausdrücklich Subsidiarität angeordnet ist, zu § 203 StGB aufgrund des Nebeneinander zwischen Datenschutzrecht und § 203 StGB in Tateinheit, § 52 StGB, vgl. Wolf, Externer Honorareinzug und ärztliche Schweigepflicht, S. 112; Dammann, in: Simitis, BDSG, § 44 Rn. 16; Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht, Rn. 679; nach a.A. soll § 203 StGB vorrangig sein, Tröndle/Fischer, StGB, § 203 Rn. 52; Gola/Schomerus, BDSG, § 44 Rn. 2; BGH RDV 2003, S. 139ff.

[498] Dammann, in: Simitis, BDSG, § 44 Rn. 9; a.A. Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 572.

dersprüchlich, zu prüfen, ob datenschutzrechtliche Normen bei § 203 StGB Rechtfertigungsgründe sind, dieselben Normen aber ihren Charakter als Erlaubnistatbestände im Datenschutzrecht verlieren und das Tatbestandsmerkmal „unbefugt" ausfüllen.

Unter Verarbeiten ist nach § 3 Abs. 4 BDSG das Speichern, Übermitteln, Verändern, Sperren und Löschen von personenbezogenen Daten zu verstehen. Im Rahmen von Outsourcingmaßnahmen wird regelmäßig zumindest eine Speicherung von personenbezogenen Daten und damit eine Verarbeitung personenbezogener Daten erfolgen. Soweit sich die Handlung allein auf ein Nutzen von Daten beschränkt, kann eine Strafbarkeit nur über § 44 BDSG i.V.m. § 43 Abs. 2 BDSG begründet werden. Damit wird nicht jedes unbefugte Nutzen erfasst, sondern nur ein Nutzen übermittelter Daten entgegen der in § 43 Abs. 2 Nr. 5 BDSG genannten Vorschriften, indem die Daten an Dritte weitergegeben werden. Eine solche Weitergabe, die ein aktives Tätigwerden erfordert, wird im Normalfall des Outsourcings planmäßig nicht stattfinden. Lediglich bei einem missbräuchlichen Heranziehen Dritter durch den Outsourcingpartner oder einzelner Mitarbeiter kann eine Strafbarkeit nach § 44 BDSG i.V.m. § 43 Abs. 2 Nr. 5 BDSG in Betracht kommen.

Liegt ein „unbefugtes Verarbeiten" i.S.v. § 43 Abs. 1 Nr. 1 BDSG vor, scheidet dennoch eine Strafbarkeit des Outsourcers regelmäßig aus. Denn der Outsourcer handelt im Normalfall nicht, wie es § 44 BDSG verlangt, gegen Entgelt oder in der Absicht sich oder einen anderen zu bereichern oder einen anderen zu schädigen. Gegen Entgelt handelt jedoch der Outsourcingpartner, also das private IT-Dienstleistungsunternehmen. Da § 44 BDSG kein Sonderdelikt ist, kommt hier der Outsourcingpartner selbst als Täter des § 44 BDSG in Betracht, während bei § 203 StGB lediglich eine Teilnehmerstrafbarkeit möglich ist[499].

§ 44 BDSG sichert den in § 5 BDSG geregelten Schutz des Datengeheimnisses strafrechtlich ab. Eine Strafbarkeit nach § 44 BDSG entfällt, wenn das Outsourcing datenschutzrechtlich zulässig ist. Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit es das

[499] Zum weiten Täterkreis bei § 44 BDSG vgl. Dammann, in: Simitis, BDSG, § 44 Rn. 5.

BDSG oder andere Vorschriften erlauben[500]. Hinsichtlich des Outsourcings solcher Daten kommen als Erlaubnisvorschriften die §§ 11, 16 und 28 BDSG in Betracht. Bereits im Rahmen der Untersuchung einer Strafbarkeit nach § 203 StGB wurde festgestellt, dass diese Vorschriften nicht zugleich strafrechtliche Erlaubnissätze darstellen. Zu prüfen bleibt, inwiefern sie als datenschutzrechtliche Erlaubnissätze für das Outsourcing medizinischer Daten eingreifen.

II. Auftragsdatenverarbeitung und Funktionsübertragung

Ein unbefugtes, gegen § 4 BDSG verstoßendes Verarbeiten personenbezogener Daten liegt nicht vor, wenn ein Fall der „Auftragsdatenverarbeitung" i.S.v. § 11 BDSG eingreift. Bei einer Auftragsdatenverarbeitung ist der Outsourcingpartner nicht als Dritter zu betrachten, eine Datenübermittlung zwischen Outsourcer und IT-Dienstleistungsunternehmen scheidet aus. Fraglich ist daher, unter welchen Voraussetzungen ein Outsourcing medizinischer Daten als „Auftragsdatenverarbeitung" i.S.v. § 11 BDSG zu qualifizieren ist.

§ 11 Abs. 1 BDSG zeigt, dass der Gesetzgeber davon ausgeht, dass die Auftragsdatenverarbeitung eine besondere Form der Datenverarbeitung ist. Der Gesetzgeber hat nicht eine eigene ausdrückliche Erlaubnis geschaffen, sondern geht von der grundsätzlichen Zulässigkeit der Auftragsdatenverarbeitung aus. Davon ausgehend stellt § 11 Abs. 1 S. 1 BDSG klar, dass der Auftraggeber für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich bleibt. Konsequent legt § 11 S. 2 BDSG dann fest, dass die in den §§ 6, 7 und 8 BDSG genannten Rechte dem Auftraggeber gegenüber geltend zu machen sind.

Die Absätze 2-4 des § 11 BDSG enthalten spezielle Voraussetzungen für das Auftragsverhältnis. Von zentraler Bedeutung ist dabei § 11 Abs. 3 BDSG. Hiernach darf der Auftragnehmer die Daten nur im Rahmen der Weisungen des Auftragge-

[500] Natürlich ist der Weg über eine Einwilligung auch hier möglich; allerdings ist bereits an anderer Stelle auf die praktischen Probleme eines solchen Weges hingewiesen worden. Im Übrigen müssen für eine datenschutzrechtlich wirksame Einwilligung zusätzlich die Voraussetzungen des § 4a BDSG beachtet werden, insbesondere § 4a Abs. 3 BDSG.

bers erheben, verarbeiten oder nutzen[501]. Der Auftragnehmer darf nicht im Sinne einer gleichberechtigten Partnerschaft in die Datenverarbeitung eingeschaltet sein. Übt der Auftragnehmer tatsächlich die Aufgabe der Datenverarbeitung eigenverantwortlich und mit voller Verfügungsgewalt aus, kann unabhängig von der Vertragsbezeichnung nicht von einer „Auftragsdatenverarbeitung" i.S.v. § 11 BDSG gesprochen werden, sondern es liegt dann eine Funktionsübertragung vor[502]. Die Bestimmung der Grenzlinie hat enorme praktische Bedeutung. Denn die datenschutzrechtliche Zulässigkeit richtet sich bei einer Funktionsübertragung nach § 16 BDSG bzw. § 28 BDSG. Außerdem würde eine Funktionsübertragung regelmäßig zu einer Verletzung der Schweigpflicht nach § 203 StGB führen.

Die Abgrenzung zwischen einer Auftragsdatenverarbeitung und einer Funktionsübertragung kann im Einzelfall schwer sein. Zu Recht wird auf diese Schwierigkeiten in der Literatur hingewiesen[503]. Sicherlich sind die Übergänge fließend und die Schwierigkeiten in der Abgrenzung führen zwangsläufig zu einer unter Rechtssicherheits- und Rechtsklarheitsaspekten wenig befriedigenden Situation. Sie können aber in der Konsequenz nicht bedeuten, dass eine Unterscheidung zwischen Auftragsdatenverarbeitung und Funktionsübertragung zu unterbleiben hat.

Auch in anderen Bereichen bestehen schwierige Abgrenzungsprobleme, ohne dass die Notwendigkeit einer Unterscheidung in Frage gestellt wird. Dies gilt beispielsweise für die Abgrenzung zwischen Arbeitnehmer und Selbständigen, die zudem noch nach unterschiedlichen Kriterien verläuft, je nach dem Rechtsgebiet, in dem die Unterscheidung notwendig wird. Da der Gesetzgeber die Einteilung nicht selbst vorgenommen hat, im Übrigen ist dies angesichts der vielfältigen Nuancen und Veränderungen in der Rechtswirklichkeit auch gar nicht abschließend möglich oder sinnvoll, aber erhebliche Konsequenzen an die eine oder andere Kategorie geknüpft hat, kann eine Entscheidung nur unter Abwägung aller Um-

---

[501] Dabei ist str., ob die Weisungsgebundenheit zu den Voraussetzungen oder den Rechtsfolgen zu zählen ist, vgl. Sieber, in: Hoeren/Sieber, Handbuch Multimedia Recht, Teil 19 Rn. 568.

[502] Vgl. zur Unterscheidung insbesondere Hilgendorf, in Hilgendorf: Informationsstrafrecht und Rechtsinformatik, S. 108f.; Evers/Kiene, DuD 2003, S. 341; Sutschet, RDV, 2004, S. 97 ff.; Kramer/Herrmann, CR 2003, S. 939; Walz, in: Simitis, BDSG, § 11 Rn. 18; Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 6 Rn. 10; vgl. für den Bereich des Outsourcings von Bankdienstleistungen Steding/Meyer, BB 2001, S. 1698 f.

[503] Vgl. Hoeren, in: Roßnagel, Handbuch des Datenschutzrechts, S. 623; Kilian/Scheja, RDV 2002, S. 180.

stände im konkreten Einzelfall erfolgen. Ein einzelnes Kriterium ist dabei weniger entscheidend, da es keine Bedeutung im Sinne einer festen, unveränderbaren Einflussgröße hat. Ausschlaggebend ist eine Gesamtbetrachtung der einzelnen Kriterien, die je nach Situation unterschiedliches Gewicht haben können. Der Arbeitnehmerbegriff ist somit zutreffend als ein entwicklungsoffener, typologischer Begriff zu bezeichnen[504].

Entsprechendes hat für den Begriff der „Auftragsdatenverarbeitung“ in Abgrenzung zur Funktionsübertragung zu gelten[505]. Der Gesetzgeber setzt die Unterscheidung nach der gewählten Systematik im BDSG stillschweigend voraus, ohne zu definieren, wann Auftragsdatenverarbeitung oder Funktionsübertragung vorliegt. Gleichwohl ergeben sich unterschiedliche Konsequenzen. Bei § 16 bzw. § 28 BDSG liegt eine Übermittlung vor, deren Zulässigkeit sich nach § 16 BDSG bzw. § 28 BDSG beurteilt, während bei der Auftragsdatenverarbeitung kein Dritter anzunehmen ist, an den übermittelt werden könnte.

Der Gesetzgeber impliziert seiner Systematik nach eine Unterscheidung zwischen Auftragsdatenverarbeitung und Funktionsübertragung. Wonach soll bei einer Aufgabe der Unterscheidung die datenschutzrechtliche Zulässigkeit auch sonst bestimmt werden? Etwa nur nach § 11 BDSG oder nach § 16 BDSG bzw. § 28, 29 BDSG oder kumulativ nach § 11 BDSG und § 16 BDSG bzw. §§ 28, 29 BDSG[506]? Keine dieser Konsequenzen entspräche der Intention oder der Systematik des Gesetzes. Vielmehr ist es allein überzeugend trotz der Abgrenzungsschwierigkeiten an der Unterscheidung zwischen Auftragsdatenverarbeitung und Funktionsübertragung festzuhalten[507].

---

[504] So das BAG in ständiger Rechtsprechung, vgl. BAG vom 23.4.1980 AP BGB § 611, Abhängigkeit, Nr. 34; BVerfG vom 20.5.1996 AP BGB § 611 Abhängigkeit, Nr. 82; a.A. Preis, in: Erfurter Kommentar zum Arbeitsrecht, § 611 Rn. 66.

[505] Abweichend teilweise die Literatur; so stellen Evers/Kiene, DuD 2003, S. 6 maßgeblich auf die Weisungsgebundenheit ab, anders wiederum Sutschet, RDV 2004, S. 101, der in der Weisungsgebundenheit eine Rechtsfolge der Auftragsdatenverarbeitung sieht und nicht eine Voraussetzung. Vielmehr sei maßgeblich auf unterschiedliche Interessen abzustellen. Kramer/Herrmann, CR 2003, S. 940f. stellen den Gefahrgedanken und das Kriterium der Überwachbarkeit in den Vordergrund.

[506] So wohl Hoeren, in: Roßnagel, Handbuch des Datenschutzrechts, S. 624.

[507] Hierfür sprechen schließlich auch die Gesetzesmaterialien, vgl. Sieber, in: Hoeren/Sieber, Handbuch Multimedia- Recht, Teil 19 Rn. 568.

Die Abgrenzung ist aus einer Gesamtbetrachtung der konkreten Umstände im Einzelfall zu leisten[508]. Auch hier kann nicht ein einzelnes Kriterium ausschlaggebend für die Zuordnung sein. Übt der Auftragnehmer nur Hilfstätigkeiten aus, dann spricht dies sicher für eine Auftragsdatenverarbeitung. Andererseits ist eine Auftragsdatenverarbeitung nicht ausgeschlossen, wenn der Auftragnehmer hochqualifizierte Tätigkeiten ausführt, solange sich aus den Gesamtumständen ergibt, dass der Auftraggeber „Herr der Daten bleibt", die Entscheidungshoheit hat, die Verfügungsgewalt über die Daten behält und sich des Auftragnehmers zur Erfüllung eigener Interessen bedient[509]. Gleichwohl können zur Orientierung Kriterien aufgestellt werden, die indiziell für oder gegen eine Einordnung als Auftragsdatenverarbeitung sprechen[510].

Nicht überzeugend ist, dass eine Auftragsdatenverarbeitung schon ausscheidet, wenn eine Funktion durch den Auftragnehmer ausgeführt wird[511]. Die Datenverarbeitung selbst und die Bereitstellung der dafür erforderlichen Ressourcen ist eine Aufgabe, die nach § 11 BDSG im Auftrag erfüllt werden kann. Alle anderen Aufgaben, für die ebenfalls eine Verarbeitung von Daten erforderlich ist, aus dem sachlichen Anwendungsbereich auszuschließen, ist nicht überzeugend. Bleibt nämlich der Auftraggeber im Außenverhältnis alleiniger Ansprechpartner, beherrscht und steuert er das Gesamtgeschehen, droht dem Betroffenen nicht mehr oder weniger Gefahr als bei einer alleinigen technischen Unterstützung der Datenverarbeitung. Der Begriff der Funktion oder Aufgabe kann beliebig weit gefasst werden und eignet sich nicht, um den Anwendungsbereich der Auftragsdatenverarbeitung zu bestimmen, da bei der sachlichen Festlegung des Aufgabeninhalts nichts über die maßgebliche personelle Verantwortung ausgesagt werden kann.

Aus der Sicht des Betroffenen ist aber allein die klare Verantwortungszuordnung maßgeblich. § 11 BDSG ordnet die Verantwortung für fremdes Handeln zu und sichert diese Verantwortung zugleich im Interesse des Betroffenen. Er will aber

---

[508] Vgl. Walz, in: Simitis, BDSG, § 11 Rn. 25; eine Abgrenzung nach den betroffenen Interessen schlägt Sutschet vor, vgl. Sutschet, RDV 2004, S. 99ff.
[509] Vgl. Kilian/Scheja, RDV 2000, S. 179f.; a.A. wohl die h.M. vgl. den 20. Tätigkeitsbericht des Bayerische Datenschutzbeauftragten 2003, S. 269.
[510] Bergmann/Möhrle/Herb, BDSG, § 11 Rn. 12; Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 108f.
[511] Vgl. Sutschet, RDV 2004, S. 99.

nicht die Erfüllung von Aufgaben durch andere sperren, sondern die Übertragung von Verantwortung. Dies zeigt auch ein Vergleich mit § 146 Abs. 1 SGB VI, der ausdrücklich die Aufgabenübertragung auf den Verband Deutscher Rentenversicherungsträger einschränkt. Das Sperren der Aufgabenübertragung ist im Bereich des öffentlichen Rechts Aufgabe der Zuständigkeitsregelungen, die nicht zur Disposition des Einzelnen stehen[512]. Im Bereich des Privatrechts hindern bei arbeitsteiligem Vorgehen die Schranken der Privatautonomie ein beliebiges Übertragen von Aufgaben[513].

Für das Outsourcing medizinischer Daten bedeutet das, dass der Vertragspartner des Outsourcers sich nicht nach § 44 BDSG strafbar machen kann, wenn das Outsourcing sich im Rahmen einer „Auftragsdatenverarbeitung" nach § 11 BDSG bewegt[514]. Dabei vermag § 11 BDSG nur zwischen Auftragnehmer und Auftraggeber rechtfertigend zu wirken. Das Heranziehen eines weiteren Subunternehmers durch den Auftragnehmer ist durch § 11 BDSG nicht gedeckt, da hierdurch die Gefahr einer Verantwortungsverlagerung aus der durch § 11 BDSG geregelten Einheit zwischen Auftragnehmer und Auftraggeber droht[515].

Das Ausgeführte gilt natürlich nur, soweit das BDSG anwendbar ist[516]. Sofern im öffentlichen Bereich andere Vorschriften zur Auftragsdatenverarbeitung vorrangig eingreifen, sind deren Zulässigkeitsvoraussetzungen maßgeblich. Hier sind zunächst die Landesdatenschutzgesetze zu nennen. Tritt eine öffentliche Stelle eines Landes als Outsourcer auf, richtet sich die Zulässigkeit einer Auftragsdatenverarbeitung wegen § 1 Abs. 2 Nr. 2 BDSG nach den entsprechenden Vorschriften der Landesdatenschutzgesetze, die weitgehend dem § 11 BDSG entsprechende Rege-

---

[512] Büllesbach/Rieß, NVwZ, 1995, S. 445; vgl. auch Walz, in: Simitis, BDSG § 11 Rn. 30; zu verfassungsrechtlichen Grenzen der Aufgabenübertragung vgl. Hartmann, Outsourcing in der Sozialverwaltung und Sozialdatenschutz, S. 27ff. und LG Konstanz vom 27.07.2006, Az.: 4 O 234/05 H.

[513] Insbesondere die §§ 134, 138, 242 BGB; vgl. allgemein zu Schranken der Privatautonomie Palandt, BGB, Einf. v. § 145 Rn. 7, 13.

[514] Neben § 11 BDSG sind bei einer Auftragsdatenverarbeitung keine weiteren Erlaubnistatbestände zu prüfen, vgl. Walz, in: Simitis, BDSG, § 11 Rn. 29; Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 111; a.A. Hoeren, in: Roßnagel, Handbuch des Datenschutzrechts, S. 624.

[515] Ebenso im Ergebnis Walz, in: Simitis, BDSG, § 11 Rn. 51.

[516] Wird durch Verschlüsselung, Anonymisierung oder Pseudonymisierung der Personenbezug der Daten aufgehoben, ist das BDSG nicht anwendbar. Dies gilt gleichermaßen für das Strafrecht wie für das Datenschutzrecht; vgl. dazu die Darstellung unter S. 48ff.

lungen enthalten[517]. Weiterhin sind im Bereich der stationären Gesundheitsversorgung die bereits an früherer Stelle angesprochenen speziellen sektorspezifischen Datenschutzregelungen der Länder zu beachten[518].

III. Vorsatz und Fahrlässigkeit

§ 44 BDSG stellt nur vorsätzliches Handeln unter Strafe. Auch bei einem Verstoß gegen § 43 Abs. 2 BDSG ist somit zumindest bedingter Vorsatz für eine Strafbarkeit nach § 44 BDSG erforderlich. Die Problematik im Vorsatzbereich entspricht der bei § 203 StGB. Ist bedingter Vorsatz zu verneinen, kommt nur das Vorliegen einer Ordnungswidrigkeit nach § 43 Abs. 2 BDSG in Betracht. Denn § 43 BDSG greift auch bei Fahrlässigkeit. Bei Verstößen gegen § 43 Abs. 2 BDSG droht eine Geldbuße von bis zu zweihundertfünfzigtausend Euro.

IV. Straftatbestände in den Landesdatenschutzgesetzen

In den Landesdatenschutzgesetzen finden sich Straftatbestände, die teilweise von § 44 BDSG abweichen[519]. So wird abweichend zu § 44 BDSG i.V.m. § 43 Abs. 2 Nr. 5 BDSG in vielen Landesdatenschutzgesetzen jegliche unbefugte Nutzung erfasst, der Versuch unter Strafe gestellt und auf eine Differenzierung zwischen Vorsatz und Fahrlässigkeit verzichtet[520]. Erfolgt bei einem Outsourcing im Rahmen einer Auftragsdatenverarbeitung nur eine Nutzung personenbezogener Daten durch den Auftragnehmer, wird dies von den Straftatbeständen der Landesdaten-

---

[517] Vgl. Art. 6 Bayerisches Datenschutzgesetz; im Übrigen enthalten die meisten Landesdatenschutzgesetze Regelungen, nach denen für öffentlich-rechtliche Wettbewerbsunternehmen die Vorschriften des BDSG bis auf den zweiten Abschnitt gelten, vgl. Art. 3 Abs. 1 S. 1 Bayerisches Datenschutzgesetz.

[518] Vgl. Art. 27 Abs. 4 Satz 5 Bayerisches Krankenhausgesetz.

[519] Nach der Rechtsprechung wird dies kaum Auswirkungen haben, da der BGH behauptet, dass § 203 StGB die Landesdatenschutzgesetze, soweit Überschneidungen bestehen, verdrängt, vgl. BGH RDV 2003, S. 130, 140.

[520] Vgl. § 41 i.V.m. § 40 Abs. 1 Nr. 1 Baden-Württembergisches Datenschutzgesetz, § 38 Abs. 1 Nr. 1 Brandenburgisches Datenschutzgesetz, § 32 Abs. 1 Nr. 1 Hamburgisches Datenschutzgesetz, § 28 Abs. 1 Nr. 1 Niedersächsisches Datenschutzgesetz, § 37 Abs. 1 Nr. 1 Rheinland-Pfälzisches Datenschutzgesetz, § 37 S. 1 Nr.1 Bremisches Datenschutzgesetz, § 40 Abs. 1 Nr. 1 Hessisches Datenschutzgesetz, § 38 Abs. 1 Nr. 1 Saarländisches Datenschutzgesetz, das aber in Abs. 2 eine Subsidiaritätsklausel enthält, wodurch ein Konflikt mit bundesrechtlichen Strafvorschriften, die den selben Sachverhalt regeln, vermieden wird, ebenso § 33 Nordrhein-Westfälisches Datenschutzgesetz; andere Landesdatenschutzgesetze bewegen sich weitgehend im Rahmen des § 44 BDSG, vgl. § 44 Schleswig-Holsteinisches Datenschutzgesetz, § 42 Datenschutzgesetz Mecklenburg- Vorpommern, Art. 37 Abs. 3 Bayerisches Datenschutzgesetz, § 43 Thüringer Datenschutzgesetz.

schutzgesetze erfasst. Hierdurch erfolgt gegenüber § 44 BDSG eine nicht unerhebliche Ausweitung der Strafbarkeit.

E. Outsourcing und strafrechtlicher Sozialgeheimnisschutz

Sofern das Outsourcing medizinischer Daten „Sozialdaten" i.S.v. § 67 Abs. 1 Satz 1 SGB X betrifft, sind das BDSG, aber auch die Landesdatenschutzgesetze, nicht anwendbar. Hier greifen die vorrangigen Vorschriften über den Schutz der Sozialdaten nach den §§ 67 ff. SGB X. In § 85a SGB X findet sich eine § 44 BDSG entsprechende Strafvorschrift. § 85 SGB X enthält eine § 43 BDSG entsprechende Bußgeldvorschrift.

I. Strafbarkeit nach § 85a SGB X

§ 85a SGB X stellt bestimmte, in § 85 Abs. 2 SGB X näher bezeichnete vorsätzliche Handlungen unter Strafe. Für das Outsourcing ist die in § 85 Abs. 2 Nr. 1 SGB X bezeichnete Handlung von Bedeutung. Wie bei § 43 Abs. 2 Nr. 1 BDSG ist dies das unbefugte Erheben oder Verarbeiten personenbezogener Daten. Weiterhin verlangt § 85a SGB X, dass die Handlung gegen Entgelt, in Bereicherungs- oder in Schädigungsabsicht begangen wird.

Diese Voraussetzungen werden für den Regelfall des Outsourcings medizinischer Daten bei dem Outsourcer nicht vorliegen. Für den Outsourcer kann regelmäßig nur eine Ordnungswidrigkeit unmittelbar nach § 85 Abs. 2 SGB X in Betracht kommen. Gegen Entgelt handelt aber der Outsourcingnehmer. Hier droht bei entsprechendem Vorsatz eine Strafbarkeit nach § 85a SGB X. Es stellt sich daher die Frage, ob eine Befugnis zur Durchbrechung des Sozialgeheimnisses hinsichtlich beabsichtigter Outsourcingmaßnahmen gefunden werden kann[521].

[521] Natürlich ist der Weg über eine Einwilligung auch hier möglich, allerdings ist bereits an anderer Stelle auf die praktischen Probleme eines solchen Weges hingewiesen worden. Im Übrigen müssen für eine sozialrechtlich wirksame Einwilligung zusätzlich die Voraussetzungen des § 67a SGB X beachtet werden, insbesondere § 67a Abs. 1 S. 4 SGB X.

II. Auftragsdatenverarbeitung nach § 80 SGB X

Die Auftragsdatenverarbeitung ist in § 80 SGB X geregelt[522]. Liegt im Outsourcing medizinischer Daten ein Fall zulässiger „Auftragsdatenverarbeitung" i.S.v. § 80 SGB X, kann kein unbefugtes Erheben oder Verarbeiten i.S.v. § 85 Abs. 2 SGB X vorliegen. Im Folgenden soll daher auf die Voraussetzungen des § 80 SGB X eingegangen werden.

Entsprechend der Regelung in § 11 BDSG ist auch bei § 80 SGB X erforderlich, dass der Auftraggeber „Herr der Daten" bleibt, die Entscheidungshoheit behält und die volle Verfügungsgewalt nicht an den Auftragnehmer abgibt. Über das Institut der „Auftragsdatenverarbeitung" darf es im Außenverhältnis zum Betroffenen nicht zu einer Delegation der Verantwortung durch den Auftraggeber oder zu einer Absenkung des Datenschutzniveaus kommen. Die Problematik der Unterscheidung von Auftragsdatenverarbeitung und Funktionsübertragung entspricht derjenigen im BDSG. Die bei § 11 BDSG angesprochenen Kriterien für eine Einordnung hinsichtlich einer Auftragsdatenverarbeitung bzw. einer Funktionsübertragung gelten auch in diesem Zusammenhang. Auch hier bedarf es einer Gesamtbetrachtung unter Abwägung aller konkreten Umstände im Einzelfall.

§ 80 SGB X weicht aber in einigen Aspekten von § 11 BDSG ab, insbesondere dann, wenn der Auftragnehmer eine nicht-öffentliche Stelle ist. Relativ unproblematisch sind dabei die Regelungen in § 80 Abs. 2 Satz 4 Nr. 1-3 SGB X. Diese Regelungen, die bestimmte Auskunfts-, Einsichts- und Kontrollrechte für den Auftraggeber fordern, sichern die alleinige Verantwortung des Auftraggebers im Außenverhältnis zum Betroffenen. Sie wollen ermöglichen, dass der Auftraggeber seiner Überwachungspflicht dem Auftragnehmer gegenüber gerecht werden kann und nicht im Nachhinein im privaten Bereich unter Hinweis auf die fehlende Kooperation des Auftragnehmers eine Überwachung des Auftragnehmers als unmöglich bezeichnet wird.

Eine erhebliche und inhaltlich problematische Abweichung von § 11 BDSG ist in § 80 Abs. 5 SGB X geregelt. Danach ist eine Auftragsdatenverarbeitung durch

[522] Auf ein konkretes Beispiel, allerdings zu § 80 SGB X, gehen Klinger/Kunkel ein, vgl. Klinger/Kunkel, Sozialdatenschutz in der Praxis, S. 84.

eine nicht-öffentliche Stelle nur unter sehr restriktiven Bedingungen möglich. Eine nicht-öffentliche Stelle kann nach § 80 Abs. 5 Nr. 1 SGB X eingeschaltet werden, wenn sonst Störungen im Betriebsablauf auftreten können. Als Störung kann insbesondere der Eintritt unvorhergesehener Ereignisse bezeichnet werden[523]. In der Regel wird diese Variante nicht einschlägig sein, weil das Outsourcing regelmäßig zur Effizienzsteigerung und Realisierung von Kostenvorteilen erfolgt. Solche Situationen erfasst allein der insoweit speziellere § 80 Abs. 5 Nr. 2 SGB X[524].

Allerdings verlangt § 80 Abs. 5 Nr. 2 SGB X, dass die übertragenen Arbeiten erheblich kostengünstiger besorgt werden können, ohne näher zu klären, was unter „erheblich kostengünstiger" zu verstehen ist. Auch in der Literatur finden sich nur zurückhaltende Erläuterungen[525].

Die nähere Bestimmung dieses Begriffs muss an der Intention des Gesetzgebers ansetzen. Der Gesetzgeber bringt über die formulierten Restriktionen zum Ausdruck, dass er bei einer Beauftragung einer nicht-öffentliche Stelle größere Gefahren sieht, als bei der Beauftragung einer öffentlichen Stelle. Er setzt damit für den Umgang mit den besonders schutzwürdigen Sozialdaten ein höheres Vertrauen in öffentliche Stellen. Daher müssen gewichtige Gründe für ein Heranziehen privater Anbieter aus finanziellen Gesichtspunkten sprechen.

Diese Bewertung mag als rechts- und wirtschaftspolitisch überkommen betrachtet werden. Diese gesetzgeberische Entscheidung ist de lege lata aber zu beachten. Eine Überschreitung gesetzgeberischen Gestaltungsspielraums kann nicht angenommen werden. Zwar sprechen für private Anbieter die Berufsfreiheit aus Art. 12 Abs. 1 GG und der Gleichheitsgrundsatz nach Art. 3 GG. Auf der anderen Seite steht aber das Sicherungsbedürfnis der Betroffenen, das aus dem Schutz ihres Rechts auf informationelle Selbstbestimmung resultiert. Das Heranziehen einer weiteren Stelle als Auftragnehmer stellt eine Einschränkung dieses Rechts dar.

---

[523] Vgl. Seidel, in: Lehr- und Praxiskommentar, SGB X, § 80 Rn. 11.
[524] So zutreffend Kessler, DuD 2004, S. 40, 42.
[525] Für das Outsourcing von Versicherungsdaten soll Grundlage ein betriebswirtschaftlicher Kostenvergleich zwischen hauseigener Datenverwaltung und einer Fremdvergabe sein, vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 115; vgl. auch Steinmeyer, in: Wannagat, Sozialgesetzbuch, Zehntes Buch, § 80, Rn. 25f., der Kriterien für die Bestimmung des Begriffs nennt.

Einschränkungen des Rechts auf informationelle Selbstbestimmung müssen dem Verhältnismäßigkeitsgrundsatz genügen, um die Einschränkungen ihrerseits zu rechtfertigen. Insbesondere muss der Zweck der beabsichtigten Gestaltung, durch die das informationelle Selbstbestimmungsrecht eingeschränkt wird, im angemessenen Verhältnis zum eingesetzten Mittel stehen.

Diesen Anforderungen ist der Gesetzgeber mit dem gefundenen Ausgleich zwischen den Interessen der nicht-öffentlichen Unternehmen an der Tätigkeit als Dienstleistungsunternehmen und dem Interesse der Betroffenen an der Wahrung ihrer informationellen Selbstbestimmung gerecht geworden. Bei der Aufstellung besonderer Anforderungen an das Heranziehen nicht-öffentlicher Stellen im Rahmen einer Datenverarbeitung im Auftrag hat sich der Gesetzgeber nicht von sachlich nicht nachvollziehbaren Gründen leiten lassen. Private Unternehmen unterliegen nämlich nicht im gleichen Maße einer Gesetzesbindung wie öffentliche Stellen. Darüber hinaus sind Sozialdaten, soweit sie „Geheimnisse“ i.S.v. § 203 StGB darstellen, kein frei handelbares Wirtschaftsgut, sondern sind wegen des fachlichen Bezugs eng an die Sozialverwaltung gebunden. Hier sind Beschränkungen des Heranziehens privater Unternehmen zur Datenverwaltung eher tolerabel als im allgemeinen Bereich personenbezogener Daten.

Daher kann auch nicht durchschlagend argumentiert werden, dass in § 11 BDSG keine Unterscheidung zwischen privaten und öffentlichen Auftragnehmern hinsichtlich der Voraussetzungen der Auftragsdatenverarbeitung erfolgt. Das BDSG gilt nämlich allgemein für personenbezogene Daten, während die §§ 67 ff. SGB X nur bei Sozialdaten anwendbar sind. Personenbezogene Daten werden erst über einen speziellen fachlichen Bezug zu den in § 35 SGB I genannten Stellen zu Sozialdaten. Wegen dieses fachlichen Bezuges haben Sozialdaten einen für die Betroffenen bedeutsamen Inhalt, der bei unbefugter Kenntnisnahme durch Dritte einen erheblichen sozialen Schaden herbeiführen kann.

Schließlich ist das Folgende zu beachten: Medizinische Daten, die Sozialdaten sind, werden oft zugleich „Geheimnisse“ i. S. v. § 203 StGB sein. Ein Offenbaren bedarf daher, sofern Geheimnisse nicht innerhalb des Kreises der zum Wissen Berufenen weitergegeben werden, einer Befugnis zum Offenbaren. Soweit keine speziellen Befugnisse greifen, kann sich die Befugnis nur aus § 34 StGB oder den

Grundsätzen der Abwägung widerstreitender Interessen oder Pflichten ergeben. In beiden Fällen muss eine Abwägung ergeben, dass das Interesse am Offenbaren das Interesse am Schutz des Rechts auf informationelle Selbstbestimmung überwiegt. Vor diesem Hintergrund erscheint die Voraussetzung, dass finanzielle Interessen nur maßgeblich sein dürfen, wenn der nicht-öffentliche Auftragnehmer die Tätigkeit erheblich kostengünstiger ausführen kann, nicht unvernünftig.

Greifen verfassungsrechtliche Bedenken nicht durch, bleibt zu klären, wann die Tätigkeit eines privaten Auftragnehmers als erheblich kostengünstiger angesehen werden kann. Diese Frage kann nur nach einem betriebswirtschaftlichen Kostenvergleich mit der öffentlichen Stelle beantwortet werden. Wegen der Vielfältigkeit, der Zukunftsbezogenheit sowie der schwer abschätzbaren Einflussfaktoren, die Erfolg oder Misserfolg von Outsourcingvorhaben ausmachen können, ist die Berechnung von Kostenvorteilen ein schwieriger Vorgang und geht notwendig mit einer Prognose einher. Um die Vorschrift des § 80 Abs. 5 SGB X nicht leerlaufen zu lassen und den Handlungsspielraum des Auftraggebers zu sichern, ist dem Auftraggeber daher ein gerichtlich nicht überprüfbarer Beurteilungsspielraum beim Kostenvergleich zuzubilligen[526]. Allerdings muss eine nachvollziehbare und verständliche Berechnung des Kostenvorteils als Entscheidungsgrundlage vorliegen. Die Berechnung muss betriebswirtschaftlichen Anforderungen genügen. Ergibt ein solcher betriebswirtschaftlicher Kostenvergleich mit öffentlichen Stellen, dass Einsparungen zu erwarten sind, wird man regelmäßig davon auszugehen haben, dass die Voraussetzung „erheblich kostengünstiger“ erfüllt ist.

§ 80 Abs. 5 Nr. 2 SGB X setzt weiterhin voraus, dass die Auftragsdatenverarbeitung nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfassen darf. Der überwiegende Teil des Datenbestandes muss beim Auftraggeber verbleiben. Unter dem überwiegenden Teil sind mehr als 50 % des gesamten Datenbestandes zu verstehen[527]. Soweit der Auftragnehmer Daten nicht speichert, darf die Auftragsdatenverarbeitung auch den gesamten Datenbestand umfassen[528].

---

[526] Ähnlich Seidel, in: Lehr- und Praxiskommentar SGB X, § 80 Rn. 11; Pickel spricht davon, dass ein „gewisser Beurteilungsspielraum für den Auftraggeber gegeben ist“, vgl. Pickel, SGB 2000, S. 202; vgl. generell zur gerichtlichen Überprüfbarkeit von unbestimmten Rechtsbegriffen Schoch, Jura 2004, S. 612 ff.

[527] Kessler, DuD 2004, S. 40, 42; Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 115 f.

[528] BT-Drucksache 12/6334, S. 11.

Eine Aufrufmöglichkeit durch den Auftragnehmer hinsichtlich der physisch beim Auftraggeber gespeicherten Daten wird durch § 80 SGB X nicht beschränkt. Dies ergibt sich aus dem insoweit klaren Wortlaut des § 80 SGB X. Wenn in der Literatur gefordert wird, dass der Auftragnehmer auf weniger als 50 % des gesamten Datenbestandes Zugriff haben darf, weil bei einer Auftragsdatenverarbeitung der Auftraggeber wegen der beibehaltenen Kontroll- und Zugriffsrechte ohnehin stets die Verfügungsgewalt über den gesamten Datenbestand hat[529], kann dem nur soweit zugestimmt werden, als ein Zugriffsrecht auf die beim Auftraggeber gespeicherten Daten gemeint ist. Denn der Gesetzgeber hat klar zum Ausdruck gebracht, dass er nur einer physischen Ortsverlagerung gespeicherter Information quantitativ Grenzen setzen wollte. Bleibt das Speichermedium beim Auftraggeber und kann der Auftragnehmer über eine Verbindung zugreifen, gilt die 50 %-Beschränkung nicht. Rechtliche Gestaltungen, die bei auswärtigem Standort des Speichermediums allein über schuldrechtliche Nutzungsrechte, beispielsweise über ein Mietverhältnis an den Räumen, in denen sich die Datenverarbeitungsanlage befindet, eine Zuordnung zum Auftraggeber erreichen sollen, würden der Voraussetzung nicht gerecht werden. Denn auf die gespeicherte Information hätte tatsächlich der Auftragnehmer Zugriff. Sie ist daher beim Auftragnehmer gespeichert und nicht beim Auftraggeber.

Zu beachten bleibt, dass mit der Zulässigkeit einer Auftragsdatenverarbeitung nichts über die Zulässigkeit nach § 203 StGB gesagt ist, da nach der hier vertretenen Auffassung § 80 SGB X keinen strafrechtlichen Erlaubnissatz darstellt. Da die Einschränkungen des § 76 SGB X auch bei § 80 SGB X gelten[530], ist eine „Auftragsdatenverarbeitung“ nach § 80 SGB X bei Sozialdaten, die dem Auftraggeber von einer nach § 203 StGB schweigepflichtigen Person zugänglich gemacht worden sind, nur zulässig, wenn die Voraussetzungen des § 203 StGB erfüllt werden.

Unklar ist weiterhin, wie festgestellt werden soll, ob mehr als 50 Prozent des gesamten gespeicherten Datenbestandes betroffen sind. In der Literatur wird darauf hingewiesen, dass bei Schriftstücken fraglich ist, ob nach Zeichen, Seiten oder

[529] Vgl. etwa Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 116.
[530] Vgl. Seidel, in: Lehr- und Praxiskommentar Sozialgesetzbuch X, § 80 Rn. 6.

Akten die Hälfte des Datenbestandes berechnet werden soll[531]. Zudem besteht bei Daten in elektronischer Form das Problem, dass diese vielfach in verschiedenen Datenformaten vorliegen und die Größe des Datenbestandes je nach Verarbeitungsphase variiert[532].

Tatsächlich ist eine exakte Überprüfung nach der jetzigen Fassung des § 80 Abs. 5 Nr. 2 SGB X kaum möglich. Der Befund *Hilgendorfs*, § 80 Abs. 5 Nr. 2 sei technisch missglückt, ist daher zutreffend[533]. Für die Anwendung der Norm bleibt aber die Frage nach welchem Maßstab der Wert des gesamten Datenbestandes als Referenzgröße zu bestimmen ist. Als Lösung bietet sich an, auf die übliche Maßeinheit für Informationseinheiten, das Byte, abzustellen. Ein Byte besteht dabei aus 8 Bit, wobei unter einem Bit die kleinste Informationseinheit in der EDV zu verstehen ist[534].

Zu fordern ist, dass nachvollziehbar der Byte-Wert des Datenbestandes zu einem bestimmten Zeitpunkt vor Beginn der Auftragsvergabe und regelmäßig danach ermittelt wird. In die Analyse sind sämtliche Speichermedien des Auftraggebers einzubeziehen. Eine 100% byte-genaue Bestimmung ist nicht erforderlich, um dem Zweck der Norm gerecht zu werden. Eine solche byte-genaue Bestimmung wäre, wenn überhaupt, nur mit unverhältnismäßigem Aufwand möglich. Ausreichend ist eine nachvollziehbare Annäherung, die eine verlässliche Orientierung über den Gesamtdatenbestand geben kann.

Dabei ist nicht auf einzelne aktuelle Datenverarbeitungsprozesse einzugehen, sondern auf ein notwendiges „back up Volumen“. Ein solches „back up“ hat nach den Grundsätzen einer ordnungsgemäßen Datenverarbeitung[535] regelmäßig zu erfolgen und ist damit taugliche Grundlage für einen Referenzwert. Der so gewonnene Wert ist hinreichend genau, um den Anforderungen in § 80 Abs. 5 Nr. 2 SGB X gerecht zu werden. Denn der Gesetzgeber ging davon aus, dass quantitativ eine Speicherung beim Auftraggeber zu begrenzen ist, weil ansonsten eine erhöhte

[531] Vgl. Kessler, DuD 2004, S. 40, 42.
[532] Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 115.
[533] Vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 116.
[534] Nicht zu verwechseln mit dem bit, das die Einheit des Informationsgehalts darstellt; vgl. Breuer, dtv-Atlas zur Informatik, S. 33.
[535] Zu diesen Grundsätzen Jürgens, in: Bäumler/Breinlinger/Schrader, Datenschutz von A-Z, O 300.

Missbrauchsgefahr besteht. Wird festgestellt, dass das gespeicherte Datenvolumen mehr als 50 % des Referenzwertes überschreitet, entfällt § 80 Abs. 5 SGB X als Rechtsgrundlage für die Auftragsdatenverarbeitung mit der Folge, dass eine rechtswidrige Datenweitergabe vorliegen kann.

Ob ein Abstellen auf die Quantität der gespeicherten Daten aus rechtspolitischer Sicht ein taugliches Kriterium ist, kann zu Recht bezweifelt werden. Dies ändert aber nichts daran, dass sich eine Auslegung daran ausrichten muss.

§ 85a SGB X stellt weiterhin wie § 44 BDSG nur vorsätzliches Handeln unter Strafe. Bei fahrlässigem Handeln kommt nur eine Ordnungswidrigkeit nach § 85a Abs. 2 SGB X in Frage, die mit einer Geldbuße in Höhe von bis zu zweihundertfünfzigtausend Euro geahndet werden kann.

F. Offshore-Outsourcing

Ging es in der vorstehenden Untersuchung um die strafrechtliche Betrachtung des Outsourcings medizinischer Daten im Inland, soll im Folgenden auch auf das Offshore-Outsourcing eingegangen werden. Beim Offshore-Outsourcing ist der Outsourcingpartner regelmäßig ein ausländisches IT-Dienstleistungsunternehmen[536]. Der Outsourcer kann sich im Inland oder im Ausland befinden. Bei der strafrechtlichen Beurteilung sind zwei Hauptaspekte zu unterscheiden. Zum einen ist fraglich, ob deutsches Strafrecht anwendbar ist. Hier ist die Reichweite deutschen Strafrechts auf ein Outsourcing mit Auslandbezug zu bestimmen. Insbesondere für Mitarbeiter ausländischer Unternehmen ist hierbei das Risiko nach deutschem Recht bestraft zu werden bedeutsam. Zum andern stellt sich die Frage, ob strafrechtlich das Heranziehen eines privaten IT-Dienstleistungsunternehmens aus dem Ausland zulässig ist.

Letztere Frage ist bezüglich § 203 StGB zu bejahen. Die gefundenen Ergebnisse zu § 203 StGB sind auch beim Heranziehen eines ausländischen IT-Dienstleistungsunternehmens gültig. Wird der Mitarbeiter eines ausländischen Dritten tatsächlich entsprechend dem Mitarbeiter eines inländischen IT-

[536] Zu Beispielen vgl. Bergmann, Grenzüberschreitender Datenschutz, S. 31.

Dienstleistungsunternehmens eingebunden, kann ebenfalls eine tatbestandliche Verantwortungseinheit angenommen werden.

Hinsichtlich einer Strafbarkeit nach § 44 BDSG ist zu differenzieren. Aufgrund § 3 Abs. 8 BDSG, der Vorgaben der Europäischen Datenschutzrichtlinie umsetzt, ist eine Auftragsvergabe an Stellen aus anderen EU- oder EWR Staaten einer Auftragsvergabe an inländische Stellen gleichgestellt. In beiden Fällen liegt keine Datenübermittlung vor, so dass sich die Zulässigkeit allein nach § 11 BDSG bemisst[537]. Eine Auftragsdatenverarbeitung außerhalb der EU- oder EWR Staaten ist im Umkehrschluss unzulässig[538]. Bewegt sich die Auftragsdatenverarbeitung im Rahmen des § 11 BDSG, kommt die Erfüllung des Straftatbestandes des § 44 BDSG nicht in Betracht. Gleiches ist wegen § 67 Abs. 10 SGB X, der § 3 Abs. 8 BDSG entspricht, hinsichtlich einer Strafbarkeit nach § 85a SGB X anzunehmen.

Grundlage für die Beantwortung der Frage, welches nationale Strafrecht Anwendung findet, sind zunächst die §§ 3-7, 9 StGB, die das sog. „internationale Strafrecht“ regeln. Diese Vorschriften sind heranzuziehen, soweit es um die Anwendbarkeit deutschen Strafrechts und damit auch des § 203 StGB geht. Weiterhin findet sich in § 1 Abs. 5 BDSG eine Vorschrift über den internationalen Geltungsbereich deutschen Datenschutz(straf-)rechts.

Für die Frage der Anwendbarkeit des StGB ist zunächst von § 3 StGB auszugehen, der das sog. „Territorialprinzip“ regelt. Hiernach ist zur Ermittlung maßgeblich auf den Begehungsort abzustellen. Begehungsort ist nach § 9 StGB entweder der Handlungsort oder der Erfolgsort. Da § 203 StGB die Verletzung von Privatgeheimnissen unter Strafe stellt und für eine Verletzung ein Übergehen des Geheimnisses aus dem Bereich des Schweigepflichtigen in den Bereich eines anderen eintreten muss, ist § 203 StGB als Erfolgsdelikt einzuordnen[539] mit der Folge, dass Begehungsort bei § 203 StGB neben dem Handlungsort auch der Erfolgsort sein kann[540]. Daher wird für den Outsourcer, der den Tatbestand des § 203 StGB verwirklicht, eine Strafbarkeit nach § 203 StGB möglich sein, sofern der Outsour-

[537] Walz, in: Simitis, BDSG, § 11 Rn. 4.
[538] Vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 88; Walz, in: Simitis, BDSG, § 11 Rn. 17; erforderlich wäre ein datenschutzrechtlicher Erlaubnissatz hinsichtlich einer Übermittlung, also z.B. § 28 BDSG.
[539] Vgl. bereits oben Fußnote 110.
[540] Zutreffend Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 87.

cer in Deutschland belegen ist und die Datenweitergabe aus dem Inland erfolgt bzw. auf Daten im Inland zugegriffen wird. Denn dann liegt der Handlungsort in Deutschland, unabhängig davon, dass der Erfolgsort im Ausland liegen kann.

Problematischer sind die Fälle, in denen im Ausland gehandelt wird. Dabei muss differenziert werden: Befindet sich der Outsourcer im Ausland und bedient sich eines inländischen Dienstleisters liegt der Erfolgsort im Inland, so dass hierüber deutsches Strafrecht Anwendung finden kann. Wenn Erfolgs- und Handlungsort im Inland liegen, kann sich eine Strafbarkeit des Ausländers nicht über die §§ 3, 9 Abs. 1 StGB ergeben, da Mittäterschaft bei der Verwirklichung der § 203 StGB aufgrund der Einordnung als Sonderdelikt nicht angenommen werden kann[541]. Nimmt der Ausländer aber an der Verwirklichung des § 203 StGB in Deutschland im Sinne einer Beihilfe oder Anstiftung teil, dann würde die Anwendung deutschen Strafrechts aus § 9 Abs. 2 StGB resultieren und sich hier durchaus Strafbarkeitsrisiken auch für ausländische Mitarbeiter von Dienstleistungsunternehmen ergeben können.

Bleibt der physikalische Standort im Ausland und erfolgt das Outsourcing im Ausland unter Heranziehung eines ausländischen Dienstleisters, dann liegen sowohl Handlungs- als auch Erfolgsort im Ausland. In solchen Fällen, in denen Erfolgs- und Handlungsort nicht auf deutschem Territorium liegen, kommt die Anwendbarkeit deutschen Strafrechts nicht über § 9 Abs. 1 StGB in Betracht. Allerdings kann deutsches Strafrecht über § 9 Abs. 2 StGB oder § 7 Abs. 1 StGB Anwendung finden[542]. § 9 Abs. 2 StGB ist einschlägig, wenn von Deutschland aus Unterstützung bei einem den Tatbestand des § 203 StGB verwirklichenden Outsourcings geleistet wird. Dabei spielt es nach § 9 Abs. 2 S. 2 keine Rolle, ob die Tat am Tatort mit Strafe bedroht ist, so dass es unerheblich ist, ob im Ausland ein § 203 StGB vergleichbarer Straftatbestand besteht. Dies ist auch sachgerecht, soweit Geheimnisse von inländischen Personen betroffen sind, da einer Verlagerung

[541] Zur Begründung über die Figur der Mittäterschaft vgl. BGH NJW 2007, S. 787; die Frage einer Mittäterschaft kann im Rahmen des § 85a SBG X bzw. § 44 BDSG Bedeutung gewinnen. Zu den geringen Anforderungen der Rechtsprechung bei der Annahme von Mittäterschaft in objektiver Hinsicht vgl. Wessels/Beulke, Strafrecht AT Rn. 528 und BGH JuS 2000, 1234. Im Rahmen geplanter Outsourcingvorhaben resultiert daraus ein erhebliches Risiko einer Täterschaft für die Outsourcingpartner.

[542] § 5 Nr. 7 StGB gilt nur für Betriebs- und Geschäftsgeheimnisse, die beim Outsourcing medizinischer Daten nicht betroffen sind; zu § 9 Abs. 2 StGB vgl. Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 87.

in Länder vorgebeugt wird, in denen ein vergleichbarer strafrechtlicher Geheimnisschutz nicht besteht. Da in dem Entsenden von Daten eine relevante Beihilfehandlung liegen kann, ist der Weg, ein Outsourcing durch eine im Ausland gegründete Tochtergesellschaft durchführen zu lassen, mit der Anwendbarkeit deutschen Strafrechts verbunden, auch wenn im Ausland die Geheimnisverletzung nicht unter Strafe gestellt ist.

§ 7 Abs. 1 StGB greift dann ein, wenn im Ausland der Tatbestand des § 203 StGB verwirklicht wird und Geheimnisse eines deutschen Geheimnisträgers betroffen sind. Allerdings muss die Tat auch im Ausland mit Strafe bedroht sein oder der Tatort keiner Strafgewalt unterliegen. Dies setzt das Vorhandensein eines mit § 203 StGB vergleichbaren Straftatbestandes voraus. Schließlich ist auch denkbar, dass das Outsourcing im Ausland durch einen Deutschen begangen wird, allerdings Geheimnisse ausländischer Personen betroffen sind. In einem solchen Fall kann sich die Anwendbarkeit deutschen Strafrechts aus § 7 Abs. 2 Nr. 1 StGB ergeben, sofern die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt.

Im Datenschutzstrafrecht ist nicht primär auf die §§ 3-7, 9 StGB, sondern auf § 1 Abs. 5 BDSG abzustellen. Dies folgt aus Erwägungsgrund 21 der Richtlinie 95/46/EG, nach dem die Richtlinie nicht die im Strafrecht geltenden Territorialitätsregeln berührt. Die Frage des anwendbaren Strafrechts ist somit, soweit an das Territorium angeknüpft wird, sowohl nach §§ 3, 9 StGB als auch nach § 1 Abs. 5 BDSG zu bestimmen, ansonsten nach § 1 Abs. 5 BDSG. Nach § 1 Abs. 5 S. 1 BDSG findet das BDSG keine Anwendung, wenn ein Outsourcer seinen Hauptsitz in einem anderen Mitgliedsstaat hat und dort das Outsourcing im Wege einer Auftragsdatenverarbeitung betreibt. Fraglich ist, ob dies wegen § 1 Abs. 5 Alt. 2 BDSG auch gilt, wenn eine Auftragsdatenverarbeitung durch eine inländische Niederlassung als Auftragsnehmer durchgeführt wird.

Der für die Frage des anwendbaren Rechts zentrale Begriff der „Niederlassung“ wird in Erwägungsgrund Nr. 19 der Richtlinie 95/46/EG erläutert. Danach setzt eine Niederlassung im Hoheitsgebiet eines Mitgliedsstaates eine effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus. Davon ausgehend wird in der Literatur eine Niederlassung i.S.v. § 1 Abs. 5 BDSG

angenommen, wenn eine gewisse räumliche oder zeitlich vorhandene Zuordnung gegeben ist[543]. Auszugehen sei von einem weiten Niederlassungsbegriff[544]. Ein Abstellen auf § 42 Abs. 2 Gewerbeordnung, der für eine Niederlassung einen festen Raum erfordert, würde der „virtuellen Welt globaler Datenflüsse nur schwer gerecht“[545]. Nach dieser Ansicht würden auch angemietete Server eine Niederlassung begründen. Dieser Ansicht ist nicht zu folgen. Das Erfordernis eines festen Raumes ermöglicht eine verhältnismäßig sichere Abgrenzung von Organisationsbereichen und legitimiert damit die Anwendung des jeweiligen Datenschutzrechts. Damit wird dem Regel-Ausnahme-Prinzip in § 1 Abs. 5 BDSG Rechnung getragen. Denn nach § 1 Abs. 5 S. 1 Alt. 2 BDSG ist als Ausnahme das BDSG anwendbar, wenn eine Niederlassung besteht. Vor dem Hintergrund, dass die Richtlinie den freien Datenverkehr in ihrem räumlichen Anwendungsbereich ermöglichen will, bedarf es zur Anwendung des aus Sicht der Stelle am Hauptsitz fremden Datenschutzrechts einer Verknüpfung der Tätigkeit einer natürlichen Person mit bestimmten Räumen, in denen die Tätigkeit organisatorisch abgebildet wird. Daher ist der Auffassung zu folgen, die den Begriff der Niederlassung in Anlehnung an § 42 Gewerbeordnung definiert. Angemietete Server fallen danach nicht unter den Begriff der Niederlassung[546].

Nach § 1 Abs. 5 S. 2 Alt. 2 BDSG ist deutsches Datenschutzrechts ausnahmsweise wieder anwendbar, wenn die Datenverarbeitung durch eine Niederlassung im Inland erfolgt. Das Gesetz geht davon aus, dass im Binnenmarkt eine Ausdehnung deutschen Datenschutzstrafrechts nicht erforderlich ist, wenn sich die maßgeblichen Aktivitäten hinsichtlich der Verarbeitungsvorgänge allein im europäischen Ausland abspielen. Anknüpfungspunkt für eine Anwendung des Datenschutzstrafrechts ist der Ort, an dem die verantwortliche Entscheidung über das Outsourcing getroffen wird unabhängig davon, wo dann das Outsourcing durchgeführt wird[547]. Man kann daher argumentieren, dass im Fall der Auftragsdatenverarbeitung durch eine inländische Niederlassung keine Datenverarbeitung durch die Niederlassung

[543] Bergmann/Möhrle/Herb, BDSG, § 1 Rn. 43.
[544] Zum Begriff der „Niederlassung“ vgl. Dammann/Simitis, in: Simitis, BDSG, § 3 Rn. 254 und Dolderer/von Garrel/Müthlein/Schlumberger, RDV 2001, S. 230.
[545] Bergmann/Möhrle/Herb, BDSG, § 1 Rn. 42.
[546] Dammann in: Simitis, BDSG, § 1, Rn. 203; a.A. Ehmann/Helfrich, EG-Datenschutzrichtlinie, Art. 4 Rn. 15.
[547] So Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik, S. 88.

erfolgt, sondern durch die im Ausland belegene Hauptstelle als Auftraggeber[548]. Zweifel an der Anwendbarkeit deutschen Datenschutzrechts könnten deshalb angebracht sein, weil die Datenverarbeitung auf Weisung und unter Kontrolle des ausländischen Unternehmens erfolgt und nach deutschem Verständnis eine Niederlassung regelmäßig keine verantwortliche Stellung darstellt, sondern einer solchen angehört[549].

Dies überzeugt nicht. Entscheidend dagegen spricht, dass den von der Datenverarbeitung im Inland Betroffenen nicht zugemutet werden kann, ihre Schutzrechte nach ausländischem Recht zu ermitteln. Die Belange des verarbeitenden Unternehmens mit Hauptsitz im europäischen Ausland sind demgegenüber hinreichend durch das Erfordernis einer Niederlassung berücksichtigt. Sofern keine Niederlassung im Inland eingerichtet ist, bleibt es beim Datenschutzrecht des Sitzlandes, das exportiert werden kann. Für diese Auffassung spricht weiterhin, dass andernfalls über die Gründung von Niederlassungen und der Ausgestaltung als Auftragsdatenverarbeitung die Regelung in § 1 Abs. 5 S. 2 Alt. 2 BDSG ausgehöhlt werden könnte. Je nach nationalen Voraussetzungen für die Auftragsdatenverarbeitung würde damit auch bei einem erheblichen Ausmaß an inländischer Datenverarbeitungsaktivität über Niederlassungen ausländisches Datenschutzrecht Anwendung finden. Demgegenüber ist dem deutschen Verständnis der Niederlassung als grundsätzlich unselbständige Einheit für das Datenschutzrecht nicht zu folgen. Denn sobald organisatorisch und räumlich abgrenzbare Einheiten vorhanden sind, in denen Daten verarbeitet werden, sind die Voraussetzungen von Art. 4 Abs. 1 lit. a der Richtlinie 95/46/EG erfüllt, wonach der Mitgliedstaat seine Vorschriften auf alle Verarbeitungen personenbezogener Daten anwendet, die im Rahmen der Tätigkeit einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedsstaats besitzt. Danach kann es nicht maßgeblich sein, ob die Verarbeitung weisungsgebunden oder nicht weisungsgebunden erfolgt. Im Hinblick auf Art. 4 Abs. 1 lit. a ist jede Niederlassung als verantwortliche Stelle anzusehen mit der Folge, dass nach § 1 Abs. 5 BDSG das BDSG Anwendung findet.

---

[548] So wohl Dammann in: Damman/Simitis, BDSG, § 1 Rn. 201, der aber für den Fall, dass eine Niederlassung im Inland Daten im Auftrag für eine ausländische Muttergesellschaft verarbeitet, nur bestimmte Regelungen des BDSG anwenden will; nicht differenzierend Bergmann/Möhrle/Herb, BDSG, § 1 Rn. 38.

[549] Vgl. Dammann in: Simitis, BDSG, § 1 Rn. 205.

Das bedeutet, dass dann, wenn der Auftraggeber, der die Outsourcingentscheidung verantwortlich trifft, in Deutschland seinen Hauptsitz hat oder eine Niederlassung in Deutschland unterhält, durch die Daten im Auftrag verarbeitet werden, deutsches Datenschutz(straf-)recht anzuwenden ist. Liegt hingegen der Sitz einer Niederlassung und der verantwortlichen Stelle als Auftraggeber in einem EU- oder EWR-Staat, dann ist das Recht dieses Landes anwendbar

Im Ergebnis findet bei grenzüberschreitenden Outsourcingvorhaben deutsches (Datenschutz-) Strafrecht in erheblichem Ausmaß Anwendung. Für Mitarbeiter ausländischer Unternehmen, die sich an Outsourcingvorhaben beteiligen, besteht daher das Risiko, sich als Teilnehmer an einer Geheimnisverletzung nach § 203 StGB, aber auch als Täter nach § 44 BDSG strafbar zu machen.

G. Gesetzgeberisches Tätigwerden

Die bisherigen Untersuchungen zeigen, dass das Outsourcing medizinischer Daten mit erheblichen Strafbarkeitsrisiken einhergeht. Auch beim Einsatz von Verschlüsselung, Anonymisierung oder Pseudonymisierung sowie Einbindung des privaten IT-Dienstleisters in die Organisation des Schweigepflichtigen ist ein möglicher Tatbestandsausschluss von der Beurteilung im Einzelfall abhängig. Hinzu kommt, dass eine datenschutzrechtliche Zulässigkeit dem Outsourcer keine Gewähr dafür gibt, dass er sich nicht nach § 203 StGB strafbar macht. Damit geht für den Outsourcer ein erhebliches Maß an Rechts- und Planungsunsicherheit einher.

Vor diesem Hintergrund erscheint de lege ferenda eine bundeseinheitliche Regelung wünschenswert. Dabei ist vom Ansatz her denkbar, dass § 203 StGB geändert wird, oder dass außerhalb des StGB für den Umgang mit medizinischen Daten eine sektorspezifische Regelung getroffen wird, die ein Outsourcing auch im Hinblick auf § 203 StGB ermöglicht. In beiden Fällen muss eine Regelung mit verfassungsrechtlichen und europarechtlichen Vorgaben vereinbar sein.

I. Gesetzgebungsrecht

Eine wünschenswerte bundeseinheitliche Regelung erfordert eine Gesetzgebungskompetenz des Bundes. Die Gesetzgebungskompetenzen werden im Grundgesetz zwischen Bund und Ländern verteilt. Nach Art. 70 Abs. 1 GG steht grundsätzlich den Ländern die Gesetzgebungskompetenz zu, soweit das Grundgesetz nicht dem Bund Gesetzgebungsbefugnisse verleiht. Art. 73 GG regelt abschließend und enumerativ die ausschließliche Gesetzgebungsbefugnis des Bundes. Außerhalb der Kompetenztitel in Art. 73 GG hat der Bund im Bereich der konkurrierenden Gesetzgebung unter den Voraussetzungen des Art. 72 GG das Recht zur Gesetzgebung.

Hinsichtlich einer sektorspezifischen, bundeseinheitlichen Regelung im Gesundheitswesen, die das Outsourcing medizinischer Daten mit zum Gegenstand hat, bestehen Bedenken hinsichtlich der Gesetzgebungsbefugnis. Die Problematik liegt darin, dass durch eine solche Regelung eine Vielzahl unterschiedlicher Materien betroffen wären, so dass eine eindeutige Zuordnung zu einem bundes- oder landesrechtlichen Kompetenztitel schwer erfolgen kann.

Sachlich müssten u.a. datenschutzrechtliche Regelungen getroffen werden. Schon dieser Bereich lässt sich als Querschnittsmaterie nicht allein dem Bund oder den Ländern zuordnen[550]. Soll dennoch eine bundeseinheitliche Regelung geschaffen werden, kann dies nur im Wege eines Staatsvertrages zwischen Bund und Ländern erfolgen[551]. Ob sich dies angesichts der unterschiedlichen angesprochenen Materien noch im Rahmen zulässiger bundesstaatlicher Kooperation bewegt, erscheint fraglich. Hier müssten eine Vielzahl eingreifender Regelungen, beispielsweise im Zivilrecht oder im Strafprozessrecht hinreichend bestimmt getroffen werden, die ansonsten unmittelbar vom Gesetzgeber getroffen werden würden. Dass dabei die Zustimmung der Parlamente erforderlich ist, lindert die Bedenken nur sehr eingeschränkt. Denn die bloße Zustimmung ist in keiner Weise ein Äquivalent zur Entscheidungsfindung in einem Gesetzgebungsverfahren. Wegen dieser Bedenken ist

[550] So sind weite Bereiche des Gesundheitswesens, darunter auch der Datenschutz im Gesundheitswesen, Ländersache; vgl. Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 223; vgl. auch Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, S. 156 ff.; Simitis, in: Simitis, BDSG, § 1 Rn. 1 ff.

[551] Vgl. den Vorschlag einer ärztlichen Kommunikationsordnung bei Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 212.

die Lösung einer sektorspezifischen Regelung außerhalb des Strafrechts nicht anzustreben.

Auch für eine Änderung des § 203 StGB benötigt der Bund die Gesetzgebungsbefugnis. Art. 74 Abs. 1 Nr. 1 GG ordnet das Strafrecht der konkurrierenden Gesetzgebung zu. Für die in Art. 72 Abs. 2 GG enumerativ aufgezählten Gesetzgebungsmaterien hat der Bund in diesem Bereich das Gesetzgebungsrecht, „wenn und soweit die Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet oder die Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse eine bundesgesetzliche Regelung erforderlich macht“. Die Voraussetzungen des Art. 72 Abs. 2 GG sind verfassungsgerichtlich eingeschränkt überprüfbar. Ein freier gesetzgeberischer Beurteilungsspielraum besteht nicht[552]. Da allerdings das Strafrecht nicht in Art. 72 Abs. 2 GG aufgeführt ist, ist die einschränkende Voraussetzung in Art. 72 Abs. 2 GG unerheblich und es bleibt bei der Zuständigkeit nach Art 72 Abs. 1 GG. Die notwendige Gesetzgebungsbefugnis liegt daher vor.

II. Verfassungsrechtliche und europarechtliche Anforderungen

Eine Änderung in § 203 StGB, die das Outsourcing medizinischer Daten erlaubt, muss verfassungsrechtlichen Anforderungen gerecht werden. Erforderlich ist, dass die Regelung dem Bestimmtheitsgebot genügt. Somit muss der Normanwender sich hinreichend klar erschließen können, wann das Outsourcing medizinischer Daten nach § 203 StGB zulässig ist. Dies kann dadurch erfolgen, dass in § 203 StGB selbst geregelt wird, unter welchen Voraussetzungen das Heranziehen privater IT-Dienstleistungsanbieter kein unbefugtes Offenbaren von Geheimnissen ist. Das Bestimmtheitsgebot schließt aber nicht aus, dass der Gesetzgeber für die Frage der strafrechtlichen Zulässigkeit mit einer Verweisungstechnik arbeitet. So ist denkbar, dass ein Outsourcing von einer behördlichen Genehmigung abhängig gemacht wird, oder auf die Zulässigkeit des Outsourcings nach datenschutzrechtlichen Vorschriften verwiesen wird.

[552] Vgl. Oeter, in: v. Mangoldt/Klein/Starck, Bonner Grundgesetz, Art. 72 Rn. 111, 115; Stettner, in: Dreier, Grundgesetz, Art. 72 Rn. 16, 17; Degenhart, in: Sachs, Grundgesetz, Art. 72 Rn. 15; Bothe, in: Alternativkommentar Grundgesetz, Art. 72 Rn. 15, von Münch/Kunig, Grundgesetzkommentar, Art. 72 Rn. 24, BVerfGE, 106, 62 (149).

Weiterhin muss eine Regelung in § 203 StGB mit dem Recht auf informationelle Selbstbestimmung vereinbar sein. Die Interessen, die für ein Heranziehen privater IT-Dienstleistungsunternehmen sprechen, müssen die Schutzinteressen des Einzelnen überwiegen, um Einschränkungen im strafrechtlichen Privatgeheimnisschutz zu rechtfertigen. Dies kann angenommen werden, wenn über das Outsourcing eine Stabilisierung und Sicherung der Leistungsfähigkeit des Outsourcers erreicht wird, ohne dass mit dem Heranziehen des Privaten eine unkontrollierte Preisgabe seiner Geheimnisse an weitere Personen zu befürchten ist.

Um dies zu erreichen muss eine Abschirmung der Daten sowie des Outsourcingverhältnisses sichergestellt sein, durch die wirksam der Zugriff von Personen außerhalb des Outsourcingverhältnisses verhindert werden kann. Weiterhin sollte strafprozessual die Beschlagnahmefreiheit bei allen Outsourcingbeteiligten sichergestellt werden. Schließlich müssen in jeder Verarbeitungsphase die Daten eindeutig als vom Betroffenen stammend identifiziert werden können. Eine Regelung durch den Gesetzgeber in § 203 StGB hat diese Leitlinien zu beachten.

Hinsichtlich europarechtlicher Vorgaben sind die Restriktionen in der Europäischen Datenschutzrichtlinie zu beachten. Dort wird für Gesundheitsdaten in Art. 8 Abs. 1 Europäische Datenschutzrichtlinie ein Verarbeitungsverbot statuiert. Ausnahmen sind in den Absätzen 2 und 3 aufgezählt. Daneben haben nach Abs. 4 die Mitgliedsstaaten die Möglichkeit, aus Gründen eines wichtigen öffentlichen Interesses Ausnahmen vorzusehen.

Fraglich erscheint aber, ob die Datenschutzrichtlinie für den Privatgeheimnisschutz nach § 203 StGB einschlägig ist. Hiergegen spricht, dass die Datenschutzrichtlinie die Verarbeitung personenbezogener Gesundheitsdaten regelt und nicht die Offenbarung von Geheimnissen. Darüber hinaus ist auch nach dem Sinn und Zweck ein strafrechtlicher Schutz nicht angesprochen. Vielmehr wird, wie der zehnte Erwägungsgrund der Datenschutzrichtlinie zeigt, die datenschutzrechtliche Sicherung des Rechts auf Privatsphäre bezweckt. Die Datenschutzrichtlinie schränkt daher den strafrechtlichen nationalen Gesetzgeber nicht ein.

H. Zusammenfassung

Nach der vorliegenden Untersuchung zum Outsourcing medizinischer Daten aus strafrechtlicher Sicht kann folgendes Gesamtergebnis festgehalten werden. Beim Outsourcing medizinischer Daten sind regelmäßig personenbezogene Informationen betroffen. Personenbezogene Information umfasst als Oberbegriff „Geheimnisse“ i.S.v. § 203 StGB sowie personenbezogene Daten im Sinne des Datenschutzrechts. Bei der Bestimmung des Personenbezuges ist es trotz der grundsätzlichen Parallelgeltung von Datenschutzrecht und § 203 StGB zulässig, auf Grundsätze aus dem Datenschutzrecht zurückzugreifen.

Für den Outsourcer medizinischer Daten droht eine Strafbarkeit nach § 203 StGB, wenn private IT-Dienstleistungsunternehmen vom schweigepflichtigen Outsourcer zur Erledigung von Aufgaben herangezogen werden und in Kontakt mit den Geheimnissen geraten. Daneben kann sich eine Strafbarkeit im Wege der Teilnahme an einer nach § 203 StGB strafbaren Geheimnisverletzung ergeben. Bei Sachverhalten mit Auslandsbezug kann es dabei zu einer Anwendung deutschen Strafrechts kommen, wenn die Teilnahmehandlung im Inland sich auf ein im Ausland erfolgendes Outsourcing bezieht oder die Teilnahmehandlung im Ausland sich auf ein im Inland erfolgendes Outsourcing bezieht. Bei § 85a SGB X und § 44 BDSG können sich ausländische Outsourcingpartner auch als Mittäter strafbar machen, da es sich bei diesen Delikten nicht um Sonderdelikte handelt.

Allerdings lässt sich durch eine entsprechende Gestaltung des Outsourcingvorhabens im Einzelfall, unabhängig davon, ob ein Schweigepflichtiger nach § 203 Abs. 1 oder Abs. 2 StGB betroffen ist, eine Strafbarkeit vermeiden. Ansatz ist dabei die Tatbestandsebene des § 203 StGB, nämlich das Merkmal „Geheimnis“ sowie das Merkmal „Offenbaren“. So kann einerseits durch eine wirksame Verschlüsselung ein „Geheimnis“ i.S.v. § 203 StGB entfallen. Andererseits besteht die Möglichkeit, Mitarbeiter des privaten externen Dienstleistungsunternehmens als Gehilfen in den Kreis der zum Wissen Berufenen zu integrieren. Hierzu muss der Dritte an die Funktion des Schweigepflichtigen so angebunden werden, dass aus objektiv-normativer Sicht von einer tatbestandlichen Verantwortungseinheit gesprochen werden kann. Dazu ist erforderlich, dass durch geeignete Sicherheitsvorkehrungen der innere Bereich zwischen Outsourcer und dem einzubindenden

Privaten vom Außenbereich wirksam abgeschirmt wird und sichergestellt wird, dass der Outsourcer das Gesamtgeschehen im Rahmen des Outsourcingvorhabens beherrscht und steuert. Regelungen aus dem Datenschutzbereich zu den Sorgfalts- bzw. Schutzmaßnahmen können dabei als Orientierungslinien für die strafrechtliche Beurteilung herangezogen werden.

Ist dies nach der Gestaltung im Einzelfall gewährleistet, dann liegt nach der hier vertretenen Auffassung kein „Offenbaren“ i.S.v. § 203 StGB vor. Hierdurch erfolgt, ohne eine Verletzung des Rechts auf informationelle Selbstbestimmung, eine sachgerechte Begrenzung des objektiven Tatbestandes des § 203 StGB, die den tatsächlichen Gegebenheiten einer arbeitsteiligen Aufgabenerledigung sowie den technischen Entwicklungen in der digitalen Informationsverarbeitung Rechnung trägt.

Auf der Ebene der Rechtswidrigkeit lässt sich der Gefahr einer Strafbarkeit nach § 203 StGB durch eine Einwilligung begegnen. Regelmäßig scheidet dabei die Möglichkeit einer konkludenten oder mutmaßlichen Einwilligung aus. Vielmehr hat eine Einwilligung ausdrücklich zu erfolgen. Für ihre Wirksamkeit ist erforderlich, dass der Betroffene die wesentlichen Informationen über das konkrete Vorgehen des Outsourcers erhält, damit er sich über Reichweite und Bedeutung seiner Einwilligung bewusst werden kann. Der Weg über eine ausdrückliche Einwilligung beim Outsourcing medizinischer Daten ist mit erheblichen Schwierigkeiten sowohl im tatsächlichen als auch im rechtlichen Bereich verbunden.

Außerhalb des Rechtfertigungsgrundes der Einwilligung bestehen für das Outsourcing von medizinischen Daten regelmäßig keine strafrechtlichen Erlaubnissätze. Dabei ist es nicht von vornherein ausgeschlossen, dass im allgemeinen Datenschutzrecht oder im Sozialrecht strafrechtliche Erlaubnissätze geregelt sind. Trotz der bestehenden Unterschiede der Rechtsgebiete kann im Einzelfall eine Norm derart auf § 203 StGB Bezug nehmen, dass ausdrücklich oder dem Sinn nach eine Durchbrechung des § 203 StGB beabsichtigt ist. Dies gilt grundsätzlich auch für Normen des Landesrechts. Allerdings stellt keine der untersuchten Normen des allgemeinen und sektorspezifischen Datenschutzrechts oder des Sozialrechts, die für ein Outsourcing herangezogen werden können, einen solchen Bezug her. Auch über die allgemeinen Rechtfertigungsgründe des Notstandes, der

Wahrnehmung berechtigter Interessen oder der Grundsätze über die Abwägung widerstreitender Interessen oder Pflichten wird das Outsourcing medizinischer Daten strafrechtlich regelmäßig nicht ermöglicht. Allenfalls in unvorhergesehenen Ausnahmesituationen ist eine Rechtfertigung nach § 34 StGB denkbar. Für den Regelfall des Outsourcings ist § 34 StGB nicht als Rechtfertigungsgrund tauglich.

Neben einer Strafbarkeit nach § 203 StGB kommt beim Outsourcing medizinischer Daten eine Strafbarkeit nach § 44 BDSG bzw. nach entsprechenden Vorschriften der Landesdatenschutzgesetze sowie eine Strafbarkeit nach § 85a SGB X in Betracht. Die Gefahr einer Strafbarkeit kann ausgeschlossen werden, wenn das Outsourcing datenschutzrechtlich bzw. sozialrechtlich zulässig ist. Neben der Möglichkeit einer Einwilligung, die nur ausdrücklich erfolgen kann, ist die Zulässigkeit eines Outsourcings medizinischer Daten über eine Ausgestaltung als Auftragsdatenverarbeitung erreichbar. Vorschriften zur Auftragsdatenverarbeitung existieren sowohl im Datenschutzrecht als auch im Sozialrecht. Diese Vorschriften ermöglichen, sofern nicht spezielle Vorschriften des sektorspezifischen Datenschutzrechts wie beispielsweise Art. 27 Bayerisches Krankenhausgesetz entgegenstehen, in bestimmten Grenzen ein Outsourcing medizinischer Daten unter Beteiligung privater IT-Dienstleistungsunternehmen. Die Normen der Auftragsdatenverarbeitung ermöglichen nicht eine selbständige und eigenverantwortliche Aufgabenerfüllung durch den Outsourcingnehmer im Sinne einer Funktionsübertragung. Vielmehr muss der Outsourcer nach einer Gesamtbetrachtung das Gesamtgeschehen erkennbar beherrschen und steuern. Die Aufgabe darf nicht durch den Auftraggeber insgesamt aus den Händen gegeben werden. Andere Vorschriften, die eine Funktionsübertragung beim Outsourcing medizinischer Daten ermöglichen würden, bestehen nicht.

Die straflose Möglichkeit des Outsourcings medizinischer Daten hängt von der Gestaltung im Einzelfall ab. Dies kann unter dem Aspekt der Rechtssicherheit und Rechtsklarheit beklagt werden. Wünschenswert ist eine bundeseinheitliche Regelung, die das Outsourcing strafrechtlich regelt. Unter den verschiedenen gesetzgeberischen Möglichkeiten ist eine Neuregelung des § 203 StGB zu favorisieren.

Abkürzungsverzeichnis

a.A.	anderer Ansicht
a.F.	alte Fassung
Abs.	Absatz
AG	Amtsgericht, Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
AMG	Arzneimittelgesetz
AO	Abgabenordnung
AP	Nachschlagewerk des Bundesarbeitsgerichts
ASCII	American Standard Code for Information Interchange
ASP	Application Service Providing
AT	Allgemeiner Teil
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BauGB	Baugesetzbuch
BayDSG	Bayerisches Datenschutzgesetz
BayObLG	Bayerisches Oberstes Landesgericht
BayVerfGH	Bayerischer Verfassungsgerichtshof
BayVGH	Bayerischer Verwaltungsgerichtshof
BB	Betriebs-Berater
BDI	Bundesverband der Deutschen Industrie
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfD	Bundesbeauftragte für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BRAO	Bundesrechtsanwaltsordnung

BSI	Bundesamt für die Sicherheit in der Informationsverarbeitung
BT	Besonderer Teil
BT-Drucksache	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
CR	Computer und Recht
DAR	Deutsches Autorecht
DSB	Der Datenschutzbeauftragte
DSG-EKD	Kirchengesetz über den Datenschutz in der Evangelischen Kirche Deutschlands
dtV	Deutscher Taschenbuch Verlag
DuD	Datenschutz und Datensicherheit
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaften
EGStGB	Einführungsgesetz zum Strafgesetzbuch
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
FS	Festschrift
GA	Goltdammer´s Archiv
GDSG	Gesundheitsdatenschutzgesetz
GG	Grundgesetz
HS	Halbsatz
ICD	International Classification of Diseases
IT	Informationstechnologie
JA	Juristische Arbeitsblätter
JR	Juristische Rundschau
Jura	Juristische Ausbildung
JuS	Juristische Schulung
KDO	Anordnung über den kirchlichen Datenschutz
KMR	Kleinknecht/Müller/Reitberger
LBerufsG	Landesberufsgericht
LG	Landesgericht

LK	Leipziger Kommentar
MBOÄ	Musterberufsordnung Ärzte
MDR	Monatsschrift für Deutsches Recht (Zeitschrift)
MDSTV	Mediendienstestaatsvertrag
MedR	Medizinrecht (Zeitschrift)
MMR	MultiMedia und Recht (Zeitschrift)
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	Neue Juristische Wochenschrift-Rechtsprechungsreport (Zeitschrift)
NK	Nomos Kommentar
NStZ	Neue Zeitschrift für Strafrecht
NStZ-RR	NStZ-Rechtsprechungsreport-Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NW	Nordrhein Westfalen
NZA	Neue Zeitschrift für Arbeitsrecht
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PKV	Private Krankenversicherung
RDV	Recht der Datenverarbeitung
S.	Seite
SGB	Sozialgesetzbuch
SGb	Sozialgerichtsbarkeit
SK	Systematischer Kommentar
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StV	Strafverteidiger
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VersR	Versicherungsrecht
VG	Verwaltungsgericht
Vorb.	Vorbemerkung
VPN	Virtual Private Network
wistra	Zeitschrift für Wirtschaft, Steuer und Strafrecht

ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

Im Übrigen folgen die Abkürzungen Kirchner, Hildebert/Butz, Cornelie, Abkürzungsverzeichnis der Rechtssprache, 5. Auflage, Berlin, 2003

Literaturverzeichnis

Abel, Ralf/Karpenstein, Ulrich
Verbesserung des öffentlichen Forderungsmanagements-
Möglichkeiten und Grenzen einer Einbeziehung privater Unternehmen, RDV 2005, S.157 – 163.

Albrecht, Hans-Jörg
Nomos Kommentar zum Strafgesetzbuch, Baden-Baden 1995,
zit.: Bearbeiter, in: Nomos Kommentar StGB .

Arens, Wolfgang
Gesellschaftsrecht, 2. Auflage, Bonn 2005.

Arzt, Gunther/Weber, Ulrich
Strafrecht Besonderer Teil, Bielefeld 2000,
zit.: Arzt/Weber, Strafrecht BT.

Ayasse, Horst
Die Grenzen des Datenschutzes in der privaten Personenversicherung, VersR 1987, S. 536 – 545.

Bachmann, Gregor
Mitbestimmung bei Umstrukturierung betrieblicher Sozialeinrichtungen, NZA 2002, S. 1130 – 1138.

Bäumler, Helmut/Breinlinger, Astrid/Schrader, Hans-Hermann
Datenschutz von A-Z, Neuwied Stand Februar 2004,
zit.: Bearbeiter, in: Bäumler/Breinlinger/Schrader, Datenschutz von A-Z.

Bake, Christian/Blobel, Bernd/Münch, Peter
Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen, 2. Auflage, Frechen 2004,
zit.: Bake, Datenschutz und Datensicherheit.

Baumann, Jürgen/Weber, Ulrich/Mitsch, Wolfgang
Strafrecht Allgemeiner Teil, 11. Auflage, Bielefeld 2003,
zit.: Baumann/Weber/Mitsch, Strafrecht AT.

Bayerischer Landesbeauftragter für den Datenschutz
20. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz, 2003,
zit.: Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz, 2003.

BDI/BITKOM
Zusätzliche Anstrengungen zur Einführung der Gesundheitskarte, MMR 2004, Heft 1, S. XX – XXI.

Berger Kurzen, Brigitte von Merzligen und Adelboden BE
E-Health und Datenschutz, Zürich 2004,

zit.: Berger Kurzen, E-Health und Datenschutz.

Bergmann, Michael
Grenzüberschreitender Datenschutz, Baden-Baden 1985,
zit.: Bergmann, Grenzüberschreitender Datenschutz.

Bergmann, Lutz/Möhrle, Roland/Herb, Armin
Datenschutzrecht, Handkommentar, Stuttgart Stand Dezember 2004,
zit.: Bergmann/Möhrle/Herb, BDSG.

Beutelspacher, Albrecht/Schwenk, Jörg/Wolfenstetter, Klaus-Dieter
Moderne Verfahren der Kryptographie, 5. Auflage, Wiesbaden 2004,
zit.: Beutelspacher/Schwenk/Wolfenstetter, Moderne Verfahren der Kryptographie.

Bieber, Helfried
Datenschutz und ärztliche Schweigepflicht, Aachen, 1995,
zit.: Bieber, Datenschutz und ärztliche Schweigepflicht.

Bizer, Johann
Gesundheitskarte, DuD 2004, S. 243 -243.

Borchert, Günter
Zur Unwirksamkeit von Schweigepflichtentbindungserklärungen in Versicherungsverträgen, NVersZ 2001, S. 1 – 4.

Braunschweig, Rainer/Geis, Ivo/Tolksdorf, Dieter/Hansen, Ilka
DACS – Data Archiving and Communication Services, MedR 2004,
S. 353 – 359.

Bräutigam, Peter
IT-Outsourcing, Berlin 2004,
zit.: Bräutigam, IT-Outsourcing.

Breuer, Hans
dtV-Atlas zur Informatik, München, 1995,
zit.: Breuer, dtV-Atlas zur Informatik.

Bruns, Wolfgang
Die Schweigepflicht der sozialen Dienste der Justiz, Frankfurt am Main 1996,
zit.: Bruns, Die Schweigepflicht der sozialen Dienste der Justiz.

BSI (Bundesamt für Sicherheit in der Informationsverarbeitung)
Chipkarten im Gesundheitswesen - Schriftenreihe zur IT-Sicherheit, Köln, 1995,
zit.: BSI, Chipkarten im Gesundheitswesen.

Büllesbach, Alfred/Rieß, Joachim
Outsourcing in der öffentlichen Verwaltung, NVwZ 1995, S. 444 – 449.

Czychowski, Christian/ Bröcker, Klaus Tim
ASP- Ein Auslaufmodell für das Urheberrecht, MMR 2002, S. 81 – 84.

Dessauer, Johannes
Kosteneinsparung im Krankenhaus; Ist die Ausgliederung hierzu der richtige Weg? Juristische Probleme, insbesondere Haftungsfragen, MedR 1993, S. 379 – 386.

Deutsch, Erwin
Das Organisationsverschulden des Krankenhausträgers, NJW 2000, S. 1745 – 1749.

Deutsch, Erwin/Spickhoff, Andreas
Medizinrecht, 5. Auflage, Berlin 2003,
zit.: Deutsch/Spickhoff, Medizinrecht.

Diering, Björn/Timme, Hinnerk/Waschull, Dirk
Sozialgesetzbuch X, Baden-Baden 2004,
zit.: Bearbeiter in: Diering/Timme/Waschull, Sozialgesetzbuch X.

Dierks, Christian
Schweigepflicht und Datenschutz in Gesundheitswesen und medizinischer Forschung, München 1992,
zit.: Dierks, Schweigepflicht und Datenschutz in Gesundheitswesen und medizinischer Forschung.

Dieterich, Thomas/Müller-Glöge, Rudi/Preis, Ulrich/Schaub, Günter
Erfurter Kommentar zum Arbeitsrecht, 8. Auflage, München 2007,
zit.: Bearbeiter, in: Erfurter Kommentar zum Arbeitsrecht.

Dolderer, Günter/ Garrel, Gerd von /Müthlein, Thomas/Schlumberger, Peter
Die Auftragsdatenverarbeitung im neuen BDSG, RDV 2001, S. 223 – 232.

Dortants, Bernd W./Hansemann, Stephan von
Die Auslagerung von „Aufgaben“ durch Krankenkassen und ihre Verbände auf Dritte, NZS 1999, S. 542 – 546.

Duhr, Elisabeth/Naujok, Helga/Danker, Birgit/Seifert, Evelyn
Neues Datenschutzrecht für die Wirtschaft, DuD 2003, S. 5 – 28.

Dreier, Horst
Grundgesetz: Kommentar, Band 1, 2. Auflage, Tübingen 2004,
zit.: Bearbeiter, in: Dreier, Grundgesetz.

Ehmann, Eugen
- Strafbare Fernwartung in der Arztpraxis, CR 1991, S. 293 – 296.

- Anmerkung zu OLG Düsseldorf: Externe Archivierung, CR 1997, S. 538 – 539.

Ehmann, Eugen/Helfrich Marcus
EG Datenschutzrichtlinie Kurzkommentar, Köln 1999,
zit.: Ehmann/Helfrich, EG Datenschutzrichtlinie.

Eichelbrönner, Nicolas
Die Grenzen der Schweigepflicht des Arztes und seiner berufsmäßig tätigen Gehilfen nach § 203 StGB im Hinblick auf die Verhütung und Aufklärung von Straftaten, Frankfurt am Main 2001,
zit.: Eichelbrönner, Die Grenzen der Schweigepflicht des Arztes.

Erman, Walter/Westermann, Harm Peter/Aderhold, Lutz
Bürgerliches Gesetzbuch, Band 1, 11. Auflage, Münster 2004,
zit.: Erman, BGB.

Ernst, Werner/Zinkahn, Willy/Bielenberg, Walter
Baugesetzbuch, Band 2, München Stand: Januar 2005,
zit.: Bearbeiter, in: Ernst/Zinkahn/Bielenberg, BauGB

Eser, Albin
Wahrnehmung berechtigter Interessen als allgemeiner Rechtfertigungsgrund, Bad Homburg 1969,
zit.: Eser, Wahrnehmung berechtigter Interessen.

Evers, Jürgen/Kiene, Lorenz
Datenschutzrechtliche Folgen der Ausgliederung von Dienstleistungen, DuD, 2003, S. 341 – 344.

Fischer, Till
Juristische Anforderungen an das Bauen und den Brandschutz im Bestand, VIII. Baurecht & Brandschutz Symposium, Frankfurt am Main 11. Februar 2004,
zit.: Fischer, Juristische Anforderungen an das Bauen und den Brandschutz im Bestand.

Frommann, Matthias/ Mörseberger, Thomas/ Schellhorn, Walter
Sozialdatenschutz, Frankfurt am Main 1985,.
zit.: Bearbeiter, in: Frommann/Mörseberger/Schellhorn, Sozialdatenschutz

Geis, Ivo/Helfrich, Marcus
Datenschutzrecht, München 2003,
zit.: Geis/Helfrich, Datenschutzrecht.

Geiss, Gerhard
Premiere im Gesundheitswesen- Kassenverbände gründen GmbH für EDV- Dienste, Die Ersatzkasse 1996, S. 294 – 296.

Gummert, Hans/Riegger, Bodo/Weipert, Lutz
Münchener Handbuch des Gesellschaftsrechts, Band 1, 2. Auflage, München 2004,
zit.: Bearbeiter, in: Gummert/Riegger/Weipert, Münchener Handbuch des Gesellschaftsrechts.

Giese, Dieter/Krahmer, Utz
Sozialgesetzbuch I und X, Kommentar, 2. Auflage, Köln 2004,
zit.: Giese/Krahmer, Sozialgesetzbuch.

Gössel, Karl Heinz/Dölling, Dieter
Strafrecht Besonderer Teil 1, 2. Auflage, Heidelberg 2004,
zit.: Gössel/Dölling, Strafrecht BT 1.

Gola, Peter/Schomerus, Rudolf
BDSG Bundesdatenschutzgesetz, 8. Auflage, München 2005,
zit.: Gola/Schomerus, BDSG

Goll, Eberhard
Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB, Tübingen 1980
zit.: Goll, Offenbarungsbefugnisse im Rahmen des § 203 Abs. 2 StGB.

Hartmann, Thies Christian
Outsourcing in der Sozialverwaltung und Sozialdatenschutz, Baden-Baden 2002,
zit.: Hartmann, Outsourcing in der Sozialverwaltung und Sozialdaten-schutz.

Hauck, Karl/Haines, Hartmut
Sozialgesetzbuch, Berlin Stand Dezember 2007,
zit.: Bearbeiter, in: Hauck/Haines, Sozialgesetzbuch.

Heintschel-Heinegg,Bernd/Stöckel, Heinz
KMR Kommentar zur Strafprozessordnung, Neuwied 2007,
zit.: Bearbeiter, in: KMR StPO.

Heinzelmann, Dirk-Michael
Die Datenübermittlung, Tübingen 1991,
zit.: Heinzelmann, Die Datenübermittlung.

Henke, Klaus-Dirk/Berhanu, Samuel/Mackenthun, Birgit
Die Zukunft der Gemeinnützigkeit von Krankenhäusern unter besonderer Berücksichtigung freigemeinnütziger Krankenhäuser, Berliner Zentrum Public Health, Berlin 2004,
zit.: Henke/Berhanu/Mackenthun, Die Zukunft der Gemeinnützigkeit von Krankenhäusern.

Hermeler, Angelika-Elisabeth
Rechtliche Rahmenbedingungen der Telemedizin, München 2000,
zit.: Hermeler, Rechtliche Rahmenbedingungen.

Heyers, Johannes/Heyers, Josef
Arzthaftung - Schutz von digitalen Patientendaten, MDR 2001, S. 1209 – 1216.

Hilgendorf, Eric

- Strafrechtliche Produzentenhaftung in der „Risikogesellschaft“, Berlin 1993,
  zit.: Hilgendorf, Strafrechtliche Produzentenhaftung in der „Risikogesellschaft“.

- Zur Lehre vom „Erfolg in seiner konkreten Gestalt“, GA 1995, S. 515 – 534.

- Grundfälle zum Computerstrafrecht, JuS 1996, S. 890 – 894; S. 1082 – 1084.

- Strafrechtliche Probleme beim Outsourcing von Versicherungsdaten, S. 81 – 118, in: Hilgendorf, Eric, Informationsstrafrecht und Rechtsinformatik, Das Strafrecht vor neuen Herausforderungen, Berlin 2004,
  zit.: Hilgendorf, in: Hilgendorf, Informationsstrafrecht und Rechtsinformatik

- Wozu brauchen wir die „objektive Zurechnung“? Skeptische Überlegun gen am Beispiel der strafrechtlichen Produkthaftung, S. 33 – 48, in: Hein rich, Bernd, Festschrift für Ulrich Weber zum 70. Geburtstag, Bielefeld 2004,
  zit.: Hilgendorf, in: FS Weber.

Hilgendorf, Eric/Frank, Thomas/Valerius, Brian
Computer- und Internetstrafrecht, Berlin 2005,
zit.: Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht.

Hoenike, Mark/Hülsdunk, Lutz
Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwilligung?, MMR 2004, S. 788 – 792.

Hoeren, Thomas
Banken und Outsourcing, DuD 2002, S. 736 – 740.

Hoeren, Thomas/Sieber, Ulrich
Handbuch Multimedia Recht, München Stand: Dezember 2006,
zit.: Bearbeiter, in: Hoeren/Sieber, Handbuch Multimedia Recht.

Holznagel, Bernd
Recht der IT-Sicherheit, München 2003,
zit.: Holznagel, Recht der IT-Sicherheit.

Hornung, Gerrit
Datenschutz für Chipkarten, DuD 2004, S. 15 – 20.

Iwanski, Patrizia
Datenschutzrechtliche Probleme von Chipkarten am Beispiel der geplanten Patientenkarte unter besonderer Berücksichtigung der europäischen Entwicklung, Berlin 1999,
zit.: Iwanski, Datenschutzrechtliche Probleme von Chipkarten.

Jähnke, Burkhard/Laufhütte, Heinrich Wilhelm /Odersky Walter
Strafgesetzbuch Leipziger Kommentar, 11. Auflage, Berlin 2000,
zit.: Bearbeiter, in: Leipziger Kommentar StGB.

Jarass, Hans/Pieroth, Bodo
Grundgesetz für die Bundesrepublik Deutschland Kommentar, 7. Auflage, München 2004,
zit.: Jarass/Pieroth, Grundgesetz.

Jescheck, Hans-Heinrich/Weigend, Thomas
Lehrbuch des Strafrechts, Allgemeiner Teil, 5. Auflage, Berlin 1996,
zit.: Jescheck/Weigend, Strafrecht AT.

Joecks, Wolfgang/Miebach, Klaus
Münchener Kommentar zum Strafgesetzbuch, Band 3, Mücnhen 2003,
zit.: Bearbeiter, in: Münchener Kommentar StGB.

Kessler, Clemens
Outsourcing von Sozialdaten zur Kostenreduktion, DuD 2004, S. 41 – 43.

Kiethe, Kurt
Strafrechtlicher Anlegerschutz durch § 400 I Nr. 1 AktG, NStZ 2004, S. 73 – 76.

Kilian, Wolfgang
Rechtliche Aspekte der digitalen medizinischen Archivierung von Röntgenunterlagen, NJW 1987, S. 695 – 698.

Kilian, Wolfgang/Scheja, Gregor
Freier Datenfluss im Allfinanzkonzern, RdV 2002, S. 177 – 188.

Kilian, Wolfgang/Heussen, Benno
Computerrechts-Handbuch, München Stand Oktober 2006,
zit.: Bearbeiter, in: Kilian/Heussen, Computerrechts-Handbuch.

Kindhäuser, **Urs**
Strafrecht, Allgemeiner Teil, Baden-Baden 2005,
zit.: Kindhäuser, Strafrecht AT.

Klinger, Roland/Kunkel, Peter-Christian
Sozialdatenschutz in der Praxis, Stuttgart 1990,
zit.: Klinger/Kunkel, Sozialdatenschutz in der Praxis.

Klöcker, Irene/Meister, Jörg
Datenschutz im Krankenhaus, Düsseldorf 2001,
zit.: Klöcker/Meister, Datenschutz im Krankenhaus.

Köpke, Jan
Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für Private Krankenversicherer, insbesondere bei der innerorganisatorischen Geheimnisweitergabe, Tübingen, 2003,

zit.: Köpke, Die Bedeutung des § 203 Abs. 1 Nr. 6 StGB für Private Krankenversicherungen.

Körner-Dammann, Marita
Weitergabe von Patientendaten an ärztliche Verrechnungsstellen, NJW 1992, S. 729 – 731.

Krahmer, Utz/Stähler, Thomas P.
Die gemeinsame Datenverarbeitung und- nutzung durch Pflege- und Krankenkassen nach dem neu gefassten § 96 SGB XI, NZS 2003, S. 193 – 196.

Kramer, Philipp/Hermann, Michael
Auftragsdatenverarbeitung- zur Reichweite der Privilegierung des § 11 BDSG, CR 2003, S. 938 – 941.

Krauskopf, Dieter/Baier, Gerhard
Soziale Krankenversicherung- Pflegeversicherung, München Stand 2005,
zit.: Bearbeiter, in: Krauskopf, Soziale Krankenversicherung- Pflegeversicherung.

Kreuzer, Arthur
Die Schweigepflicht von Krankenhausärzten gegenüber Aufsichtsbehörden, NJW 1975, S. 2232 – 2236.

Kühl, Kristian
Strafrecht Allgemeiner Teil, 5. Auflage, München 2002,
zit.: Kühl, Strafrecht AT.

Kühne, Hans-Heiner
Berufsrecht für Psychologen, Baden-Baden 1987,
zit.: Kühne, Berufsrecht für Psychologen.

Kupjetz, Jörg
Moderne Produktions- und Absatzformen im Spiegel strafrechtlicher Verantwortlichkeit, Heidelberg 2002,
zit.: Kupjetz, Moderne Produktions- und Absatzformen.

Kußmann, Niels
Lexikon der Kommunikations- und Informationstechnik, 3. Auflage, Heidelberg 2001,
zit.: Kußmann, Lexikon der Kommunikations- und Informationstechnik.

Lackner, Karl/Kühl, Kristian
Strafgesetzbuch mit Erläuterungen, 26. Auflage, München 2007,
zit.: Lackner/Kühl, StGB.

Lang, Franziska
Das Recht auf informationelle Selbstbestimmung des Patienten und die ärztliche Schweigepflicht in der gesetzlichen Krankenversicherung, Baden-Baden 1997,
zit.: Lang, Das Recht auf informationelle Selbstbestimmung.

Langkeit, Jochen
Umfang und Grenzen der ärztlichen Schweigepflicht gemäß § 203 Abs. 1 Nr. 1 StGB, NStZ 1994, S. 6 – 9.

Laufhütte, Heinrich Wilhelm/ Rissing-van Saan, Ruth/Tiedemann, Klaus
Strafgesetzbuch Leipziger Kommentar, 12. Auflage, Band 3, 2006,
zit.: Bearbeiter, in: Leipziger Kommentar StGB.

Laufs, Adolf/ Uhlenbruck, Wilhelm
Handbuch des Arztrechts, 3. Auflage, München 2002,
zit.: Bearbeiter, in: Laufs/Uhlenbruck, Handbuch des Arztrechts.

Lehmann, Thomas M./Mayer zu Bexten, Erdmuthe
Handbuch der Medizinischen Informatik, München 2002,
zit.: Lehmann/Mayer, Handbuch der Medizinischen Informatik.

Lemke, Michael/Julius, Karl-Peter/Krehl, Christoph/Rautenberg, Erardo Cristofero/Temming, Dieter
Heidelberger Kommentar zur Strafprozessordnung, 3. Auflage, Heidelberg 2001,
zit.: Bearbeiter, in: Heidelberger Kommentar StPO.

Lensdorf, Lars/Steger, Udo
Auslagerung von IT-Leistungen auf Public Private Partnerships, CR 2005, S. 161 – 169.

Lewinski, Kai von
Schweigepflicht von Arzt und Apotheker, Datenschutzrecht und aufsichtsrechtliche Kontrolle, MedR 2004, S. 95 – 104.

Lilie, Barbara
Medizinische Datenverarbeitung, Schweigepflicht und Persönlichkeitsrecht im Deutschen und Amerikanischen Recht, Göttingen 1980,
zit.: Lilie, Medizinische Datenverarbeitung, Schweigepflicht und Persönlichkeitsrecht.

Löwe, Ewald/Rosenberg, Werner/Rieß, Peter
Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 24. Auflage, Band 1, Berlin 1988,
zit.: Bearbeiter, in: LR StPO.

Luttenberger, Norbert/Reischl, Joachim/Schröder, Markus/Stürzebecher, Claus S.
Datenschutz in der pharmakogenetischen Forschung- eine Fallstudie, DuD 2004, S. 356 – 363.

Mahlein, Irene A. I.
Outsourcing im öffentlichen Krankenhaus, Das Krankenhaus, S. 104 – 108.

Mand, Elmar
Datenschutz in Medizinnetzen, MedR 2003, S. 393 – 400.

Maunz, Theodor/Dürig, Günter
Grundgesetz, 8. Auflage, München Stand 2007,
zit.: Bearbeiter, in: Maunz/Dürig, Grundgesetz.

Maurach, Reinhart/ Schroeder, Friedrich-Christian/ Maiwald, Manfred
Strafrecht Besonderer Teil, Teilband 1, 9. Auflage, Heidelberg 2003,
zit.: Maurach/Schroeder/Maiwald, Strafrecht BT.

Maurach, Reinhart/Zipf, Heinz/Gössel, Karl Heinz/Schroeder, Friedrich-Christian
Strafrecht Allgemeiner Teil, 8. Auflage, Heidelberg 1992,
zit.: Maurach/Zipf, Strafrecht AT.

Maurer, Hartmut
Allgemeines Verwaltungsrecht, 16. Auflage, München 2006,
zit.: Maurer, Allgemeines Verwaltungsrecht.

Maydell, Bernd Baron von/ Ruland, Franz
Sozialrechtshandbuch, 3. Auflage, Baden-Baden 2003,
zit.: Maydell/Ruland, Sozialrechtshandbuch.

Meier, André
Der rechtliche Schutz patientenbezogener Gesundheitsdaten, Karlsruhe 2003,
zit.: Meier, Der rechtliche Schutz patientenbezogener Gesundheitsdaten.

Meyer, Regina/Brocks, Holger/Nordmann, Christine
Gericht kontra Datenschutz: Kein strafrechtlicher Schutz mehr für Fahrzeughalterdaten?, RDV 2000, S. 11 – 14.

Meyer-Goßner, Lutz
Strafprozessordnung, 50. Auflage, München 2007,
zit.: Meyer-Goßner, StPO.

Mrozynski, Peter
SGB I Sozialgesetzbuch, 3. Auflage, München 2003,
zit.: Mrozynski, SGB I.

Münch, Ingo von/Kunig, Philip
Grundgesetzkommentar, 5. Auflage, München 2003,
zit.: Münch/Kunig, Grundgesetzkommentar.

Münch, Peter
Technisch-organisatorischer Datenschutz, 2. Auflage, Frechen 2005,
zit.: Münch, Technisch-organisatorischer Datenschutz.

Müthlein, Thomas/Heck, Johannes
Outsourcing und Datenschutz, 2. Auflage, Frechen 1997,
zit.: Müthlein/Heck, Outsourcing und Datenschutz.

Niedermair, Harald
Verletzung von Privatgeheimnissen im Interesse des Patienten? Aus der Rechtsprechung zur ärztlichen Schweigepflicht, S. 363 – 288, in: Roxin, Claus/Schroth, Ulrich**,** Medizinstrafrecht, 2. Auflage, Stuttgart 2001,
zit.: Niedermair, in: Roxin/Schroth, Medizinstrafrecht.

Niesel, Klaus
Kassler Kommentar Sozialversicherungsrecht, München Stand September 2007,
zit.: Bearbeiter, in: Kassler Kommentar Sozialversicherungsrecht.

Otto, Harro
Strafrechtliche Konsequenzen aus der Ermöglichung der Kenntnisnahme von Bankgeheimnissen, wistra 1999, S. 201 – 206.

Palandt, Otto
Bürgerliches Gesetzbuch, 67. Auflage, München 2007,
zit.: Palandt, BGB.

Pfeifer, Gerd
Karlsruher Kommentar zur Strafprozessordnung, 5. Auflage, München 2003,
zit.: Bearbeiter, in: Karlsruher Kommentar StPO.

Pickel, Harald
Organisatorische Vorkehrungen zum Schutz der Sozialdaten und besondere Datenverarbeitungsarten, SGb 2000, S. 198 – 202.

Podlech, Adalbert
Der Informationshaushalt der Krankenkassen: datenschutzrechtliche Aspekte, Baden-Baden 1995,
zit.: Podlech, Der Informationshaushalt der Krankenkassen.

Proeller, Isabella
Auslagerung in der hoheitlichen Verwaltung, Bern 2002,
zit.: Proeller, Auslagerung in der hoheitlichen Verwaltung.

Pschyrembel, Willibald
Klinisches Wörterbuch, 261. Auflage, Berlin 2007,
zit.: Pschyrembel, Klinisches Wörterbuch.

Püschel, Jan
Informationsfreiheit bei Public Private Partnership, Der Fall Toll Collect, DuD 2004, S. 290 – 296.

Rasmussen, Heike
Der Schutz medizinischer Daten im Sozialdatenschutz, NZS 1998, S. 67 – 73.

Ratzel, Rudolf/Lippert, Hans-Dieter
Kommentar zur Musterberufsordnung der deutschen Ärzte, 3. Auflage, Berlin 2002,

zit.: Ratzel/Lippert, MBOÄ.

Rebmann, Kurt/Säcker, Franz Jürgen/Heinrichs, Helmut/Krüger, Wolfgang/Schlichting, Gerhard/Sonnenberger, Hans Jürgen/Schwab, Dieter/Westermann, Harm Peter/Ulmer, Peter/Quack, Friedrich
Münchner Kommentar zum Bürgerlichen Gesetzbuch, Band 4, 4. Auflage, München 2005,
zit.: Bearbeiter, in: Münchner Kommentar BGB.

Redeker, Helmut
Handbuch der IT-Verträge, Köln Stand Oktober 2007,
zit.: Bearbeiter, in: Redeker, Handbuch der IT-Verträge.

Rein, Detlev
Die Bedeutung der §§ 203 ff StGB für die private Personenversicherung, VersR 1976, S. 117 – 124.

Rieger, Hans-Jürgen
Lexikon des Arztrechts, Berlin 1984,
zit.: Rieger, Lexikon des Arztrechts.

Rogall, Klaus
Die Verletzung von Privatgeheimnissen (§ 203 StGB), NStZ 1983, S. 1 – 9.

Rossnagel, Alexander
Handbuch des Datenschutzrechts, München 2003,
zit.: Rossnagel, Handbuch des Datenschutzrechts.

Roxin, Claus
- Unterlassen, Vorsatz und Fahrlässigkeit, Versuch und Teilnahme im neuen Strafgesetzbuch, JuS 1973, S. 197 – 202.

- Strafrecht, Allgemeiner Teil, Band 1, 3. Auflage, München 1997,
  zit.: Roxin, Strafrecht AT 1.

Rudolphi, Hans-Joachim/Frisch, Wolfgang/Paeffgen, Hans-Ullrich/ Rogall, Klaus/ Schlüchter, Ellen/Wolter, Jürgen
Systematischer Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz, München Stand September 2007,
zit.: Bearbeiter, in: Systematischer Kommentar StPO.

Sachs, Michael/Battis, Ulrich
Grundgesetz, 3. Auflage, München 2003,
zit.: Bearbeiter, in: Sachs, Grundgesetz.

Saeltzer, Gerhard
Sind diese Daten personenbezogen oder nicht?, DuD 2004, S. 218 – 227.

Samson, Erich
Erfolgszurechnung und Risiko- Kritische Anfragen an die Lehre von der

objektiven Zurechnung, S. 587 - 598, in: Prittwitz, Cornelius, Festschrift für Klaus Lüderssen zum 70. Geburtstag, Baden- Baden 2002,
zit.: Samson, in: FS Lüderssen.

Schäfer, Peter
Aerztliche Schweigepflicht und Elektronische Datenverarbeitung, Zürich 1978,
zit.: Schäfer, Aerztliche Schweigepflicht und Elektronische Datenverarbeitung.

Schaffland, Hans-Jürgen/Wiltfang, Noeme
BDSG Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Berlin Stand Januar 2005,
zit.: Schaffland/Wildfang, BDSG.

Schlund, Gerhard
- Zu Fragen der ärztlichen Schweigepflicht, JR 1977, S. 265 – 269.

- Grundsätze ärztlicher Verschwiegenheit im Rahmen der Verkehrssicherheit, DAR 1995, S. 1 – 5.

Schmidt, Klaus K.
Ärztliche Schweigepflicht und Sozialdatenschutz, Göttingen 1985,
zit.: Schmidt, Ärztliche Schweigepflicht und Sozialdatenschutz.

Schmitz, Roland
- Verletzung von (Privat)geheimnissen - Der Tatbestand des § 203 StGB, JA 1996, S. 772 – 777.

- Verletzung von (Privat)geheimnissen - Probleme der Rechtfertigung, JA 1996, S. 949 – 955.

Schneider, Jochen
Handbuch des EDV-Rechts, 3. Auflage, Köln 2003,
zit.: Schneider, Handbuch des EDV-Rechts.

Schnitzler, Jörg
Das Recht der Heilberufe, Baden-Baden 2004,
zit.: Schnitzler, Das Recht der Heilberufe.

Schnorr, Stefan/ Wissing, Volker
Auf dem Weg zum gläsernen Patienten?, ZRP 2001, S. 487 – 488.

Schoch, Friedrich
- Nachbarschutz im öffentlichen Baurecht, Jura 2004, S. 317 – 325.

- Der unbestimmte Rechtsbegriff im Verwaltungsrecht, Jura 2004, S. 612 – 618.

Schönke, Adolf/Schröder, Horst
Strafgesetzbuch, 27. Auflage, München 2006,
zit.: Bearbeiter, in: Schönke/Schröder, StGB.

Schott, Wolfgang
Die Geheimnispflicht der Sozialversicherungsträger nach dem Sozialgesetzbuch I und X, Frankfurt 1991,
zit.: Schott, Die Geheimnispflicht der Sozialversicherungsträger.

Schrödter, Hans/Breuer, Rüdiger
Baugesetzbuch, 7. Auflage, München 2005,
zit.: Bearbeiter, in: Schrödter, BauGB.

Schulte, Jörg/Wehrmann, Rüdiger/Wellbrock, Rita
Das Datenschutzkonzept des Kompetenznetzes Parkinson, DuD 2002, S. 605 – 610.

Schulz, Lorenz
Genetische Datenbanken und Selbstbestimmung, DuD 2001, S.12 – 19.

Seelos, Hans-Jürgen
- Wörterbuch der medizinischen Informatik, Berlin, 1990
  zit.: Seelos, Wörterbuch der medizinischen Informatik.

- Patientendaten: Terminologische und informationsrechtliche Aspekte, DuD 1993, S. 433 – 437.

Simitis, Spiros
Kommentar zum Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden 2006
zit.: Bearbeiter, in: Simitis, BDSG.

Sinz, Elmar/Plaha, Markus/Ulbrich, Achim vom Ende
Datenschutz und Datensicherheit in einem landesweiten Data-Warehouse-System für das Hochschulwesen, Bamberg 2002,
zit.: Sinz, Datenschutz und Datensicherheit in einem landesweiten Data-Warehouse- System für das Hochschulwesen.

Söbbing, Thomas
Handbuch IT-Outsorcing, 3. Auflage, Heidelberg 2006,
Zit.: Bearbeiter, in: Söbbing, IT-Outsourcing.

Soergel, Hans Theodor
Bürgerliches Gesetzbuch, Band 4/1, Berlin 2000,
zit. Soergel, BGB.

Sokol, Betina
- Der Fall „de CODE“, DuD 2001, S. 5 – 11.

- Gesundheitsdatenbanken und Betroffenenrechte: Das isländische Beispiel, NJW 2002, S. 1767 – 1769.

Staudinger, Julius von/Brändl, Franz/Weber, Wilhelm/Werner, Alfred/Kaduk, Hubert/Kiefersauer, Fritz/Nipperdey, Hans Carl/Schäfer, Karl/Berg, Hans
J.v. Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetzen und Nebengesetzen, 11. Auflage, Berlin 2006,
zit.: Staudinger, BGB.

Steding, Ralf/Meyer, Guido
Outsourcing von Bankdienstleistungen: Bank- und datenschutzrechtliche Probleme der Aufgabenverlagerung von Kreditinstituten auf Tochtergesellschaften und sonstige Dritte, BB 2001, S. 1693 – 1701.

Stern, Klaus
Das Staatsrecht der Bundesrepublik Deutschland, Band 3, München 1980,
zit.: Stern, Staatsrecht.

Stober, Rolf
Private Sicherheitsdienste als Dienstleister für die öffentliche Sicherheit?, ZRP 2001, S. 260 – 266.

Stößel, Frank Volker
Outsourcing in der öffentlichen Verwaltung, Frankfurt 1998,
zit.: Stößel, Outsourcing in der öffentlichen Verwaltung.

Sutschet, **Holger**
Auftragsdatenverarbeitung und Funktionsübertragung, RDV 2004, S. 97 – 104.

Taraschka, Klaus
„Auslandsübermittlung" personenbezogener Daten im Internet, CR 2004, S. 280 – 286.

Taupitz, Jochen
Integrative Gesundheitszentren: neue Formen interprofessioneller ärztlicher Zusammenarbeit, MedR 1993, S. 367 – 378.

Tinnefeld, Marie-Theres/Ehmann, Eugen/Gerling, Rainer
Einführung in das Datenschutzrecht, 4. Auflage, München 2005,
zit.: Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht.

Tröndle, Herbert/Fischer, Klaus
Strafgesetzbuch und Nebengesetze, 55. Auflage, München 2007,
zit.: Tröndle/Fischer, StGB.

Umbach, Dieter/Clemens, Thomas
Grundgesetz, Heidelberg 2002,
zit.: Umbach/Clemens, Grundgesetz.

Ulsenheimer, Klaus
Arztstrafrecht in der Praxis, 3. Auflage, Heidelberg 2003,
zit.: Ulsenheimer, Arztstrafrecht in der Praxis.

Ulsenheimer, Klaus/Heinemann, Nicola
Rechtliche Aspekte der Telemedizin-Grenzen der Telemedizin, MedR 1999, S. 197 – 203.

Vahle, Jürgen
Medizinische Daten und Datenschutz, DuD 1991, S. 614 – 619.

Vetter, Reinhard
Chancen und Risiken zentralistischer Patientendatenbestände- zentraler Datenpool der Krankenversicherung, Elektronischer Patientenpass und zentraler Rechner, DuD 2003, S. 39 – 43.

Vogel, Otto
Zum strafrechtlichen Schutz des Sozialgeheimnis, Münster 1994,
zit.: Vogel, Zum strafrechtlichen Schutz des Sozialgeheimnis.

Waltermann, Raimund
Sozialrecht, 4. Auflage, Heidelberg 2004,
zit.: Waltermann, Sozialrecht.

Wannagat, Georg/Eichenhofer, Eberhard
Sozialgesetzbuch, Kommentar zum Recht des Sozialgesetzbuchs, SGB X 1-3, Köln Stand Mai 2002,
zit.: Bearbeiter, in: Wannagat, Sozialgesetzbuch.

Weichert, Thilo
- Datenschutz- Audit und Gütesiegel im Medizinbereich, MedR 2003, S. 674 – 681.

- Die Krux mit der ärztlichen Schweigepflichtsentbindung für Versicherungen, NJW 2004, S. 1695 – 1700.

- Die elektronische Gesundheitskarte, DuD 2004, S. 391 – 403.

Wellbrock, Rita
Datenschutzrechtliche Aspekte des Aufbaus von Biobanken für Forschungszwecke, MedR 2003, S. 77 – 82.

Welzel, Hans
Studien zum System des Strafrechts, ZStW 58, S. 491 – 566.

Wessels, Johannes/Beulke, Werner
Strafrecht Allgemeiner Teil, 37. Auflage, Heidelberg 2007,
zit.: Wessels/Beulke, Strafrecht AT.

Westerhold, Margot Gräfin von /Berger, Konrad
Der Application Service Provider und das neue Schuldrecht, CR 2002, S. 81-88.

Wilde, Christian Peter/Ehmann, Eugen/Niese, Marcus /Knoblauch, Anton
Bayerisches Datenschutzgesetz, München Stand November 2006,
zit.: Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz.

Wilmes, Caroline/Dietl, Helmut/Velden, Remco van der
Die strategische Ressource „data warehouse“, Wiesbaden 2004,
zit.: Wilmes, Die strategische Ressource „data warehouese“.

Wissmann, Martin
Telekommunikationsrecht, 2. Auflage, Frankfurt 2006,
Zit.: Bearbeiter, in: Wissmann, Telekommunikationsrecht.

Wolf, Christian
Externer Honorareinzug und ärztliche Schweigepflicht, Hamburg 2003,
zit.: Wolf, Externer Honorareinzug und ärztliche Schweigepflicht.

Wolff, Hans J./Bachof, Otto/Stober, Rolf
Verwaltungsrecht, Band 1, 11. Auflage, 1999, Band 2, 6. Auflage, 2000,
Band 3, 5. Auflage, München 2004,
zit.: Wolff/Bachof/Stober, Verwaltungsrecht.

Wulffen von, Mathias
SGB X , Kommentar, 5. Auflage, München 2005,
zit.: Bearbeiter, in: von Wulffen, SGB X.

Würthwein, Sibylle
Innerorganisatorische Schweigepflicht im Rahmen des § 203 StGB, Stuttgart 1992,
zit.: Würthwein, Innerorganisatorische Schweigepflicht.

Zwiehoff, Gabriele
Strafrechtliche Aspekte des Organisationsverschuldens, MedR 2004,
S. 364 – 373.