4 Zweckändernde automatisierte Auswertung personenbezogener Daten mit anonymen Ergebnissen

Wie sieht die datenschutzrechtliche Bewertung eines Vorgangs aus, in dem personenbezogene Daten von einem automatisierten Prozess zu einem anderen Zweck als dem der Behandlung verarbeitet werden und im Ergebnis keine personenbezogenen Daten offenbart werden? Beispielsweise könnte ein solcher Prozess Behandlungsdaten nach passenden Patienten für neue Studien durchsuchen und eine anonyme Fallzahl zurückgeben, anhand der die Machbarkeit einer Studie mit solchen Patienten abgeschätzt werden könnte. Wäre für eine solche Verarbeitung eine eigene datenschutzrechtliche Rechtsgrundlage erforderlich?

Vorliegend ist ein automatisierter Prozess zu untersuchen, in den personenbezogene Daten zu einem anderen Zweck als dem der Behandlung eingestellt werden, der aber lediglich anonyme Ergebnisse an die den Prozess anstoßenden Bediener des entsprechenden Computersystems zurückgibt (diesen „offenbart").[75] Bewertungsmaßstab ist hierbei einerseits das Datenschutzrecht im engeren Sinne, also die Datenschutzgesetze von Bund und Ländern (dazu sogleich Kapitel I.4.1), und andererseits sonstige Regeln des Datenschutzrechts im weiteren Sinne, worunter insbesondere die nach § 203 StGB sanktionierte ärztliche Schweigepflicht fällt (dazu unten Kapitel I.4.2).

75 Unter „Offenbaren" wird im Kontext dieser Frage zunächst also auch die einrichtungsinterne Kenntnisnahme erfasst und nicht – wie im Rahmen von § 203 StGB – lediglich die Datenübertragung oder ggf. auch die Zugriffsgewährung an einen Dritten, wobei es sich bei den anonymen Ergebnisdaten ohnehin nicht um personenbezogene Daten oder Patientengeheimnisse handelt. Ob bei einem Outsourcing des automatisierten Prozesses und noch personenbezogenen Input-Daten ein Offenbaren im Sinne von § 203 StGB vorliegt, wird in Kapitel I.4.2 der nachfolgenden Antwort untersucht (S. 47ff.).

Die vorliegende Frage zielt auf eine rein anonyme Rückgabe von Fallzahlen oder anderen absolut anonymisierten Daten ab, ohne dass die Ergebnisse der automatisierten Auswertung in irgendeiner Weise personenbezogen verwendet werden können. Der beispielhafte Anwendungsfall der Machbarkeitsabschätzung macht dies deutlich. In diesem Anwendungsfall geht es um eine möglichst realistische Schätzung der Anzahl der Patienten, die voraussichtlich in der Laufzeit einer geplanten Studie aufgrund passender Ein- und Ausschlusskriterien potenziell rekrutierbar sein werden. Hierfür werden die Daten bereits behandelter Patienten aus der Vergangenheit genutzt, da dies die beste Schätzungsgrundlage für das kommende „Patientengut" liefert. Somit werden im Regelfall auch die Patienten, deren Daten für die Machbarkeitsabschätzung herangezogen wurden, nicht für die Rekrutierung in der später laufenden Studie angesprochen. Deshalb ist die absolute Anonymisierung der Daten (hier durch bloße Fallzahlen) eine immanente Selbstbeschränkung des Anwendungsfalls und keine Einschränkung des intendierten Nutzenpotenzials.

Somit ist der hier im Fokus stehende Anwendungsfall der Machbarkeitsabschätzung (englisch: feasibility study) von der Rekrutierungsunterstützung zu unterscheiden. Im letzteren Fall möchte man tatsächlich genau die Patienten ansprechen, deren Datensätze man in einem Suchlauf als potenziell rekrutierungsrelevant identifiziert hat.

4.1 Bewertung aus Sicht des Datenschutzrechts im engeren Sinne

4.1.1 Umgang mit „personenbezogenen Daten" trotz anonymen Outputs?

Der Vorgang des Einstellens von Daten in einen automatisierten Prozess wäre nur dann an datenschutzrechtlichen Maßstäben zu messen, wenn „personenbezogene Daten" Gegenstand dieses Verfahrens wären. Für diese vorgelagerte Frage ist wiederum das zwar in unterschiedlichen Normen verankerte, letztlich aber vom Wortlaut der jeweiligen Legaldefinition her bundeseinheitliche Kriterium des Personenbezugs maßgeblich.[76]

4.1.1.1 Grundlegende Unterscheidung nach personenbezogenen oder anonymen Input-Daten

Nach Maßgabe der hierzu aufgestellten Kriterien[77] wird man eine personenbezogene Verwendung nur bejahen können, wenn Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person Gegenstand bzw. Input-Daten des automatisierten Prozesses sind. Falls der Prozess dagegen lediglich an bereits anonymisierten Daten ansetzt,[78] greift schon von vornherein kein datenschutzrechtlicher Erlaubnisvorbehalt.

76 Wobei es (aus dem Blickwinkel der Rechtssicherheit: leider) in der Auslegung und auch der Anwendung durch die Aufsichtsbehörden Unterschiede geben kann, auf welche in Kap. I.2 eingegangen wurde, s.o. S. 11ff.

77 Vgl. ausführlich oben S. 11ff.

78 Dabei genügt nach herrschender Meinung eine faktische Anonymisierung, wobei allerdings – wegen der Möglichkeit der Re-Identifizierung durch Mustervergleich – innerhalb einer Einrichtung, welche weiterhin über den personenbezogenen Ausgangsdatenbestand verfügt, bei Erhaltung eines Einzelfallbezugs im Rahmen einer angestrebten Anonymisierung hohe Anforderungen an die Annahme faktischer Anonymität zu stellen sind.

Selbst bei personenbezogenen Input-Daten stellt sich allerdings die Frage, ob angesichts des anonymen Outputs der hier betrachteten Auswertungen nach Sinn und Zweck des Datenschutzrechts ein Erlaubnisvorbehalt, also das Erfordernis einer spezifischen datenschutzrechtlichen Grundlage, sei es eine Einwilligung oder eine Rechtsvorschrift, entbehrlich ist. Dabei geht es um die Frage, ob und ggf. unter welchen Voraussetzungen der rein „statistische" Zweck bzw. die Zielsetzung einer bloß anonymen Ausgabe (z.B. von Fallzahlen) eine automatisierte Verarbeitung personenbezogener Daten aus dem Anwendungsbereich des Datenschutzrechts ausnimmt. In der Regel sind die Zwecke des Datenumgangs für die vorgreifliche Frage des Personenbezugs zwar nicht maßgeblich, sondern erst im Rahmen der Anwendung von datenschutzrechtlichen Erlaubnissen zur berücksichtigen. Soweit es sich um nicht personenbezogene, also rein statistische Zwecke handelt, könnte dies aber anders zu beurteilen sein.

Im Folgenden soll daher zunächst untersucht werden, ob und inwieweit in die hier betrachteten Auswertungsprozesse noch personenbezogene Daten eingestellt werden (sogleich Kap. I.4.1.1.2), bevor auf die Frage eingegangen wird, ob selbst bei technischer Verarbeitung von personenbezogenen Daten angesichts der anonymen Ergebnisse noch eine personenbezogene Datenverwendung im Sinne des Datenschutzrechts vorliegt (unten Kap. I.4.1.1.3)

4.1.1.2 Personenbezogener oder anonymer Input bei Datenbank-Auswertungen

Die zu bewertende automatisierte Auswertung setzt zunächst an den ohnehin zu Behandlungszwecken gespeicherten personenbezogenen Daten an, wenn auch die Ergebnisse nur anonym zur Verfügung gestellt werden. Diese oder Teile von diesen werden durch die intendierte Auswertung für andere Zwecke im technischen Sinne weiterverarbeitet, also zumindest in den Arbeitsspeicher des Computersystems geladen und typischerweise mit vorgegebenen Kriterien oder Mustern abgeglichen.

Dabei stellt sich zuerst die Frage, ob die in den Auswertungsprozess bzw. den Arbeitsspeicher zu Auswertungszwecken eingestellten Daten überhaupt personenbezogen sind, also identifizierende Teile enthalten. Dies wäre eindeutig der Fall, wenn ein Datensatz eingestellt würde, der einer bestimmten Person zugeordnet ist, also mit unmittelbaren Identifizierungsmerkmalen wie dem Namen versehen ist. Üblicherweise werden die betrachteten Daten jedoch in Datenbanksystemen nicht in einem einheitlichen Datensatz pro Betroffenem, sondern in verschiedenen Tabellen vorgehalten. Dabei werden die unmittelbar identifizierenden Stammdaten wie Name und Adresse i.d.R. in einer eigenen Tabelle gespeichert und einem Datenbank-internen Schlüssel, dem sogenannten Primärschlüssel, zugeordnet. Die eigentlichen Merkmale der betroffenen Person, im vorliegenden Kontext also deren Behandlungsdaten, werden in eigenen Tabellen ebenfalls diesem Primärschlüssel und über diesen nur mittelbar dem Betroffenen zugeordnet, welcher dann lediglich über Zwischenschritte bestimmbar ist. Für im Ergebnis anonyme Auswertungen wird i.d.R. der Zugriff auf nur mittelbar personenbezogene Datensätze aus solchen Tabellen genügen. Betrachtet man nur die auf dieser Basis in den Prozess eingestellten Daten ohne die außerhalb liegende Zuordnung des Primärschlüssels zum Betroffenen, dann könnte für sich betrachtet der Prozess selbst schon als anonym angesehen werden, also nicht nur dessen Ergebnis. Zieht man hingegen das gesamte im Computer- bzw. Datenbanksystem repräsentierte Wissen in Betracht, ist der Auswertungsprozess gleichwohl

personenbezogen. Diese Sichtweise liegt zunächst nahe, da das genannte Wissen der verantwortlichen Stelle grundsätzlich zur Verfügung steht, auch wenn sie sich in der Programmierung des Prozesses, was die Ergebnisausgabe angeht, selbst beschränkt. Dies gilt auch bei Zwischenschaltung weiterer Schlüssel oder Pseudonyme.

Lediglich eine vorgeschaltete Anonymisierung des Inputs für den Auswertungsprozess würde zu einer anderen Bewertung schon im Ansatz führen. Eine solche Anonymisierung erscheint zwar nicht ausgeschlossen, jedoch umso schwieriger, je differenzierter (wenn auch nicht personenbezogen) die Auswertung im Ergebnis und damit erst recht in der Ausgangsbasis sein soll. Denn je differenzierter die im Prozess auszuwertende Datenbasis ist, desto leichter lässt sich der Personenbezug durch Mustervergleich mit dem Gesamtdatenbestand erschließen.[79] Vor diesem Hintergrund bestehen hier auch an die Annahme faktischer Anonymität hohe Anforderungen.

Diese Herausforderung würde sich ebenfalls bei der Bewertung des Outputs stellen, sofern hier noch ein Einzelfallbezug erhalten bleiben soll. Bei Ausgabe absolut anonymer Ergebnisse wie bei bloßen Fallzahlen liegt jedoch unproblematisch Anonymität vor.

4.1.1.3 Personenbezug der Datenverwendung?

Selbst bei der technischen Verarbeitung personenbezogener Daten innerhalb des Auswertungsprozesses ist jedoch angesichts der nicht personenbezogenen Ergebnisse fraglich, ob es sich auch um eine Verwendung im datenschutzrechtlichen Sinn handelt. Unter einer Datenverwendung in diesem Sinn versteht man ein Verarbeiten oder ein Nutzen.

Datenverarbeitung

Eine Verarbeitung ist im Speichern, Verändern, Übermitteln, Sperren oder Löschen personenbezogener Daten zu sehen (§ 3 Abs. 4 BDSG).[80]

Speichern in diesem Sinn ist „das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung“ (§ 3 Abs. 4 Nr. 1 BDSG). Zwar findet wie bereits ausgeführt zumindest eine Speicherung im Arbeitsspeicher des Computersystems statt. Doch muss dies gemäß dem Schlussteil der Legaldefinition dem „Zweck ihrer weiteren Verarbeitung oder Nutzung“ dienen, was naheliegenderweise so zu interpretieren ist, dass auch die nachgelagerte Verwendung noch personenbezogen sein, die dem neuen Zweck dienende Speicherung personenbezogener Daten also eine gewisse Dauer haben muss. Das bloß temporäre Selektieren bzw. selektive Laden von Datensätzen oder Teilen von diesen stellt damit kein eigenständiges und gesondert zu rechtfertigendes Speichern dar. Etwas anderes könnte nur gelten, wenn zumindest einer bestimmbaren Person (z.B. über einen Primärschlüssel) zuordenbare (Zwischen-)Ergebnisse nicht (wie im

79 Zudem wird nicht immer einfach zu erschließen sein, welche Daten überhaupt in den Arbeitsspeicher geladen werden, denn das physische Datenbankschema kann gerade bei moderneren relationalen Datenbankensystemen im Gegensatz zu älteren satzbasierten Systemen vom satzorientierten logischen Schema abweichen, so dass u.U. im Hintergrund auch Daten geladen werden, auf welche nicht gezielt zugegriffen wird.

80 Die Terminologie der Datenschutzrichtlinie 95/46/EG sowie vieler LDSG weicht hiervon ab und fasst jeglichen Umgang mit personenbezogenen Daten, also auch die hier nicht aufgezählten Phasen der vorgelagerten Erhebung und der nachgelagerten Nutzung unter dem Begriff der Verarbeitung zusammen, was aber letztlich zu keiner anderen Bewertung führt.

Arbeitsspeicher) nur flüchtig, sondern persistent (also den laufenden Prozess überdauernd) beispielsweise in eigenen Tabellen in der Datenbank gespeichert würden. Dies kann durch eine entsprechende Ausgestaltung der vorliegend untersuchten automatisierten Prozesse ausgeschlossen werden, insbesondere durch einen Verzicht auf die Generierung möglicherweise personenbezogener Zwischenergebnisse oder deren sofortige Löschung.[81]

Allerdings muss die originäre Speicherung der auszuwertenden und noch personenbezogenen Daten zulässig sein, sonst dürfte die daran anknüpfende Auswertung ebenfalls als unzulässig gelten. Bezüglich der Behandlungsdaten bestehen zumindest einrichtungsintern aber für die Dauer der Behandlung und der daran anschließenden Aufbewahrungspflichten entsprechende Zulässigkeitstatbestände.[82]

Übermitteln ist „das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass a) die Daten an den Dritten weitergegeben werden oder b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft" (§ 3 Abs. 4 Nr. 3 BDSG). Eine solche Übermittlung läge vor, wenn an einen eigenverantwortlichen Dritten (nicht bloß einen weisungsgebundenen Auftragsdatenverarbeiter) personenbezogene Daten übertragen würden oder er die Verarbeitungsergebnisse auf andere Weise einer Person zuordnen könnte.[83] Soweit der Dritte jedoch keinen Zugang zum Gesamtsystem, insbesondere also der Zuordnung der Datensatz-Primärschlüssel zu den jeweils Betroffenen hat, und für ihn auch keine sonstigen Möglichkeiten zur Identifizierung durch Mustervergleich bestehen, kann dies ausgeschlossen werden. Um eine (Re-)Identifizierung durch Mustervergleich hinreichend auszuschließen, müssten die Daten für den empfangenden Dritten zumindest faktisch anonym sein, was zu einer Entfernung der unmittelbaren Identifikatoren zwingt sowie eine Ausdünnung der Quasi-Identifikatoren und, wenn der Patient auch bei dem Dritten behandelt wurde oder wird, auch der medizinischen Daten nahelegt.

Verändern ist „das inhaltliche Umgestalten gespeicherter personenbezogener Daten" (§ 3 Abs. 4 Nr. 2 BDSG). Dies liegt vor, wenn der Informationsgehalt (die Semantik) der Daten geändert wird.[84] Nicht ausreichend sind bloß syntaktische Änderungen, also beispielsweise die Selektion bestimmter Datensätze oder Datenfelder oder auch die Anlage neuer Tabellen in einer Datenbank, selbst wenn dadurch der bisher schon vorhandene Informationsgehalt leichter erkennbar sein mag. Denn nach einer Ver-

81 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 124 (zur kurzzeitigen Zwischenspeicherung im Verlauf automatisierter Verarbeitungs- oder Kommunikationsprozesse, wenn die Löschung in direktem zeitlichem Zusammenhang automatisch gesichert ist), Rdnr. 191, 195 (zu rein rechnerinternen Prozessen, die bei „alsbaldiger" Löschung evtl. personenbezogener interner Zwischenergebnisse kein Nutzen personenbezogener Daten darstellen).

82 Vgl. die Ausführungen zu Frage 5 aus dem Pflichtenheft (s. Anhang S. 353) unten in Kap. I.6, wo es zwar um Qualitätssicherung und Forschung geht, zur Abgrenzung aber auch die Vorschriften zur Datenverarbeitung zu Behandlungszwecken gestreift werden. Soweit die Auswertung nach Maßgabe der folgenden Ausführungen nicht personenbezogen ist, steht ihr auch eine Sperrung der Daten nach Abschluss der Behandlung für die Dauer der jeweiligen Aufbewahrungsfristen (vgl. § 35 Abs. 2 S. 2 Nr. 3, Abs. 3 BDSG) nicht entgegen.

83 Unter den genannten Bedingungen besteht aber auch ein Rechtfertigungsbedarf für die Einschaltung eines Auftragsdatenverarbeiters, denn dann läge mit einer technischen Übertragung zwar keine Übermittlung im rechtlichen Sinne, aber doch eine Form des Nutzens vor (s.u. S. 37ff.), welche über die Einhaltung der entsprechenden Regelungen (wie § 11 BDSG oder die Sondervorschriften der LKHG) zu rechtfertigen ist. Außerdem läge ein Offenbaren von Patientengeheimnissen vor, wenn der Auftragnehmer oder der Dritte nicht nur kontrollierten Zugang im Rahmen der Fernwartung zu einem Datenbestand in der Behandlungseinrichtung erhält, sondern der Datenbestand in dessen eigenen Machtbereich übertragen wird, falls die (hinreichende) Möglichkeit der Kenntnisnahme des Personenbezugs besteht, selbst wenn tatsächlich keine Kenntnis hiervon genommen wird (jedenfalls bei persistenter Datenübertragung, s. dazu unten S. 47ff.).

84 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 129.

änderung im hier verlangten Sinn muss eine andere Information als zuvor vorliegen.[85] Daher genügt der bloße Vergleich gespeicherter Werte nicht; wenn aber das Ergebnis des Vergleichs fixiert wird, liegt ein Speichern vor.[86] Dies gilt auch für den Abgleich mit vorgegebenen Werten (wie Ein- und Ausschlusskriterien für Studien); ein festgehaltenes Ergebnis führt hier zur Speicherung eines neuen Datums und nicht zur inhaltlichen Umgestaltung vorhandener Daten, wobei es für die Anwendung des Datenschutzrechtes darauf ankommt, ob für das gespeicherte Datum ein Personenbezug herstellbar ist. Diese Voraussetzung ist beim Festhalten anonymer Fallzahlen nicht gegeben.

Auch wenn § 3 Abs. 6 BDSG das Anonymisieren seinem Wortlaut nach als Sonderform des Veränderns personenbezogener Daten sieht, liegt doch keine Veränderung im Sinne der entsprechenden Legaldefinition (§ 3 Abs. 4 Nr. 2 BDSG) vor, weil es sich bei der Anonymisierung lediglich um eine Reduktion, nicht aber eine Substitution vorhandener Informationen handelt.[87] Dies trifft auch auf das Anonymisieren der Ergebnisse der vorliegend zu bewertenden automatisierten Auswertung zu. Die Anonymisierung erfolgt i.d.R. über das Löschen von (möglicherweise) die Betroffenen identifizierenden Merkmalen, soweit überhaupt solche vorab verarbeitet wurden.

Löschen ist „das Unkenntlichmachen gespeicherter personenbezogener Daten" (§ 3 Abs. 4 Nr. 5 BDSG). In vorliegendem Kontext könnte man damit auf den ersten Blick ein Löschen eventueller Identifikationsmerkmale bei Generierung der anonymen Ergebnisse als rechtfertigungsbedürftigen Vorgang in Betracht ziehen. Jedoch führt das Löschen des Personenbezugs gerade aus dem Anwendungsbereich des Datenschutzrechts heraus, weshalb es nach dessen Sinn und Zweck, jedenfalls im vorliegenden Kontext, vertretbar ist, diesen Vorgang keiner besonderen datenschutzrechtlichen Rechtfertigungspflicht zu unterwerfen, da der den primären (Behandlungs-) Zwecken dienende personenbezogene Ausgangsdatenbestand – entsprechend der hierfür geltenden Aufbewahrungspflichten – erhalten bleibt und nur eventuell noch personenbezogene Zwischenergebnisse der anderen Zwecken dienenden Auswertung gelöscht werden.[88] Letztlich bestimmt auch § 35 Abs. 2 S. 1 BDSG, dass nicht-öffent-

85 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 129.

86 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 129.

87 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 129; Gola/Schomerus, BDSG, § 3 Rdnr. 31.

88 So schließt Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 124, ein Speichern im Sinne des BDSG aus, wenn lediglich kurzzeitig zwischengespeicherte personenbezogene Daten sofort wieder gelöscht werden; gleiches gilt für den Ausschluss eines rechtfertigungsbedürftigen Nutzens zum Zweck statistischer (nicht personenbezogener) Auswertungen, welche nicht personenbezogene Zwischenergebnisse nur rechnerintern erstellen und sogleich wieder löschen (Dammann, a.a.O., § 3 Rdnr. 191, 195). Dies würde sich nicht damit vertragen, in den genannten Fällen einen besonderen Rechtfertigungsbedarf für das Löschen anzunehmen. Damit dürfte die Annahme eines grundsätzlichen datenschutzrechtlichen Löschungsverbots durch Dammann, a.a.O., § 3 Rdnr. 172ff., nicht für die eingangs erwähnten Sonderfälle der bloßen Löschung von zwischengespeicherten Daten gelten. In diesen Fällen könnte man sogar von impliziten Löschungspflichten (zur Vermeidung des Personenbezugs) ausgehen, die neben die von Dammann, a.a.O., § 3 Rdnr. 172ff., explizit genannten Löschungsgebote (§§ 20, 35 BDSG) treten. Ein im Übrigen von Dammann, a.a.O., § 3 Rdnr. 172ff. angenommenes Löschungsverbot ist mit dem Wortlaut des § 4 Abs. 1 BDSG zwar vereinbar (die dort unter Erlaubnisvorbehalt gestellte Verarbeitung erfasst grundsätzlich auch das Löschen). Nach Sinn und Zweck des Datenschutzrechts erscheint es aber nicht zwingend und könnte außerdem zu Verwerfungen gegenüber der recht ausgeklügelten Systematik geschäftlicher und medizinischer Aufbewahrungspflichten mit ihren jeweils eigenständigen Rechtsgrundlagen führen (wobei im Anwendungsbereich des BDSG jedenfalls die Löschungsregelung des § 35 Abs. 2 S. 1 diese Gefahr beseitigt). Diese besonderen Aufbewahrungspflichten sind freilich um eine spezifisch datenschutzrechtliche Protokollierung im Rahmen der Datensicherheit zu ergänzen, welche nötig sind, um insbes. kontrollieren zu können, ob nur Berechtigte Zugriff auf personenbezogene Daten und Zugang zu den entspr. IT-Systemen erhalten haben, wie es die Anlage zu § 9 BDSG fordert (vgl. Dammann, a.a.O., § 3 Rdnr. 184ff.). Bei diesen Protokollierungspflichten handelt es sich aber nicht um (originäre) Pflichten zur vollständigen Aufbewahrung personenbezogener Daten, sondern um derivative Pflichten zur Aufbewahrung von Zugriffslogfiles oder Ähnlichem, welche an einen vorgelagerten Umgang mit personenbezogenen Daten anknüpfen.

liche Stellen ihre Daten jederzeit löschen können, sofern das Gesetz nicht aufgrund von Aufbewahrungsfristen oder schutzwürdigen Interessen des Betroffenen eine Sperrung der Daten vorsieht.[89]

Etwas anderes könnte bei der Löschung nur bestimmter personenbezogener Merkmale, nicht aber des gesamten Personenbezugs gelten, wobei in Ersterem auch eine inhaltliche Umgestaltung im Sinne des Veränderns liegen kann, wenn ein gelöschtes Datenfeld einen eigenen Aussagegehalt hat („Fehlanzeige").[90]

Dies ist bei den vorliegend zu untersuchenden Prozessen jedoch nicht der Fall. Damit greift auch für das Anonymisieren von ursprünglich personenbezogenen Daten dann im Ergebnis kein datenschutzrechtlicher Erlaubnisvorbehalt, wenn hierdurch Aufbewahrungspflichten oder schutzwürdige Belange des Betroffenen nicht verletzt werden.[91] Davon ist auszugehen, wenn der Ausgangsdatenbestand erhalten bleibt und nur ein anonymisierter Abzug für Zwecke der Sekundärnutzung erstellt werden soll.

Datennutzung

Vom Wortlaut her käme aber zumindest der Auffangtatbestand des Nutzens personenbezogener Daten in Betracht. Denn das „Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt" (§ 3 Abs. 5 BDSG).[92] Hiervon wird jeder Gebrauch der Daten erfasst, der zu bestimmten Wirkungen führt.[93] Beispielsweise ist die Kenntnisnahme personenbezogener Daten eine Form der Nutzung, wobei das Nutzen die Kenntnisnahme nicht zwingend voraussetzt.[94] Wenn eine Kenntnisnahme der personenbezogenen Daten oder sonstige Folgen für den Betroffenen aber praktisch ausgeschlossen werden können, dann erstreckt sich das Nutzen der Daten nicht auf den Personenbezug und bedarf keiner datenschutzrechtlichen Grundlage.[95]

Dies ist vor dem Hintergrund zu sehen, dass der Wortlaut des Gesetzes zwar von jeder „Verwendung personenbezogener Daten" spricht (§ 3 Abs. 5 BDSG), was im technischen Sinne i.d.R. auch bei den hier untersuchten automatisierten Auswertungen ohne personenbezogenes Ergebnis der Fall ist. Allerdings wird der Zweck des Datenschutzrechts, nämlich „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird" (§ 1 Abs. 1 BDSG),[96] durch eine rein anonyme Auswertung nicht tangiert. Und

89 Wobei hier dahingestellt bleiben kann, ob es sich hierbei um eine konstitutive Erlaubnis und damit eine implizite Bestätigung eines Erlaubnisvorbehaltes oder nur um eine Klarstellung handelt.

90 Beispielsweise ergibt sich aus dem Melderegister nach Löschung der Angabe „evangelisch", dass der Betroffene nicht (mehr) Mitglied einer Religionsgemeinschaft mit Berechtigung zum Einzug von Kirchensteuer ist; Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 129; Gola/Schomerus, BDSG, § 3 Rdnr. 31.

91 So nicht nur zur nachfolgenden Verwendung anonymisierter Daten, sondern auch – konsistent zu dem vorliegend zur Löschung gefundenen Ergebnis – zum Vorgang des Anonymisierens: Gola/Schomerus, BDSG, § 3 Rdnr. 43. Anderer Ansicht (allerdings ohne nähere Begründung) Metschke/Wellbrock, Datenschutz in Wissenschaft und Forschung, Abschnitt 3.3, S. 20: „Die Erzeugung anonymisierter Daten aus personenbezogenen Einzelangaben unterliegt aber noch den Datenschutzvorschriften."

92 Zur Qualifikation als Auffangtatbestand: Gola/Schomerus, BDSG, § 3 Rdnr. 42.

93 Gola/Schomerus, BDSG, § 3 Rdnr. 42. Eine unmittelbare menschliche Interaktion ist aber nicht erforderlich. Es genügt, wenn ein Computersystem programmgemäß, also automatisiert, bestimmte Prozeduren auslöst, welche letztlich Wirkungen auf eine natürliche Person haben, so beispielsweise bei automatischen Defibrillatoren in Herzschrittmachern.

94 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 189.

95 Zum Erfordernis der Erstreckung der Verwendung auf den Personenbezug: Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 191.

96 Dieser prototypische Gesetzeszweck des BDSG lässt sich auch auf andere datenschutzrechtliche Vorschriften übertragen.

die Vorschriften des Datenschutzrechts sind gemäß diesem Zweck (dem „telos" der entsprechenden Gesetze, also teleologisch) auszulegen. So muss nicht immer der vom Wortlaut her naheliegende Wortsinn das richtige Auslegungsergebnis darstellen, sondern es sind im Rahmen des noch möglichen Wortsinns auch andere, dem Gesetzeszweck eher entsprechende Ergebnisse denkbar. Im Extremfall kann höchst ausnahmsweise der Wortlaut aus diesen Gründen auch teleologisch reduziert, d.h. ein Ergebnis vertreten werden, das nicht mehr vom noch möglichen Wortsinn gedeckt ist.[97] Das vorliegend gefundene Ergebnis dürfte aber noch im Rahmen teleologischer Auslegung des Wortlautes ohne teleologische Reduktion begründet werden können.

So werden auch bei rein statistischen Auswertungen rechnerintern zwar in der Regel die Datensätze bestimmter oder bestimmbarer Betroffener angesprochen,[98] was jedoch vernachlässigt werden kann, wenn das Ergebnis anonym ist und eventuell innerhalb des automatisierten Prozesses generierte personenbezogene Zwischendateien unverzüglich ohne reguläre Möglichkeit der Kenntnisnahme gelöscht werden.[99] Solche Auswertungen stellen also keine personenbezogene Nutzung dar, die im Hinblick auf den Datenschutz rechtfertigungsbedürftig wäre.[100] Dies gilt jedenfalls dann, wenn der automatisierte Prozess nicht nur innerhalb eines Computersystems abläuft, sondern sich dieses auch innerhalb der verantwortlichen Stelle befindet.

Wenn personenbezogene Daten allerdings persistent an eine außerhalb der Behandlungseinrichtung stehende Person oder Stelle weitergegeben werden, also physisch für gewisse Dauer in deren Verfügungsbereich gelangen, liegt in jedem Fall ein datenschutzrechtlich rechtfertigungsbedürftiger Vorgang vor, bei dem es nicht auf personenbezogene Ergebnisse oder die tatsächliche Kenntnisnahme (auch der Input-Daten) durch den Außenstehenden ankommt. Wenn die außenstehende Stelle ein eigenverantwortlicher Dritter ist, liegt (wie bereits ausgeführt) eine Übermittlung personenbezogener Daten vor.[101] Falls der Außenstehende ein weisungsgebundener Auftragsdatenverarbeiter ist, liegt in der technischen Datenübertragung an diesen wohl eine Sonderform der Nutzung personenbezogener Daten.[102]

Fraglich ist, ob dies auch gilt, wenn personenbezogene Input-Daten lediglich für die kurze Laufzeit eines automatisierten Prozesses extern im technischen Sinn verarbeitet (dem Wortlaut des Datenschutzrechts nach also wohl genutzt), anschließend aber sofort und ebenfalls automatisch gelöscht werden. Die Legaldefinition des Übermittelns, welche insoweit auch für potentielle Auftragsdatenverarbeiter analog herangezogen werden kann, spricht von der Weitergabe „gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten" (§ 3 Abs. 3 Nr. 3 Buchst. a BDSG). Die Referenz an die Speicherung deutet darauf hin, auch hier ein gewisses über die

97 Einen entsprechenden Schritt hat der BGH, Urt. v. 23.06.2009 – VI ZR 196/08 (spickmich), BGHZ 181, 328, juris Rdnr. 42, im entschiedenen Fall in Bezug auf den Verzicht auf das in § 29 Abs. 2 S. 1 Nr. 1 BDSG an sich vorgesehene Erfordernis der glaubhaften Darlegung eines berechtigten Interesses vorgenommen, wobei das Gericht dies selbst noch als „verfassungskonforme Auslegung" bezeichnet.

98 S. oben S. 33f.

99 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 191, 195.

100 Gola/Schomerus, BDSG, § 3 Rdnr. 42a.

101 S. oben Abschnitt Datenverarbeitung in Kap. I.4.1.1.3, S. 34ff..

102 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 195 (Übersendung zur Auftragsdatenverarbeitung); s.a. oben Abschnitt Datenverarbeitung in Kap. I.4.1.1.3, insbes. Fn. 83, S. 35.

Laufzeit eines kurzen Prozesses hinausgehendes Persistenzerfordernis anzunehmen.[103] Und die durch Datenverarbeitung gewonnenen Ergebnisse sollen letztlich nicht mehr personenbezogen sein, so dass es vertretbar erscheint, auch insoweit von keinem Erlaubnisvorbehalt auszugehen, jedenfalls solange die Abschottung des Prozesses von der Behandlungseinrichtung als originär verantwortlicher Stelle kontrolliert wird, diese also auch die Programmierung des automatisierten Prozesses verantwortet, wobei auch hierfür Auftragnehmer eingeschaltet werden können, welche allerdings im Sinne informationeller Gewaltenteilung idealerweise von denjenigen Auftragnehmern getrennt sein sollten, deren Rechnerkapazitäten genutzt werden. Auf diese Weise dürften sich die Risiken der Herstellung des Personenbezugs durch externe Stellen ausreichend reduzieren lassen. Der sicherste Weg bei Einschaltung externer Stellen wäre jedoch die Berufung auf eine Erlaubnisnorm oder die (faktische) Anonymisierung vor (sei es auch nur temporärer) Weitergabe.

Kein Erlaubnisvorbehalt bei abgeschotteten Prozessen mit rein anonymer Datenausgabe

Auch im vorliegend zu untersuchenden Machbarkeits-Szenario werden zwar möglicherweise personenbezogene Daten im technischen Sinne von einem automatisierten Prozess temporär (zu anderen Zwecken als denen der Behandlung) verarbeitet oder zumindest genutzt. Dies hat aber nicht den Zweck, der verantwortlichen Stelle personenbezogene Erkenntnisse über die Betroffenen zu vermitteln oder für diese sonstige Konsequenzen mit sich zu bringen, weshalb letztlich keine unter Erlaubnisvorbehalt stehende personenbezogene Verwendung im datenschutzrechtlichen Sinn vorliegt.[104]

Wenn die auszuwertende Datenbasis oder zumindest die in den Auswertungsprozess eingestellten Daten nicht bereits anonym sind, dürfte die bloße Zielsetzung und reguläre Programmierung, keine personenbezogenen Ergebnisse auszugeben, jedoch unter Umständen nicht genügen. Hier sind zusätzliche technische und organisatorische Sicherheitsmaßnahmen in Betracht zu ziehen, die tatsächlich verhindern, dass doch personenbezogene Ergebnisse geliefert oder noch personenbezogene, wenn auch an sich rechnerinterne Zwischenergebnisse z. B. von Administratoren des Computersystems „abgefangen" werden. In jedem Fall sind – wie bereits ausgeführt – eventuell personenbezogene Zwischenergebnisse unverzüglich zu löschen, denn nur unter dieser Bedingung können rechnerinterne Vorgänge vernachlässigt werden.[105] Das notwendige Maß der Sicherheitsvorkehrungen bzw. der Abkapselung des Prozesses richtet sich nach dem Schutzbedarf der betroffenen Daten und der Auswertung.

Einen vergleichbaren Ansatz verfolgt letztlich auch Art. 2 Abs. 3 LDSG BY, der explizit bestimmt, dass für „personenbezogene Daten in automatisierten Dateien, die aus-

103 S. oben zur Speicherung S. 35. Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 124, nennt mit der kurzzeitigen Zwischenspeicherung auf einem Internetknoten im Verlauf automatisierter Verarbeitungs- oder Kommunikationsprozesse, wenn die Löschung in direktem zeitlichem Zusammenhang ebenfalls automatisch gesichert ist, ein Beispiel, das eine „Externalisierung" dieser Laufzeit-Argumentation andeutet, also deren Übertragbarkeit auf derart flüchtige Datenweitergaben.

104 So geht auch das BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05 u.a. (Kennzeichenerfassung), BVerfGE 120, 378, juris Rdnr. 68, „in den Fällen der elektronischen Kennzeichenerfassung" davon aus, dass es nicht zu „einem Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung kommt […], wenn der Abgleich mit dem Fahndungsbestand unverzüglich vorgenommen wird und negativ ausfällt (sogenannter Nichttrefferfall) sowie zusätzlich rechtlich und technisch gesichert ist, dass die Daten anonym bleiben und sofort spurenlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden"; diese Voraussetzungen sah es in dem zu entscheidenden Fall allerdings als nicht gegeben an.

105 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 191, 195.

schließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden", nur bestimmte Vorschriften dieses Gesetzes gelten, insbesondere das Datengeheimnis (Art. 5) sowie die Verpflichtung zu technischen und organisatorischen Sicherheitsvorkehrungen gemäß Art. 7, nicht aber das Verbot mit Erlaubnisvorbehalt in Art. 15 Abs. 1.[106] Aufgrund dieser ausdrücklichen Regelung bedarf es im Anwendungsbereich des bayerischen LDSG keiner besonderen teleologischen Auslegung bzw. Reduktion der Verwendung personenbezogener Daten. Eine entsprechende Anwendung des Rechts ist jedoch aufgrund dieser Methoden auch im Anwendungsbereich anderer Datenschutzgesetze nicht ausgeschlossen.[107]

Beim bloßen Aufsummieren der Zahl von Patienten, welche bestimmte Bedingungen erfüllen, wird man aber keine besonderen Schutzvorkehrungen über die normale Programmierung einer lediglich anonymen Ausgabe (wie die einer Fallzahl) sowie die ohnehin angezeigten Sicherheitsmaßnahmen[108] hinaus treffen müssen. Denn hierbei handelt es sich um eine relativ einfache Auswertung und selbst rechnerintern würden allenfalls personenbezogene Zwischenergebnisse generiert („erfüllt Patient die Ein- bzw. Ausschlusskriterien"), deren Aussagegehalt sich auch durch einen Blick in die Datenbank bzw. einen manuellen Zugriff unschwer erschließen ließe.

Einen höheren Schutzbedarf dürften komplexere Verfahren, wie sie beim Data-Mining zum Einsatz kommen, aufweisen. Letztlich kann auch Data-Mining keine Zusammenhänge erkennen, welche nicht schon im Ausgangsdatenbestand angelegt waren. Allerdings sind die Zusammenhänge, welche durch entsprechend komplexe Verfahren zum Vorschein gebracht werden, doch eher verborgen und nicht ohne weiteres, falls überhaupt, durch einen Blick in die Datenbank oder manuelle Zugriffe zu erkennen. Hier sind daher besondere Vorkehrungen zu treffen, die sicherstellen, dass der automatisierte Auswertungsprozess nicht manipuliert wird und personenbezogene Zwischenergebnisse mit entsprechend hohem Erkenntniswert doch ausgegeben werden. Das wissenschaftliche Nutzenpotenzial solcher Verfahren kann zwar höher sein als der einfacher Auswertungen, dies gilt aus Sicht des Persönlichkeitsschutzes zunächst aber eben auch für das „Schadenspotential", so dass auch eine geringere Wahrscheinlichkeit der personenbezogenen Kompromittierung des an sich auf Anonymität angelegten Auswertungsprozesses im Rahmen einer Risikoanalyse relevant werden kann.

Des Weiteren besteht ein erhöhter Schutzbedarf im Hinblick auf technisch-organisatorische Maßnahmen auch bei nur temporärer Weiterleitung noch personenbezogener Input-Daten an externe Stellen, damit diese die Programmierung des automatisierten Prozesses nicht ohne Weiteres ändern können und von der Kenntnisnahme der Dateninhalte abgehalten werden. Eine persistente, über die befristete Laufzeit

106 Daneben gelten aus dem LDSG BY auch Art. 17 Abs. 4 (besondere Zweckbindung, hier auf ausschließlich verarbeitungstechnische Zwecke), Art. 25 (Sicherstellung des Datenschutzes, behördlicher Datenschutzbeauftragter), aus dem Bereich der Datenschutzaufsicht durch den LfD Art. 29–31, Art. 32 Abs. 1–3 (ohne Abs. 4 zum Verfahrensverzeichnis nach Art. 27) und Art. 33 sowie die Sanktionsnorm des Art. 37 (Ordnungswidrigkeiten, Strafvorschriften).

107 Ein Umkehrschluss dahingehend, dass im Anwendungsbereich anderer Datenschutzgesetze, welche keine entsprechende Regelung enthalten, auch automatisierte Prozesse ohne personenbezogenes Ergebnis erlaubnispflichtig wären, ist keineswegs zwingend, gerade wenn diese Gesetze von anderen Hoheitsträgern (Bund, andere Bundesländer) erlassen wurden, da man insoweit nicht von einer vollständig einheitlichen Rechtsordnung und damit einer gezielten Abweichung ausgehen kann. Insofern liegt eine Art Analogie im Rahmen teleologischer Rechtsanwendung näher, denn immerhin die Zwecke der entsprechenden Gesetze sind mit dem Schutz von Persönlichkeitsrechten beim Umgang mit personenbezogenen Daten die gleichen.

108 Insbesondere die Abschottung des Krankenhausnetzes nach außen, abgeschwächt auch zwischen Fachabteilungen.

des jeweiligen Prozesses hinausgehende Speicherung personenbezogener Daten bei externen Stellen würde allerdings in jedem Fall unter den Erlaubnisvorbehalt fallen.

4.1.2 Hilfsweise: Bedeutung einer Zweckänderung im Datenschutzrecht

Für den Fall, dass in den angesprochenen im Ergebnis anonymen Auswertungsprozessen (z.B. im Machbarkeitsszenario) doch ein personenbezogenes Verwenden zu sehen wäre,[109] soll im Folgenden hilfsweise darauf eingegangen werden, welche Konsequenzen sich aus Sicht des Datenschutzrechts aus einer solchen Zweckänderung ergeben. Denn angesichts des Umstands, dass die Daten ursprünglich zu Behandlungszwecken erhoben wurden, die Einstellung in den Suchlauf aber nicht hierzu, sondern zu Zwecken der Forschung erfolgt, liegt eine Zweckänderung vor. Die hierbei gewonnenen Erkenntnisse können auch bei der Bewertung des hier nicht im Mittelpunkt stehenden klar personenbezogenen Rekrutierungsszenarios helfen.

4.1.2.1 Herleitung und inhaltliche Reichweite des Zweckbindungsgrundsatzes

Als wesentliches Leitprinzip gilt im Datenschutzrecht der Zweckbindungsgrundsatz. Er wurde durch das Bundesverfassungsgericht im Volkszählungsurteil aus dem Recht auf informationelle Selbstbestimmung hergeleitet, wodurch ihm Verfassungsrang zukommt.[110] Eine Entsprechung findet sich auch in Art. 6 Abs. 1 Buchst. b der europäischen Datenschutzrichtlinie 95/46/EG.[111] Auf Grund seiner Ausprägung als allgemeines Prinzip lässt sich der Zweckbindungsgrundsatz allen Datenschutzgesetzen gleichsam vor „die Klammer" ziehen.[112]

Inhaltlich folgt aus dem Zweckbindungsgrundsatz, dass jeder Datenumgang nur zu einem vorab festzulegenden und hinreichend bestimmten Zweck erfolgen darf.[113] Grundsätzlich kann danach keine Vorratsdatenspeicherung zulässig sein, bei der die Zwecke erst im Moment des Zugriffs auf die Daten definiert werden.[114] Daraus folgt zugleich, dass jeder Datenumgang, der zu einem anderen als dem ursprünglichen Zweck erfolgt, qualitativ als neuer Abschnitt der Datenverarbeitung anzusehen ist, welcher für sich genommen ein eigenes Rechtfertigungsbedürfnis hervorruft. Denn ändern sich die Zwecke einer Datenverarbeitung, sind unter Umständen gänzlich neue Belange in die regelmäßig erforderliche Abwägung der widerstreitenden Interessen einzustellen.

109 Sei es, weil eine abweichende Rechtsmeinung vertreten wird, oder weil Sicherungsvorkehrungen unterlassen oder umgangen werden und doch ein personenbezogenes Ergebnis ausgegeben wird.
110 Grundlegend BVerfGE 65, 1, 45ff.
111 Näher zur Zweckbindung auf europäischer Ebene Dammann, in: Simitis, BDSG, § 14 Rdnr. 37.
112 Vgl. Helfrich, in: Hoeren/Sieber/Holznagel, Multimediarecht, Teil 16.1 IV Rdnr. 79.
113 Helfrich, in: Hoeren/Sieber/Holznagel, Multimediarecht, Teil 16.1 IV Rdnr. 81.
114 Für den Bereich öffentlicher Stellen vgl. BVerfG, NJW 2010, 833, 838; grundlegend BVerfGE 65, 1 (46). Dies schließt jedoch eine Vorratsdatenspeicherung nicht generell aus, sondern stellt sie unter besonderen Rechtfertigungsbedarf und macht sie von begleitenden Sicherungen abhängig, wozu zumindest auch die (möglichst konkrete) Vorab-Festlegung der grundsätzlich zulässigen Zugriffszwecke gehört, auch wenn erst im Nachhinein entschieden werden kann, ob im Einzelfall ein Zugriff für diese Zwecke erforderlich ist.

4.1.2.2 Notwendigkeit eigener Rechtsgrundlage für zweckändernde Verarbeitungen

Der Befund, dass eine Datenverarbeitung zu neuen Zwecken gleichzeitig auch eine neue rechtfertigungsbedürftige Datenverarbeitungsphase darstellt, führt aber noch nicht zwangsläufig dazu, hierfür auch eine eigenständige, gerade an die zweckändernde Verarbeitung anknüpfende Rechtsgrundlage als erforderlich anzusehen.

Denkbar erschiene es nämlich grundsätzlich, zur Rechtfertigung der neuen zweckändernden Datenverarbeitungsphase – wie sonst auch – auf einen allgemeinen Erlaubnistatbestand zu rekurrieren. In diesem Fall würde indes unberücksichtigt bleiben, dass eine Datenverarbeitung zu geänderten Zwecken unter (horizontal) gänzlich neuen „Vorzeichen" steht, während die einzelnen Datenverarbeitungen eines zu den ursprünglichen Zwecken erfolgenden Datenumgangs lediglich (vertikal) in die Tiefe gehen, dabei aber immer vor dem selben Hintergrund – der Verfolgung eines einheitlichen Zwecks – erfolgen. Mit gleichsam in Reihe geschalteten Zwecken geht in aller Regel aber auch eine stärkere Beeinträchtigung der Interessen der Betroffenen einher. Wenn nämlich ein und dasselbe Datum unter Aufgabe der ursprünglichen Intention und gleichzeitiger Berufung auf einen neuen Zweck erneut verarbeitet bzw. genutzt wird, ist regelmäßig auch der Verwendungszusammenhang ein völlig neuer.

Angesichts des Grundrechts auf informationelle Selbstbestimmung erscheint es daher nicht fernliegend, für jede Zweckänderung auch ein eigenständiges Regelungsbedürfnis im Sinne einer eigenen Rechtsgrundlage zu fordern, zumal die genannten Erwägungen mit Blick auf die potenziell größere Gefahr für die Persönlichkeitsrechte der Betroffenen ausreichend abstrahierbar und generalisierbar erscheinen. Eine solche eigene Rechtsgrundlage sehen konsequenterweise die Datenschutzgesetze auch vor.[115] Fehlte eine solche, wäre die Zweckänderung insoweit nicht über die allgemeinen Zulässigkeitstatbestände legitimierbar und damit unzulässig, da jene nur einen Datenumgang zu dem jeweils originären Zweck rechtfertigen können.

4.1.2.3 Erfordernis bereichsspezifischer Rechtsgrundlage für Forschungszwecke

Weitergehend ist dann aber zu klären, ob für den vorliegenden Fall der Verarbeitung zu Zwecken der Anfertigung von Studien u.ä. insoweit sogar eine bereichsspezifische Rechtsgrundlage erforderlich ist. Dies muss sich nach den allgemeinen Grundsätzen richten, die Aussagen über die Notwendigkeit einer Rechtsgrundlage treffen, im öffentlichen Bereich also z.B. nach dem Grundsatz des Vorbehalts des Gesetzes. Ein eigenes Regelungsbedürfnis ist danach immer dann anzunehmen, wenn hinreichend generalisierbare grundrechtsbeeinträchtigende Sachverhalte einheitlichen Wertungen bzw. Beurteilungsmaßstäben unterstellt werden können. Für die Notwendigkeit einer spezifischen Rechtsgrundlage in den vorliegenden Konstellationen spricht die Rechtsprechung des Bundesverfassungsgerichts zur hinreichenden Bestimmtheit und Bereichstypik von datenschutzrechtlichen Erlaubnistatbeständen.[116] Eine solche ist erst recht dann zu fordern, wenn sich – wie hier – klar identifizierbare jeweils grundrechtlich geschützte Rechtspositionen gegenüberstehen und der Gesetzgeber die Abwägungsentscheidung bereits durch eine entsprechende Ausgestaltung der Tatbestände antizipieren kann.

115 Vgl. auf Bundesebene § 14 Abs. 2 und § 28 Abs. 2 BDSG.
116 BVerfGE 65, 1, 46.

Vorliegend ist nämlich zu berücksichtigen, dass der Zweck der Anfertigung von Studien dem Schutzbereich der Wissenschaftsfreiheit aus Art. 5 Abs. 3 GG unterfällt, da es sich hierbei um Forschung, d.h. um geistige Tätigkeiten handelt, die das Ziel verfolgen, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen.[117] Der verfassungsrechtliche Begriff der Forschung ist damit denkbar weit gehalten, sodass Einschränkungen (z.B. in Bezug auf den tatsächlichen Mehrwert eines bestimmten Forschungsvorhabens) erst auf Ebene der Abwägung vorzunehmen sind. Spiegelbildliche Erwägungen finden sich auch in der datenschutzrechtlichen Literatur zum einfachgesetzlichen § 40 BDSG, die sich ausführlich mit der Frage beschäftigt, was unter „wissenschaftlicher Forschung" zu verstehen ist. Einigkeit besteht hier jedenfalls darin, dass hierunter nur eine unabhängige Forschung fallen soll,[118] was bei privater Forschungstätigkeit problematisch sein kann, aber nicht generell ausgeschlossen ist. Einen Datenumgang zum Zweck der wissenschaftlichen Forschung wird man dann ablehnen müssen, wenn die wissenschaftliche Tätigkeit gegenüber rein wirtschaftlichen Motiven von lediglich untergeordneter Bedeutung ist.[119] Andererseits wird man eine unabhängige Forschung nicht schon in Fällen ablehnen müssen, in denen zwar eine Beauftragung und die Mittelbereitstellung durch einen Dritten erfolgt, dieser aber keinen bestimmungsgemäßen Einfluss auf den Forschungsprozess und insbesondere das -ergebnis nehmen kann.[120] Grundsätzlich könnte daher auch eine aus rein wirtschaftlichen Motiven heraus erfolgende Forschung durch Unternehmen der Pharmaindustrie unabhängig strukturiert sein.[121] Die Forschung muss also nicht bloßer Selbstzweck sein.[122]

Festzuhalten ist damit, dass der vorliegend vorgenommene Datenumgang zu Forschungszwecken erfolgt, sodass im Rahmen der Beurteilung der Zulässigkeit der Zweckänderung eine Abwägung zwischen dem Recht auf informationelle Selbstbestimmung und der Wissenschaftsfreiheit vorzunehmen ist. Für die Wissenschaftsfreiheit fällt dabei ins Gewicht, dass diese nicht unter einem Gesetzesvorbehalt steht. Eine Einschränkung dieser Freiheit kann somit nicht aufgrund irgendwelcher Gemeinwohlaspekte oder sonst als schutzwürdig angesehener Interessen erfolgen, wobei diese Belange grundsätzlich im Ermessen des Gesetzgebers stehen, sondern muss auf Rechtsgüter gestützt werden, die sich unmittelbar aus der Verfassung ergeben. Zu diesen verfassungsimmanenten Gütern gehört jedoch das Grundrecht auf informationelle Selbstbestimmung. Zudem folgt aus der Wissenschaftsfreiheit kein Anspruch auf unmittelbaren Zugang zu personenbezogenen Daten.[123] Daraus leiten der Bundesgesetzgeber und viele Landesgesetzgeber ab, dass die Wissenschaftsfreiheit in einer abstrakten Abwägung gegenüber den Interessen der Patienten tendenziell eine schwächere Position einnimmt. Dies spiegelt sich in den Formulierungen von Erlaubnisnormen wider, die ein erhebliches Überwiegen des wissenschaftlichen Forschungsinteresses gegenüber dem Interesse des Patienten am Ausschluss des Datenumgangs bezogen auf ein konkretes Forschungsvorhaben verlangen.[124] Dies gilt vor

117 Grundlegend BVerfGE 35, 79 = NJW 1973, 1176, 1176.
118 Vgl. nur Gola/Schomerus, BDSG, § 40 Rdnr. 7ff.; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 40 Rdnr. 5.
119 Gola/Schomerus, BDSG, § 40 Rdnr. 8.
120 Vgl. Gola/Schomerus, BDSG, § 40 Rdnr. 8.
121 Vgl. Gola/Schomerus, BDSG, § 40 Rdnr. 8.
122 Gola/Schomerus, BDSG, § 40 Rdnr. 10.
123 Kempen, in: Epping/Hillgruber, BeckOK GG, 2009, Art. 5 Rdnr. 182.
124 So in § 28 Abs. 8, 6 Nr. 4 BDSG und den meisten LDSG und LKHG, s.u. Kap. I.6, S. 75ff.

allem auch mit Blick auf den Umstand, dass für die Anfertigung von Studien nicht immer personenbezogene Daten erforderlich sind. Diese Abwägungsgesichtspunkte sind für den Gesetzgeber vorhersehbar, sodass es sich insoweit anbietet, eine eigene bereichsspezifische Rechtsgrundlage für Zweckänderungen zu Forschungszwecken zu schaffen. Dem ist der Gesetzgeber im Datenschutzrecht gefolgt.[125] Bei der Anwendung der entsprechenden Regelungen kann jedoch als ein Aspekt, der die Zulässigkeit der Sekundärnutzung durch die behandelnde Einrichtung selbst begünstigt, angeführt werden, dass hierbei kein originärer Anspruch auf Zugang zu personenbezogenen Daten realisiert wird, sondern lediglich eine Freiheit zur Verwendung der ohnehin bereits vorliegenden Patientendaten zu Zwecken der wissenschaftlichen Forschung ausgeübt wird.

4.1.2.4 Bestimmtheit der Rechtsgrundlagen und Vorhabensbezug

Problematisch ist dennoch, ob die vorliegend in Rede stehende Verwendung, wäre sie denn personenbezogen, durch die vorhandenen forschungsspezifischen Regelungen zu zweckändernden Verarbeitungen sensibler Daten überhaupt legitimierbar wäre. Denn der Gesetzgeber – des Bundes und der meisten Bundesländer – gibt im Rahmen der entsprechenden Tatbestände regelmäßig einen strengen Maßstab vor und verlagert die Rechtfertigungslast der Zweckänderung deutlich auf die Seite der verantwortlichen Stelle. So muss die Zweckänderung gerade *erforderlich* sein, um die wissenschaftliche Forschung betreiben zu können.[126] Darüber hinaus darf der Forschungszweck nicht auch auf andere Weise oder überhaupt nicht bzw. nur mit *unverhältnismäßig hohem Aufwand* erreicht werden können. Ferner muss das wissenschaftliche Interesse an der Forschung das Interesse des Betroffenen am Unterlassen einer zweckändernden Verarbeitung *erheblich* überwiegen.

Damit werden nicht unerhebliche Hürden aufgestellt, aus denen sich zugleich ergibt, dass die Zulässigkeit einer zweckändernden Verarbeitung auch zu Forschungszwecken auf rein gesetzlicher Grundlage einen Ausnahmefall darstellt.[127] Folglich müssten regelmäßig besondere Umstände angeführt werden können, weshalb das Forschungsvorhaben gerade mit Blick auf eine Verwendung personenbezogener Daten als gerechtfertigt anzusehen sein soll. In der Regel darf der Betroffene also nicht ungefragt zum Forschungsobjekt werden.[128]

Um eine entsprechende Abwägungsentscheidung überhaupt treffen zu können, sind die Umstände des konkreten Vorhabens (Zahl der Kenntnis erlangenden Personen, nicht auszuschließende Eventualitäten, Belastung für den Betroffenen) sorgfältig zu identifizieren.[129] Gelingt dies nicht, kann streng genommen eine Abwägung überhaupt nicht erfolgen. Für die Zweckänderung bedeutete dies aber dann zugleich, dass diese als unzulässig anzusehen wäre.

125 Vgl. auf Bundesebene § 14 Abs. 5 und § 28 Abs. 8 BDSG. Die landesrechtlichen Regelungen sehen überwiegend vergleichbare Vorschriften vor, vgl. auch Heckmann, in: Taeger/Gabel, BDSG, § 14 Rdnr. 125.

126 Vgl. hierzu und zu den folgenden Voraussetzungen exemplarisch auf Bundesebene § 14 Abs. 5 und § 28 Abs. 8 BDSG. Die Landesdatenschutz- bzw. Landeskrankenhausgesetze enthalten überwiegend ähnlich strenge Vorgaben. Im Einzelnen dazu unten zu Frage 5 aus dem Pflichtenheft, Kap. I.6, S. 75ff.

127 Ähnlich Heckmann, in: Taeger/Gabel, BDSG, § 14 Rdnr. 118

128 Vgl. Gola/Schomerus, BDSG, § 40 Rdnr. 5.

129 Dammann, in: Simitis (Hg.), BDSG, § 14 Rdnr. 92.

Bedenken gegen ein Rekurrieren auf diese Rechtsvorschriften könnten deshalb im vorliegenden Gesamtkontext bestehen, da diese Zweckänderungen lediglich für konkrete eigene Forschungsvorhaben der verantwortlichen Stelle zulassen. Nicht rechtfertigen können diese Normen i.d.R. die Verwendung personenbezogener Daten zu unbestimmten Forschungszwecken bzw. zum Aufbau von abstrakten Datenpools, auf die später zwar für konkrete Vorhaben zurückgegriffen werden soll, welche aber im Zeitpunkt der Einspeicherung gerade noch nicht feststehen, sei es was das Studienziel angeht oder auch die beteiligten Einrichtungen.[130]

Diese Bedenken beträfen aber vor allem solche Studienportale, die für prinzipiell jegliche Form von Forschung offene sind, soweit die Behandlungsdaten dort noch personenbezogen wären.[131] Bei einer bereits einrichtungsintern durchgeführten Anonymisierung stellen sich jedoch auch solche Portale insoweit als unproblematisch dar, da die entsprechenden Verarbeitungsvorgänge dann keinem datenschutzrechtlichen Erlaubnisvorbehalt unterliegen.[132] In Modellen, die einem entsprechenden Vorbehalt unterliegen, wie beispielsweise solche mit einer einrichtungsübergreifenden Pseudonymisierung durch einen Datentreuhänder, steht mit der Einwilligung grundsätzlich eine datenschutzrechtliche Erlaubnis eigener Art zur Verfügung.[133] Von den vorliegenden Bedenken könnten aber insbesondere Forschungsmodelle betroffen sein, die lediglich auf einer einrichtungsinternen Pseudonymisierung ohne Einwilligung beruhen, soweit hierdurch eine, sei es auch ausschließlich einrichtungsintern vorgehaltene und verwendbare, nur pseudonyme, also noch personenbezogene Datenbank für allgemeine Forschungszwecke entsteht.[134] Hierauf soll abschließend erst nach Klärung weiterer Aspekte näher eingegangen werden.[135]

4.1.2.5 Exkurs: Personenbezogene Suchläufe zur Rekrutierung von Probanden

Vorliegend soll ergänzend zur eigentlichen Fragestellung nach dem Personenbezug der im Ergebnis anonymen Auswertungen, also dem Szenario der Machbarkeitsuntersuchung, in Bezug auf die eben angerissenen Zulässigkeitsfragen lediglich kurz auf das Szenario der Probandenrekrutierung durch personenbezogene Suchläufe eingegangen werden.

Auch die zuletzt genannten Auswertungen setzen entsprechende Ein- und Ausschlusskriterien für die Suche nach geeigneten Probanden im Patientenbestand voraus. Insoweit müssen die Studienvorhaben also schon ein Mindestmaß an Konkretisierung aufweisen, denn andernfalls lägen noch keine solchen Kriterien vor.

Solange nur einfache Suchläufe bzw. Selektionen nach sich bereits unmittelbar aus den Behandlungsdaten ergebenden Kriterien durchgeführt werden, dürfte dies für ein bestimmtes Forschungsvorhaben im Sinne der gesetzlichen Forschungsklauseln ausreichen. Denn das notwendige Maß an Bestimmtheit richtet sich auch nach der Schwere des Eingriffes in das informationelle Selbstbestimmungsrecht und damit

130 Vgl. Heckmann, in: Taeger/Gabel, BDSG, § 14 Rdnr. 89; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rdnr. 177; wohl ein weniger enges Verständnis zugrunde legend Dammann, in: Simitis (Hg.), BDSG, § 14 Rdnr. 91.
131 Was im Rahmen des cloud4health-Projektes jedoch ausgeschlossen werden soll.
132 So im Architekturmodell 1 des cloud4health-Projektes (vgl. die Darstellung im Pflichtenheft im Anhang).
133 So im Architekturmodell 3 des cloud4health-Projekts. Zu den Herausforderungen der Informiertheit und Bestimmtheit der Einwilligung s.u. zu Frage 5 aus dem Pflichtenheft, insbes. S. 117ff.
134 So im Architekturmodell 2 des cloud4health-Projekts.
135 S. unten Kap. I.6, S. 75ff.

nach dem Ausmaß der Datenverwendung, welches bei den genannten einfachen Suchläufern eher gering ist.

Gerade wenn ein automatisierter Suchlauf zur Identifizierung geeigneter Probanden in den Behandlungsdaten dazu dienen soll, von den betroffenen Patienten die Einwilligung in eine Studienteilnahme einzuholen, dürfte diese Suche und Ansprache auch im Rahmen der Abwägung nach den üblichen Forschungsklauseln regelmäßig zulässig sein, jedenfalls wenn es um ein nicht ganz untergeordnetes Forschungsinteresse geht und nicht von vornherein ausgeschlossen ist, dass eine hinreichende Zahl von so identifizierten Patienten im Ergebnis tatsächlich einwilligt. Dies erscheint selbst bei einer recht strengen Forschungsklausel wie der in § 28 Abs. 6 Nr. 4 BDSG vertretbar, welche u.a. ein erhebliches Überwiegen der Forschungs- gegenüber den Betroffeneninteressen sowie die praktische Alternativlosigkeit dieses Vorgehens fordert.[136]

Eine umfassendere Abwägung mit offenem Ausgang wird aber nötig sein, wenn die Auswertung nicht in der einfachen Selektion nach unmittelbar vorhandenen Datenwerten besteht, sondern selbst bereits ein komplexes Verfahren zur Aufdeckung bisher nicht ohne Weiteres erkennbarer Zusammenhänge im vorhandenen Datenbestand darstellt, welche dann als Zwischenergebnisse für die weitere Selektion dienen. Gleiches gilt, wenn Auswertungen, auch einfachere, durch eine externe Stelle und nicht die Behandlungseinrichtung selbst vorgenommen werden sollen.

Eine Unzulässigkeit auf Basis der üblichen Forschungsklauseln kann sich zudem dann ergeben, wenn der Patient vorab einen begründeten Widerspruch gegen eine solche Heranziehung seiner Daten eingelegt hat, was insbesondere bei besonders stigmatisierten oder persönlich auch in der Retrospektive belastenden Erkrankungen der Fall sein könnte.

Zwar wäre grundsätzlich denkbar, von allen behandelten Patienten vorab die Einwilligung für einen Probandensuchlauf einzuholen bzw. zu erbitten.[137] Falls dies aber erst geschehen soll, wenn Selektionskriterien für ein konkretes Vorhaben feststehen, müsste die Behandlungseinrichtung an bereits entlassene Patienten noch einmal herantreten, so diese denn überhaupt noch erreichbar sind. Für die bloße Durchführung eines Probandensuchlaufes dürfte dies in der Regel einen unangemessenen Aufwand darstellen, so dass die für die konkrete Studie erforderliche Vor-Selektion tauglicher Probanden auf Grundlage gesetzlicher Forschungsklauseln als praktisch alternativlos und damit regelmäßig als zulässig angesehen werden kann.

Gegenüber einer allgemeinen Einwilligung in solche Suchläufe, die unabhängig von konkreten Vorhaben und Selektionskriterien schon mit Patientenaufnahme eingeholt werden soll, könnten Bedenken im Hinblick auf ihre Bestimmtheit bestehen. Zwar können bei geringfügigeren Eingriffen in das informationelle Selbstbestimmungsrecht auch geringere Anforderungen an die Bestimmtheit der Einwilligung angelegt werden. Bedenken im Hinblick auf die Wirksamkeit einer solchen allgemeinen Einwilligung lassen sich gleichwohl nicht ohne weiteres ausräumen. Freilich

136 Ein Outsourcing dieses Suchlaufes auf von anderen Stellen betriebene Rechenzentren könnte rein datenschutzrechtlich als Auftragsdatenverarbeitung privilegiert zulässig sein (z.B. nach § 11 BDSG). Allerdings dürfte dann auch ein Offenbaren im Sinne von § 203 StGB vorliegen, welches nach ganz herrschender Meinung nicht über § 11 BDSG (der nicht einmal einen Gesundheitsbezug aufweist) und nach herrschender Meinung auch nicht über § 28 Abs. 6 BDSG gerechtfertigt werden kann, da das BDSG den Schutz durch die Schweigepflicht nicht verringern soll. In Betracht kämen aber spezifische Vorschriften zur Patientendatenverarbeitung im Auftrag nach den LKHG. S. zum Ganzen unten S. 47ff.

137 Sozusagen eine Einwilligung zur Schaffung der Voraussetzung für die Einholung einer weiteren Einwilligung.

sollte eine Klinik, welche allgemein solche Suchläufe plant, in ihren Datenschutzhinweisen zumindest kurz darauf eingehen, auch wenn dieses Vorgehen auf eine gesetzliche Erlaubnis gestützt wird.

4.1.2.6 Rückfallargument: Machbarkeitsabschätzungen auf Basis von Forschungsklauseln zulässig

Diese zur Rekrutierungsunterstützung gefundenen Ergebnisse bzw. deren regelmäßige Zulässigkeit auf Basis der üblichen Forschungsklauseln dürften erst recht auf im Ergebnis anonyme Auswertungen, jedenfalls solche einfacher Art, im Szenario der Machbarkeitsabschätzung übertragen werden können, sollte man diese – entgegen der oben in Kap. 4.1.1 getroffenen Annahme[138] – doch als personenbezogenes Verwenden ansehen. Hier würde sich der Umstand der lediglich anonymisierten Ergebnisausgabe in der Abwägung regelmäßig zu Gunsten der Zulässigkeit auswirken, wenn der Prozess nur einrichtungsintern abläuft. Bei einem Outsourcing der Abschätzung müsste jedoch, soweit hierbei ein Zugriff auf personenbezogene (Input-) Daten nicht ausgeschlossen ist, eine umfassendere Abwägung mit offenerem Ergebnis durchgeführt werden.

4.2 Vereinbarkeit mit der Schweigepflicht der Heilberufe

Zum Datenschutz im weiteren Sinn zählt auch die ärztliche Schweigepflicht, wie sie sich in den Berufsordnungen (vgl. § 9 MBO-Ä) und insbesondere in § 203 StGB findet.

4.2.1 Verletzung von Privatgeheimnissen (§ 203 StGB)

Im Hinblick auf § 203 StGB ist festzustellen, dass für eine Verletzung der Schweigepflicht in diesem Sinne nach dem Gesetzeswortlaut ein „Offenbaren" fremder Geheimnisse (wie Patientendaten) nötig ist. Dabei ist allerdings umstritten, ob hierfür die tatsächliche Kenntnisnahme durch einen Außenstehenden erfolgen muss oder das bloße Eröffnen der Möglichkeit der Kenntnisnahme genügt.[139]

4.2.1.1 Kein Bruch der Schweigepflicht durch interne Kenntnisnahme oder anonyme Weitergabe

Die ausschließlich einrichtungsinterne Kenntnisnahme durch behandelndes Personal und jedenfalls auch das Personal der gleichen Fachabteilung sowie die „Gehilfen der Ärzte" aus der internen IT-Administration wären damit jedenfalls schon nicht tatbestandsmäßig.

Werden lediglich anonyme Fallzahlen weitergegeben, wodurch nur die Machbarkeit einer Studie abschätzbar wird, liegt zudem bereits kein „fremdes Geheimnis", geschweige denn ein „Offenbaren" vor.[140] Eine Strafbarkeit scheidet damit insoweit

138 S. oben S. 32ff.
139 Für das Erfordernis der Einräumung einer Verfügungsgewalt über die Daten Paul/Gendelev, ZD 2012, 315, 319. Näher dazu sogleich S. 48ff. und unten S. 262.
140 Fischer, StGB, § 203 Rdnr. 30.

grundsätzlich aus, könnte aber in Betracht kommen, wenn später eine Deanonymisierung durch den externen Datenempfänger ermöglicht würde, was bei anonymen Fallzahlen aber als ausgeschlossen angesehen werden kann.

4.2.1.2 Offenbaren beim Outsourcing: Kenntnisnahme oder Möglichkeit der Kenntnisnahme?

Soweit der automatisierte Prozess jedoch mit noch personenbezogenen Input-Daten arbeitet und (zum Teil) auf einen externen Dienstleister bzw. in eine „Cloud" ausgelagert wird, stellt sich die Frage, ob nicht doch ein Offenbaren im Sinne von § 203 StGB vorliegt. Dies hängt nicht unwesentlich davon ab, ob für eine solche Tathandlung die tatsächliche Kenntnisnahme durch Außenstehende gefordert wird oder die Möglichkeit der Kenntnisnahme ausreicht.

In der strafrechtlichen Kommentarliteratur wird zwar im Ansatz meist ausgeführt, dass ein Geheimnis offenbart wird, wenn es „in irgendeiner Weise an einen anderen gelangt" ist.[141] Letztlich wird aber doch nach der Art der (potenziellen) Mitteilung eines Geheimnisses differenziert. Bei mündlichen Mitteilungen, also flüchtiger Sprache, ist die tatsächliche Kenntnisnahme erforderlich, während bei verkörperten Geheimnissen das Verschaffen des Gewahrsams wie durch Zugang eines Schriftstücks mit der Möglichkeit der Kenntnisnahme genügt.[142]

Persistente Datenweitergabe

Somit reicht bei personenbezogenen Daten, jedenfalls wenn diese wie üblich in Dateiform verkörpert sind, grundsätzlich die bloße Möglichkeit der Kenntnisnahme aus. Demzufolge liegt jedenfalls ein Offenbaren vor, wenn gespeicherte Geheimnisse, etwa auf Datenträger oder durch Datenfernübertragung, weitergegeben werden und persistent, also für eine für den Versender unbestimmte bzw. vom Empfänger bestimmte Dauer, in den Gewahrsam bzw. die faktische Verfügungsgewalt des Letzteren gelangen.[143]

Gewährung von Zugang zum eigenen Computersystem

Das die bloße Möglichkeit der Kenntnisnahme weiter konturierende Erfordernis der Gewahrsamsverschaffung ist allerdings bei der bloßen Gewährung von Zugriffsrechten auf das eigene Computersystem problematisch, solange kein tatsächlicher Zugriff auf personenbezogene Daten durch Außenstehende erfolgt, ein solcher aber möglich ist.

Teils wird argumentiert, dass dem Herumliegenlassen von Patientenakten in eigenen Räumen in der analogen Welt entsprechend die bloße Möglichkeit der Kenntnisnahme digitaler Daten nicht ausreiche, sondern eine tatsächliche Kenntniserlangung oder Gewahrsamsverschaffung durch einen gesonderten Zugriff für ein Offenbaren

141 Lenckner/Eisele, in: Schönke/Schröder, StGB, § 203 Rdnr. 19; Cierniak, in: Joecks/Miebach (Hg.), Münchner Kommentar, StGB, § 203 Rdnr. 52.

142 Lenckner/Eisele, in: Schönke/Schröder, StGB, § 203 Rdnr. 19; Schünemann, in: Leipziger Kommentar, StGB, § 203 Rdnr. 41; Cierniak, in: Joecks/Miebach (Hg.), Münchner Kommentar, StGB, § 203 Rdnr. 52; hierfür spricht auch das Urt. des Reichsgerichts v. 09.07.1917 (V 54/17, RGSt 51, 184, 189) zum Verrat von Geschäftsgeheimnissen nach § 17 UWG, wo deren Übersendung als ausreichend angesehen wurde.

143 Lenckner/Eisele, in: Schönke/Schröder, StGB, § 203 Rdnr. 20 m.w.N.

vorausgesetzt wird. Der Schweigeverpflichtete soll sich auch in dieser Konstellation nur dann strafbar machen, wenn er die erforderlichen Sicherheitsvorkehrungen außer Acht gelassen hat, denn nur dann stehe das Unterlassen der Verhinderung des Zugriffs dem aktiven Offenbaren gleich.[144] Wenn ein Zugriff folglich nur durch objektiv nicht absehbares bzw. nicht mit zumutbaren Mitteln vermeidbares „Hacking" erfolgt, dann liegt nach dieser Ansicht Straffreiheit vor. Falls mit der bewussten Gewährung des Zugangs zum eigenen Computersystem aber bereits technische Zugriffsrechte auf personenbezogene Daten eingeräumt werden, liegt kein solches Hacking vor; hier wird man in der Regel eine Pflicht zur Sicherung vor solchen Zugriffen durch (Live-)Beobachtung oder zumindest Protokollierung der fremden Aktivitäten im eigenen Computersystem annehmen müssen.[145]

Anderen Teilen der rechtswissenschaftlichen Literatur genügt in der analogen wie der digitalen Welt grundsätzlich das Verschaffen der Möglichkeit der Kenntnisnahme für eine Offenbarung – im digitalen Bereich etwa durch Gewährung von Zugriffsrechten für externes Servicepersonal auf die gesamte EDV-Anlage.[146]

Letztlich überzeugen die Argumente der ersten Auffassung für Aufträge zur reinen (Fern-)Wartung von Computersystemen eher. Für diese restriktivere Auslegung spricht auch, dass das in § 203 StGB vorausgesetzte „Offenbaren" eine gewisse Offenkundigkeit des Personenbezugs für den Empfänger nahelegt.[147] Allerdings sollten die technischen Zugriffsrechte auf personenbezogene Daten hierbei auf das absolut notwendige Mindestmaß beschränkt und allgemein Zugriffe überdies so weit wie möglich protokolliert werden. Ein tatsächlicher Zugriff auf personenbezogene Daten verbunden mit deren persönlicher (menschlicher) Kenntnisnahme oder einer Gewahrsamserlangung stellt aber auch hier, wenn er im Rahmen der eingeräumten technischen Rechte und ohne deren Erweiterung durch Hacking erfolgte, ein grundsätzlich strafbares Offenbaren dar, welches nur durch Schweigepflichtentbindung oder gesetzliche Befugnis gerechtfertigt werden kann.[148]

Flüchtige Datenweitergabe

Eine flüchtige Datenweitergabe erfolgt in Konstellationen, in denen personenbezogene Informationen, die Patientendaten oder sonstige durch § 203 StGB geschützte

144 Lenckner/Eisele, in: Schönke/Schröder, StGB, § 203 Rdnr. 20; in der Tendenz auch Schünemann, in: Leipziger Kommentar, StGB § 203 Rdnr. 41; entsprechend zur analogen Welt (bloßes Herumliegenlassen genügt noch nicht): Cierniak, in: Joecks/Miebach (Hg.), Münchner Kommentar, StGB, § 203 Rdnr. 52. Der Schwerpunkt der Vorwerfbarkeit wird dabei nicht im aktiven und bewussten Einräumen von Zugriffsrechten gesehen, sondern in der unterlassenen Verhinderung des tatsächlichen Zugriffs.

145 Vgl. zur Vermeidung von Verletzungen der Privatsphäre nach Art. 8 EMRK in Klinikinformationssystemen durch proaktive Zugriffsrestriktionen oder zumindest retrospektive Zugriffskontrolle über Protokolle: EGMR, Urt. v. 17.07.2008 – Individualbeschwerde Nr. 20511/03, I../. Finnland. Dabei ist allerdings zu berücksichtigen, dass die Gewährung des administrativen Zugangs für Außenstehende die Integrität der Logfiles (Protokolle) gefährdet, da diese mit Administrationsrechten i.d.R. geändert oder gelöscht werden können.

146 Fischer, StGB, § 203 Rdnr. 30a, wenn auch mit der Einschränkung, dass man bei einem allgemeinen Zugang zu sehr „großen Datenbeständen nicht schon eine konkrete Zugriffsmöglichkeit auf jedes einzelne Geheimnis annehmen" könne, wobei dies in Rdnr. 30b gleich wieder mit folgenden Worten relativiert wird: „Wer aus Bequemlichkeit darauf verzichtet, seinen Schreibtisch aufzuräumen oder seinen PC vor Zugriffen zu schützen und die Kenntniserlangung Dritter in Kauf nimmt, offenbart durch Unterlassen". Ehmann, CR 1991, 293, lässt bei Fernwartung von Software uneingeschränkt die bloße Zugriffsmöglichkeit genügen. Entspr. zur analogen Welt (Ermöglichung der Kenntnisnahme seitens unbefugter durch unverschlossenes Liegenlassen von Patientenakten): Lackner/Kühl, StGB, § 203 Rdnr. 17; Ulsenheimer, in: Laufs/Kern (Hg.); Handbuch des Arztrechts, § 66 Rdnr. 9.

147 S. dazu und zum strafrechtlichen Bestimmtheitsgebot auch unten S. 262.

148 Was die IT-Wartung aber auch deutlich erschweren kann, da eine Fehleranalyse nicht selten am effizientesten an gezielten Zugriffen auf konkrete (fehlerbehaftete und z.T. eben personenbezogene) Datensätze ansetzt.

Geheimnisse enthalten, lediglich flüchtig extern technisch verarbeitet werden, nach Ende der Laufzeit des entsprechenden Prozesses aber im externen System (wie einer Cloud) sofort wieder gelöscht werden.[149] Zunächst einmal liegt auch hier im technischen Sinne eine Weitergabe gespeicherter Daten vor, weshalb man von einem Offenbaren ohne tatsächliche Kenntnisnahme ausgehen könnte. Allerdings erfolgt die externe Speicherung oder sonstige Verwendung nur kurzzeitig, also flüchtig, weswegen in Analogie zur mündlichen Mitteilung eine tatsächliche Kenntnisnahme verlangt werden könnte.

Wenn während der Laufzeit des entsprechenden Prozesses Patientengeheimnisse gegen die Kenntnisnahme durch den externen Dienstleister abgeschottet sowie bei Ende der Laufzeit sofort und automatisch gelöscht werden, wobei dieser Prozess vom Schweigeverpflichteten bzw. dessen (internen) Gehilfen beherrscht wird und für den Dienstleister nicht ohne Weiteres manipulierbar ist, erscheint es daher vertretbar, ein Offenbaren zu verneinen. Dies würde auch der oben als vertretbar befundenen datenschutzrechtlichen Bewertung entsprechen, welche eine Datenübermittlung oder sonst rechtfertigungspflichtige Form der Datenweitergabe (insbes. an Auftragsdatenverarbeiter) unter den genannten Bedingungen ablehnt.[150]

Das faktische und damit auch rechtliche Risikopotential erscheint gegenüber der entsprechenden Auffassung bei der Gewährung von Wartungszugriffen jedoch höher, da nicht nur Dienste, sondern auch Daten, wenn auch nur auf kurze Zeit angelegt, „outgesourct" werden und diese eben doch mehr verkörpert sind als das gesprochene Wort. Dies erleichtert eine (sei es auch durch Hacking) angemaßte Kenntnis- oder (persistente) Gewahrsamserlangung durch den Outsourcingnehmer (Auftragsdatenverarbeiter).

Pseudonymisierung/Anonymisierung oder Offenbarungsbefugnisse

Im Sinne der Rechtssicherheit wäre es daher, vor (sei es auch nur kurzeitiger) Auslagerung der Behandlungsdaten auch in dieser Konstellation eine faktische Anonymisierung[151] vorzunehmen oder zulässigerweise auf eine Offenbarungsbefugnis (Einwilligung bzw. Schweigepflichtentbindung oder eine das Behandlungsverhältnis einbeziehende Weitergabeerlaubnis) zu rekurrieren.

Dabei ist jedoch zu beachten, dass eine allgemeine Erlaubnis zur Auftragsdatenverarbeitung wie § 11 BDSG keine gesetzliche Offenbarungsbefugnis darstellt, da das BDSG nach seinem § 1 Abs. 3 S. 2 spezielle Berufsgeheimnisse wie die ärztliche Schweigepflicht unberührt lässt, deren Schutz also nicht verringern, sondern ihn nur ergänzen soll.[152] Demnach ist für das Offenbaren von Patientengeheimnissen neben einer datenschutzrechtlichen Erlaubnis auch eine gesondert zu prüfende Befugnis

149 Als Alternative zur Löschung kommt eine rein Client-basierte Verschlüsselung im externen System in Betracht, also eine solche mit Schlüssel – außerhalb der Laufzeit jedenfalls – ausschließlich in der Hand des Kunden/Schweigeverpflichteten. Problematisch ist hier das Risiko des Abfangens des Schlüssels oder entschlüsselter Daten durch den externen Dienstleister, welches aufgrund der persistenten, wenn auch verschlüsselten externen Speicherung größerer Datenmengen als wohl höher als im Szenario der sofortigen Löschung nach Ende der Laufzeit im externen System eingestuft werden muss.

150 S. oben S. 35, 38f.

151 Zumindest für den Outsourcingnehmer, ggf. durch effektive interne Pseudonymisierung.

152 ULD, Patientendatenverarbeitung im Auftrag, Abschnitt 1. Allg. zu diesem Begründungszusammenhang: Dix, in: Simitis (Hg.), BDSG, § 1 Rdnr. 175ff.

im Sinne des § 203 StGB für die Rechtmäßigkeit einer Datenweitergabe[153] erforderlich (sogenannte Zwei-Schranken-Theorie),[154] welche nicht in den Normen des BDSG gesehen werden kann.[155] Wenn allerdings Erlaubnisnormen anderer Gesetze auch die Weitergabe von Daten aus der durch § 203 Abs. 1 Nr. 1 StGB geschützten Vertrauensbeziehung zwischen Arzt und Patient mit erfassen, dann stellt die datenschutzrechtliche Erlaubnis gleichzeitig eine Offenbarungsbefugnis dar. Letzteres ist unter anderem der Fall bei den speziellen Regelungen zur Auftragsdatenverarbeitung in den Landeskrankenhausgesetzen, worauf später eingegangen wird.[156]

4.2.2 Berufsrechtliche Verschwiegenheitspflicht (§ 9 Abs. 1 MBO-Ä)

Die gleichen Maßstäbe wie zur strafrechtlich sanktionierten Schweigepflicht sind auch an die Verschwiegenheitspflicht entsprechend § 9 Abs. 1 MBO-Ä anzulegen.

4.3 Ergebnis

Automatisierte Auswertungen mit rein anonymen Ergebnissen stellen keine personenbezogene Datenverwendung dar, selbst wenn in den entsprechenden Prozess noch personenbezogene Daten eingestellt werden, dieser aber so abgeschottet abläuft, dass es zu keiner personenbezogenen Datenausgabe kommt. Somit unterliegt dieser Vorgang keinem datenschutzrechtlichen Erlaubnisvorbehalt.

Hilfsweise könnte insbesondere auch im Rahmen der auf eine Einzelfallabwägung abstellenden üblichen Forschungsklauseln argumentiert werden, dass eine zweckändernde Datenverwendung („Sekundärnutzung“) durch solche Auswertungen jedenfalls zulässig ist, da die Betroffeneninteressen hier praktisch kaum berührt werden und die Abschätzung der Machbarkeit einer über Ein- und Ausschlusskriterien bereits konkretisierten Studie ein wichtiger Aspekt effizienter wissenschaftlicher Forschung ist.

Für ein Offenbaren im Sinne der ärztlichen Schweigepflicht ist die Kenntnisnahme oder zumindest die Möglichkeit der Kenntnisnahme eines Patientengeheimnisses durch einen einrichtungsfremden Dritten erforderlich. Eine Verletzung der Schweigepflicht scheidet daher von vornherein aus, wenn der automatisierte Prozess lediglich innerhalb der Behandlungseinrichtung abläuft, selbst dann, wenn es zu einer

153 Darunter ist eine Übertragung im technischen Sinn, nicht zwingend auch eine Übermittlung im datenschutzrechtlichen Sinn (an einen eigenverantwortlichen Dritten) zu verstehen.

154 BGH, Urt. v. 11.12.1991 – VIII ZR 4/91, BGHZ 116, 268, = NJW 1992, 737, Rdnr. 26–28; Dix, in: Simitis (Hg.), BDSG, § 1 Rdnr. 175ff., 186f.; Cierniak, in Joecks/Miebach (Hg.), Münchner Kommentar, StGB, § 203 Rdnr. 51; Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 84ff. Nur einen von mehreren normativen Ansätzen (wenn auch wohl den wichtigsten) stellt dabei § 1 Abs. 3 S. 2 BDSG dar. Eine ausführliche dogmatische Begründung liefert Beyerle, Rechtsfragen medizinischer Qualitätskontrolle, S. 121ff.

155 Nach herrschender Meinung gilt dies auch für die explizit Gesundheitsdaten nach § 3 Abs. 9 BDSG einbeziehenden (Übermittlungs-)Erlaubnisse nach § 28 Abs. 6–8 BDSG (in diese Richtung jeweils in Simitis (Hg.), BDSG: Dix, § 1 Rdnr. 181; Simitis, § 28 Rdnr. 295f.), wovon Abs. 7 sich sogar explizit auf die medizinische Versorgung bezieht, wobei im zuletzt genannten Fall aber auch die datenschutzrechtliche Erlaubnis explizit unter den Vorbehalt der ärztlichen Schweigepflicht gestellt wird (Simitis, a.a.O., § 28 Rdnr. 313ff.). Unter den Datenschutzaufsichtsbehörden eindeutig dieser Auffassung: LfD ST, VIII. Tätigkeitsbericht 2005–2007, Abschnitt 9.2. A.A. (ohne nähere Begründung) Kazemi, VersR 2012, 1492, nach welchem § 28 Abs. 8 BDSG i.d.R. eine gesetzliche Offenbarungsbefugnis nach § 203 StGB darstellt.

156 S. unten S. 259ff.

personenbezogenen Datenausgabe kommen würde, zumindest soweit letztere den Bereich der in die Behandlung involvierten Fachabteilungen nicht überschreitet.[157]

Beim Outsourcing des automatisierten Prozesses auf von anderen Stellen betriebene Rechenzentren muss dieser so abgeschottet sein, dass regelmäßig kein Zugriff dieser Stellen auf personenbezogene Daten möglich ist, sofern solche Daten überhaupt in den Prozess eingestellt werden, damit weder eine rechtfertigungspflichtige Datenübertragung noch ein Offenbaren im Sinne der Schweigepflicht vorliegt. Abschottung bedeutet hier von der Behandlungseinrichtung zu verantwortende programmtechnische Absicherungen gegen einen Zugriff des externen Betreibers auf personenbezogene Input-Daten und/oder Zwischenergebnisse sowie deren sofortige Löschung in den Systemen des Betreibers nach Ablauf des zeitlich begrenzten Prozesses. Rechtssicherer wird es in dieser Konstellation aber sein, sich entweder zulässigerweise auf eine Schweigepflicht-spezifische Offenbarungsbefugnis zu berufen oder aber die Input-Daten vor Weitergabe an den Dritten zu anonymisieren. Die genannte Offenbarungsbefugnis kann sich aufgrund Gesetz, insbesondere bereichsspezifischer Regelungen in den Landeskrankenhausgesetzen, oder aus einer Schweigepflichtentbindung ergeben, wobei beide Befugnisformen regelmäßig auch eine datenschutzrechtliche Erlaubnis darstellen.[158]

157 Weiter als diese Fachabteilungsgrenze, welche nur ausnahmsweise auch für die datenschutzrechtlichen Übermittlungsschranken maßgeblich ist (s.u. S. 255f.), dürfte auch eine eventuelle innerorganisatorische Schweigepflicht nicht gehen.

158 Umgekehrt stellt aber nicht jede datenschutzrechtliche Erlaubnis eine Offenbarungsbefugnis dar. Näheres hierzu oben Abschnitt „Pseudonymisierung/Anonymisierung oder Offenbarungsbefugnisse" in Kap. I.4.2.1.2, S. 50f., und unten zu Frage 5 aus dem Pflichtenheft, s. Kap. I.6, S. 75ff. Die Schweigepflichtentbindung kann zwar grundsätzlich formlos erteilt werden, während die datenschutzrechtliche Einwilligung i.d.R. der Schriftform bedarf. Soweit eine Schweigepflichtentbindung aber wirksam schriftlich erteilt wird, genügt sie üblicherweise auch den Anforderungen an die Einwilligung nach Datenschutzrecht.