**Thilo Weichert**

# Die zentrale Speicherung von Daten der gesetzlichen Krankenversicherung

*Ende 2019 wurde das* Digitale-Versorgung-Gesetz *beschlossen, mit dem unter dem Stichwort* Datentransparenz *auf pseudonymer Basis eine bevölkerungsweite Datenbank mit Gesundheitsdaten u. a. für Forschungszwecke geschaffen wird, ohne dass hinreichende Vorkehrungen für einen datenschutzkonformen Umgang mit den Daten getroffen werden.*

## 1 Gesetzgeber beschließt Gesundheitsdatenbank

Die Empörung vieler Bürgerrechtler war und ist groß: Bundesgesundheitsminister Jens Spahn stellt ein *Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation*, abgekürzt *Digitale-Versorgung-Gesetz*, vor und zieht es durch, so dass es mit wenigen Änderungen Ende 2019 in Kraft tritt[1]: In dem Gesetz ist eine zentrale Speicherung aller Leistungsdaten von gesetzlich Krankenversicherten vorgesehen, also der Gesundheitsdaten von mehr als 70 Millionen Bürgerinnen und Bürger. Das Gespenst der zentralen Speicherung der Daten der Gesetzlichen Krankenversicherung (GKV) einschließlich der elektronischen Patientenakten, mit dem über Jahre hinweg der elektronischen Gesundheitskarte (eGK) und der Telematik-Infrastruktur (TI) das Leben und Entwickeln – zu Unrecht – schwer gemacht wurde, wird plötzlich Realität, wenn auch die Ablage der Daten nicht mit Klarnamen, sondern unter Pseudonym erfolgen soll. Das Bundesgesundheitsministerium (BMG) will mit den Daten „Datentransparenz" herstellen; die pseudonymisierten Datensätze sollen insbesondere in der Gesundheitsforschung genutzt werden können.

Konkret geht es unter der Überschrift *Datentransparenz* um eine Neufassung der §§ 303a-303f SGB V. Dieser zweite Titel des 10. Kapitels des SGB V wurde 2003 eingeführt. Unter der damaligen rot-grünen Bundesregierung sollte – mit aktiver Unterstützung von Datenschützern – eine Datengrundlage geschaffen werden für Zwecke des Risikostrukturausgleichs, aber auch für andere anonyme Auswertungszwecke. Dieses Instrument fristete über viele Jahre hinweg ein Mauerblümchendasein. Das soll sich mit dem Willen der schwarz-roten Regierung und deren Minister Spahn nun grundlegend ändern.

*„Gesundheitsbank" für alle? – Foto: Manfred Antranias Zimmer*

Erst kurz vor der endgültigen Beschlussfassung im Bundestag drang die Relevanz der geplanten Änderung ins öffentliche Bewusstsein. Die Kritik am Regierungsvorschlag führte dazu, dass drei Tage vor der entscheidenden Sitzung im Bundestag als Änderung beschlossen wurde, die Übermittlung durch die Krankenkassen nicht mit dem eindeutig zuordenbaren Versichertenkennzeichen vorzunehmen, sondern unter einem nicht zuordenbaren spezifischen Pseudonym. Mehr an Korrektur schien der Mehrheit nicht nötig. Eine Analyse des nun verabschiedeten Gesetzes zeigt, dass die Gesundheitsdaten der deutschen Bevölkerung künftig nicht gerade frei verfügbar sein werden, dass aber die Sicherung dieser Daten unzureichend ist.

## 2 Das gesetzliche Verfahren der *Datentransparenz*

Gemäß dem neuen Gesetz erfolgt eine massive Ausweitung sowohl des Datensatzes wie auch der möglichen Nutzungen. Der europäische Gesetzgeber hat in der Datenschutz-Grundverordnung (Artikel 9 Absatz 2 lit. i DSGVO) festgelegt, dass die Auswertung zentralisierter Gesundheitsdaten ausschließlich „aus Gründen des öffentlichen Interesses" zulässig ist, etwa zwecks „Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren" oder zur „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten". Auch bei einer Verwendung für wissenschaftliche Forschungszwecke nach Artikel 9 Absatz 2 lit. j DSGVO muss, wenn eine privilegierte Datennutzung erfolgen soll (Artikel 5 Absatz 1 lit. b DSGVO), ein überwiegendes öffentliches Interesse vorliegen.[2] Artikel 9 Absatz 2 lit. i, j DSGVO fordert zudem „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person". Davon ist im nun geltenden DVG nicht viel zu finden.

Zuständig für die Datentransparenz sind eine Vertrauensstelle und ein Forschungsdatenzentrum (früher: Datenaufbereitungsstelle). Die Benennung dieser „öffentlichen Stellen des Bundes" erfolgt per Rechtsverordnung durch das BMG. Sie sind räumlich, organisatorisch und personell eigenständig, d. h. auch voneinan-

der getrennt zu führen und unterliegen der Rechtsaufsicht des BMG (§ 303a Absatz 1, 2 SGB V), das also nur eine Rechtskontrolle durchführen und keine fachlichen Weisungen geben darf. Eine rechtliche Unabhängigkeit hätte man zweifellos klarer und besser ins Gesetz schreiben können.

Die Daten werden von den Krankenkassen über den Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband) zu jedem Versicherten mit einem nur kurzfristig verwendeten „Lieferpseudonym" angeliefert. Der GKV-Spitzenverband prüft die Daten auf Vollständigkeit, Plausibilität und Konsistenz und klärt offene Fragen mit der jeweiligen liefernden Krankenkasse ab und übermittelt dann die Daten incl. Alter, Geschlecht und Wohnort des Patienten, Angaben zum Versicherungsverhältnis sowie den Kosten- und Leistungsdaten nach den §§ 295, 295a, 300, 301, 301a und 302 SGB V an das Forschungsdatenzentrum ohne Lieferpseudonym mit einer Arbeitsnummer. Auch die Angaben zu den Leistungserbringern (also Ärzten, Apotheken usw.) werden vor der Übermittlung pseudonymisiert. Der GKV-Spitzenverband liefert parallel eine Liste der Lieferpseudonyme mit deren Zuordnung zu den Arbeitsnummern an die Vertrauensstelle (§ 303b SGB V).

Bisher stand für den sehr beschränkten Umfang der gesammelten pseudonymen Datensätze der Risikostrukturausgleich (§ 268 SGB V) im Vordergrund. Künftig können grundsätzlich alle Kosten- und Leistungsdaten übermittlungspflichtig gemacht werden. In einer Rechtsverordnung werden Art und Umfang der Daten (Datenfelder und Detailtiefe) bestimmt (§ 303a Absatz 4 Nr. 1 SGB V). Erfasst werden Krankenhausbehandlung (§ 301), ambulante Versorgung (§§ 295, 295a), Arzneimittel (§ 300), Heil- und Hilfsmittel incl. Digitalanwendungen (§ 302), Dienste von Hebammen (§ 301a) und anderen Leistungserbringern (etwa Physiotherapeuten, § 302). Die Ausweitung umfasst nun auch Angaben zu den Leistungserbringern.[3] Bzgl. der Angaben zum Wohnort der Patientinnen und Patienten sollen insbesondere in Großstadtgemeinden und Flächenkreisen Zuordnungen zu Lebens- und Sozialräumen möglich sein. Die Angaben zum Versichertenverhältnis können Angaben zum Versichertenstatus, Vitalstatus einschließlich des Sterbedatums der Versicherten umfassen.[4]

Die Vertrauensstelle überführt die Lieferpseudonyme in periodenübergreifende Pseudonyme, so dass „für das jeweilige Lieferpseudonym eines jeden Versicherten periodenübergreifend immer das gleiche Pseudonym erstellt wird, aus dem Pseudonym aber nicht auf das Lieferpseudonym oder die Identität des Versicherten geschlossen werden kann" (§ 303c Absatz 2). Die Vertrauensstelle übermittelt dann diese Pseudonyme mit den Arbeitsnummern dem Forschungsdatenzentrum und löscht die Lieferpseudonyme, Arbeitsnummern und übermittelten Pseudonyme (§ 303c Absatz 3 SGB). Die Generierung der Pseudonyme wird in einer Rechtsverordnung geregelt (§ 303a Absatz 4 Nr. 3).

Das Forschungsdatenzentrum hat nach § 303d Absatz 1 SGB V die Aufgabe, die angelieferten Daten zu speichern, aufzubereiten und auszuwerten. Dazu gehört die Qualitätssicherung der Daten, die Prüfung von Anträgen auf Datennutzung, das Führen eines Antragsregisters mit Informationen zu den Nutzungsberechtigten incl. Vorhaben und deren Ergebnisse und die Bereitstellung der benötigten Daten an die Nutzungsberechtigten (§ 303e Absatz 1 SGB V). Zudem soll die Stelle das Verfahren evaluieren und weiterentwickeln. Im Rahmen der Antragsprüfung hat das Forschungsdatenzentrum das Reidentifizierungsrisiko bei jeder Datenpreisgabe zu „bewerten und unter angemessener Wahrung des angestrebten wissenschaftlichen Nutzens durch geeignete Maßnahmen zu minimieren" (§ 303d Absatz 1 Nr. 5). Die Speicherdauer ist maximal 30 Jahre (§ 303d Absatz 4). Die Forderung nach einer Verlängerung dieser Aufbewahrungsfristen steht im Raum.[5]

Die Liste der potenziell Nutzungsberechtigten ist lang (§ 303e Absatz 1): GKV-Spitzenverband, Bundes- und Landesverbände der Krankenkassen, Kassenärztliche Bundesvereinigung und Kassenärztliche Vereinigungen, Spitzenorganisationen der Leistungserbringer auf Bundesebene, Stellen zur Gesundheitsberichterstattung (Statistik, Bund und Länder), Einrichtungen unabhängiger wissenschaftlicher Forschung (incl. Hochschulen), gemeinsamer Bundesausschuss (gBA), Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen (IQWiG), Institut des Bewertungsausschusses (InBA), Patienten- und Behindertenbeauftragte (Bund, Länder), Institut für Qualitätssicherung und Transparenz im Gesundheitswesen (IQTIG), Institut für das Entgeltsystem im Krankenhaus (INEK GmbH), oberste Bundes- und Landesbehörden (also z. B. das BMG), Bundeskammern der Ärzte, Zahnärzte, Psychotherapeuten und Apotheker, Deutsche Krankenhausgesellschaft (DKG). Neu ist die Empfangsbefugnis von öffentlich geförderten außeruniversitäten Forschungseinrichtungen, also z. B. der Fraunhofer-Gesellschaft, der Helmholtz-Gesellschaft, der Leibniz-Gemeinschaft sowie der Max-Planck-Gesellschaft.[6]

Als Nutzungszwecke werden in § 303e Absatz 2 aufgeführt: Steuerungsaufgaben durch die Kollektivvertragspartner, Verbesserung der Versorgungsqualität, Planung von Leistungsressourcen (z. B. Krankenhausplanung), Unterstützung politischer Entscheidungen, Analyse und Entwicklung sektorenübergreifender Versorgungsformen und von Krankenkassen-Einzelverträgen, Gesundheitsberichterstattung sowie generell die Forschung.

Für diese Zwecke liefert das Forschungsdatenzentrum Auswertungen „anonymisiert und aggregiert" (§ 303e Absatz 3). Heikel ist, dass das Forschungsdatenzentrum auch pseudonymisierte Einzeldatensätze bereitstellen darf. Dafür muss ein Antragsteller darlegen, dass dies „für einen nach Absatz 2 zulässigen Nutzungszweck, insbesondere für die Durchführung eines Forschungsvorhabens, erforderlich ist". Der Nutzer muss „einer Geheimhaltungspflicht nach § 203 des Strafgesetzbuchs unterliegen" und technisch-organisatorisch gewährleisten, dass Datenminimierung praktiziert wird (§ 303e Absatz 4).

Die Nutzenden sollen auf die Einzeldatensätze nur unter Kontrolle des Forschungsdatenzentrums verarbeiten dürfen, was über einen „Gastarbeitsplatz in den Räumen des Forschungsdatenzentrums oder über einen gesicherten Fernzugriff" stattfinden soll. Die Nutzung der erlangten Daten ist nur zweckgebunden zulässig; die Nutzenden haben „darauf zu achten, keinen Bezug zu Personen, Leistungserbringern oder Leistungsträgern herzustellen" (§ 303e Absatz 5).

§ 303a Absatz 4 ermächtigt das BMG in Abstimmung mit dem Bundesforschungsministerium (BMBF) zum Erlass einer Rechts-

verordnung zwecks Konkretisierung der Verfahren (Datenumfang, Pseudonymisierungsverfahren, Bereitstellung von Einzeldatensätzen, Aufbewahrungsfrist, Evaluation, Weiterentwicklung). Gemäß § 303d Absatz 2 wird ein Arbeitskreis der Nutzungsberechtigten eingerichtet, der „an der Ausgestaltung, Weiterentwicklung und Evaluation des Datenzugangs" beratend mitwirkt.

## 3 Bewertung

Tatsächlich wird im Forschungsdatenzentrum eine zentrale Datensammlung von hochsensiblen Gesundheitsdaten von sämtlichen in Deutschland gesetzlich Versicherten auf- bzw. ausgebaut. Falsch ist, wie von Kritikern manchmal suggeriert wird, dass damit dem Missbrauch Tür und Tor geöffnet wird. Doch trotz der vorgesehenen Vorkehrungen bestehen rechtliche und voraussichtlich auch praktische Defizite. Anders als viele Kritiker halte ich die Nutzung der GKV-Gesundheitsdaten für Forschungszwecke für sinnvoll, wenn diese zur Weiterentwicklung unseres Gesundheitssystems und zum Fortschritt im Bereich der medizinischen Forschung genutzt werden. Ohne valide statistische Daten, die im medizinischen Bereich äußerst differenziert sein müssen, ist eine qualifizierte Gesundheitsberichterstattung nicht möglich.[7] Diese ist nötig als Grundlage für eine gerechte und effiziente staatliche Politik, für die Justierung des Abrechnungssystems sowie für das Erkennen von grundlegenden Entwicklungen und Zusammenhängen.[8]

Eingriffe in das Recht auf informationelle Selbstbestimmung sind aber nur zulässig, wenn diese im überwiegenden Allgemeininteresse erfolgen und hinreichende technisch-organisatorische und verfahrensrechtliche Vorkehrungen getroffen werden.[9]

Im deutschen Datenschutzrecht hatte bisher bei Forschungsnutzungen die Einwilligung absoluten Vorrang.[10] Dem gegenüber sieht Artikel 5 Absatz 1 lit. b DSGVO eine grundsätzliche und generelle Erlaubnis einer Zweitnutzung von personenbeziehbaren Daten für Forschungszwecke vor. Die DSGVO ist erheblich forschungsfreundlicher als das bisherige deutsche Recht, indem sie zwar Garantien für die Betroffenen fordert, nicht aber deren Zustimmung. Damit soll die Repräsentativität von wissenschaftlichen Auswertungen gesichert werden. Auch wenn für einen Ausgleich zwischen Forschungsfreiheit und Datenschutz gemäß der DSGVO eine generelle Widerspruchsmöglichkeit nicht zwingend ist, sind Vorkehrungen zum Betroffenenschutz nötig, etwa eine erhöhte Transparenzpflicht gepaart mit einem projektspezifischen Widerspruchsrecht.[11] Dass den Betroffenen im DVG überhaupt keine Rechte zugestanden werden, ist ein berechtigter Kritikpunkt an den Regelungen zur Datentransparenz.

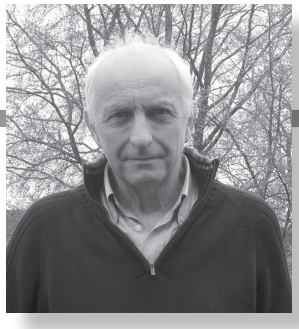
Für die meisten der nutzungsberechtigten Stellen genügen aggregierte, also vollständig anonymisierte Auswertungsergebnisse. Diese Stellen werden im Gesetz mit Forschenden in eine Reihe gestellt, die wichtige Fragestellungen oft nur mit personenbeziehbaren Einzeldatensätzen beantworten können. So öffnet der Gesetzestext die Tür für die Übermittlung von Einzeldatensätze an Stellen, die diese definitiv nicht erhalten sollten.

Das DVG erlaubt nicht nur die aggregierte Datennutzung, sondern auch die Auswertung von Einzeldatensätzen, wenn nachvollziehbar dargelegt wird, dass diese für einen zulässigen Nutzungszwecke erforderlich sind. Die Hürden für die Weiternutzung der Einzeldatensätze sind denkbar niedrig: 1. Die Empfänger müssen einer beruflichen Schweigepflicht unterliegen. 2. Die Datenminimierung muss technisch-organisatorisch abgesichert werden. 3. Es besteht eine gewisse Zweckbindung sowie 4. ein Reidentifizierungsverbot (§ 303e Absatz 4, 5). Eine saubere Abschottung, also eine räumliche, organisatorische und personelle Trennung zwischen der Erfüllung der operativen Aufgaben einer Stelle und der pseudonymen Verarbeitung von Transparenzdaten[12] ist nicht vorgesehen; ebenso fehlen sonstige wirksame Vorkehrungen gegen eine Reidentifizierung der pseudonymen Daten.[13]

Die Sicherheitsvorkehrung, dass eine Auswertung der für den jeweiligen Nutzenden freigeschalteten Einzeldatensätzen nur auf dem IT-System des Forschungszentrums zulässig sein soll, scheint wenig praxistauglich zu sein. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) soll die technische Sicherheit der technischen Analyseplattform des Forschungsdatenzentrums gewährleisten. Wenn Forschende Pseudonymdatensätze nicht mitnehmen können, um sie weiter auszuwerten, dürften sie viele wichtige Fragestellungen nicht oder nur schwer bearbeiten können.

Das Forschungsdatenzentrum hat das „spezifische Reidentifikationsrisiko in Bezug auf die durch Nutzungsberechtigte nach § 303e beantragten Daten zu bewerten" (§ 303d Absatz 1 Nr. 5). D. h. Risikobewertung, Fehler- bzw. Risikobehebung und Evaluation sollen in einer Hand liegen. Dies ist ein Unding. Hier bedarf es der Einschaltung einer unabhängigen Kontrollinstanz. Es ist nicht damit zu rechnen, dass der Verordnungsgeber eine solche künftig vorsehen wird (§ 303a Absatz 4 Nr. 4).

Die Sicherung der Vertraulichkeit über den Verweis auf die berufliche Schweigepflicht ist nicht ausreichend: § 203 StGB hat als



**Thilo Weichert**

Dr. **Thilo Weichert**, Netzwerk Datenschutzexpertise, 2004 bis 2015 *Landesbeauftragter für Datenschutz Schleswig-Holstein*, Vorstandmitglied der *Deutschen Vereinigung für Datenschutz e. V. (DVD)*.

Sanktionsinstrument derzeit in der Praxis keine bzw. nur symbolische Bedeutung; Ermittlungen sind selten; Sanktionierungen sind die absolute Ausnahme.[14]

Für die Datentransparenz sind keinerlei spezifischen Kontrollmechanismen vorgesehen. Dieses Defizit wird auch nicht durch eine verstärkte Datenschutzkontrolle kompensiert. Bei hochsensitiven, zentralisierten hoheitlichen Formen der Datenverarbeitung, die keinen sonstigen öffentlichen Kontrollmechanismen oder einer hinreichenden Transparenz unterliegen, hat das BVerfG gegenüber dem generellen Aufsichtsinstrumentarium verstärkte Maßnahmen gefordert, etwa kontinuierliche Regelkontrollen.[15]

Ungenügend sind auch die vorgesehenen Transparenzmaßnahmen. Das vorgesehene öffentliche Antragsregister (§ 303d Absatz 1 Nr. 6) mit Angaben zu Nutzungsberechtigten, Vorhaben und deren Ergebnissen[16] ist für eine wirksame Hinterfragung ungeeignet, solange nicht erkennbar ist, inwieweit welche Einzeldatensätze von den Nutzenden verarbeitet wurden.

Der Gesetzgeber hat sich nicht an ein Grundsatzproblem herangetraut, indem er es offen lässt, wann ein Forschungsprojekt in den Genuss eines privilegierten Datenzugangs kommen darf. Das BVerfG hat Forschung beschrieben als einen auf wissenschaftlicher Eigengesetzlichkeit (Methodik, Systematik, Beweisbedürftigkeit, Nachprüfbarkeit, Kritikoffenheit, Revisionsbereitschaft) beruhenden Prozess zum Auffinden von Erkenntnissen, ihrer Deutung und ihrer Weitergabe. Wissenschaftliche Forschung ist „alles, was nach Inhalt und Form als ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist".[17] Es gibt in Deutschland aber keine Stelle und kein Verfahren, mit dem diese Anforderungen an privilegierte Forschung festgestellt und überprüft werden. Hierfür bedarf es aber klarer Kriterien, Regeln und Prozesse.[18] Für den Zugang zu den sensitiven GKV-Transparenzdaten verlangt das DVG nicht mehr, als dass die Forschung öffentlich gefördert wird. Dabei handelt es sich ausschließlich um einen finanziellen Aspekt, bei dem der Grundrechtsschutz keine Rolle spielt und ein öffentliches Interesse (der Institution, nicht des konkreten Projekts) allenfalls zu vermuten ist. Aus Sicht des Grundrechtsschutzes ist es nötig, dass Anforderungen an die Unabhängigkeit, die Transparenz, die Sicherungsvorkehrungen und das öffentliche Interesse des konkreten Projektes gestellt werden und diese im Rahmen eines administrativen Vorgangs geprüft, festgestellt und evtl. sanktioniert werden.

## 4 Ergebnis

Das Digitale-Versorgung-Gesetz ist mit seinen Regelungen zur Datentransparenz schlecht gemacht. Es gibt sich zwar nominell Mühe, Vorkehrungen zum Datenschutz zu treffen. Dabei fällt auf, dass vorrangig technische Maßnahmen vorgesehen sind. Das Instrument der Pseudonymisierung wird als Generalwaffe zur Verhinderung des individualisierten Datenmissbrauchs in Stellung gebracht. Für diesen grundsätzlich zu begrüßenden technischen Schutz wird aber kein administrativer Unterbau geschaffen. Pseudonymisierung generell wie im einzelnen Projektfall setzt Kompetenz, Dokumentation, Erprobung und Kontrolle voraus und gibt es nicht zum Nulltarif. Die Reidentifizierung pseudonymer Daten ist mit modernen Methoden der Auswertung oft ein Kinderspiel. Sollte das DVG und dessen Datentransparenz beim Bundesverfassungsgericht oder dem Europäischen Gerichtshof auf den Prüfstand gestellt werden, so dürfte dies schlecht für das Spahn´sche Projekt ausgehen, da die technisch-organisatorischen und prozeduralen Anforderungen ungenügend für den Grundrechtsschutz der GKV-Versicherten sind. Damit wird letztlich dem berechtigten Anliegen, eine bessere Datenbasis für die medizinische Forschung zu schaffen, ein Bärendienst erbracht.

Es ist erschreckend, mit welcher Unkenntnis die Politik mit den Bedürfnissen medizinischer Forschung und des Datenschutzes umgeht. Nicht praktikabel dürfte sich die Nutzung der Datentransparenz für die medizinischen Forschung erweisen, bei der es um ein Verschneiden von Klinikdaten mit GKV-Daten geht. Da das Digitale-Versorgungs-Gesetz nun mal in Kraft ist, muss dessen Umsetzung jetzt aufmerksam, fachkundig und kritisch begleitet werden. An Problembewusstsein hierfür scheint es bei vielen Stellen noch zu fehlen. Letztlich muss aber nicht nur das Bewusstsein der Beteiligten erhöht werden; nötig ist ein völlig neues gesetzliches Austarieren von Forschungsfreiheit und Datenschutz, gerade hier im medizinischen Bereich.

## Anmerkungen

1 *G. v. 09.12.2019, BGBl. I S. 2562.*
2 *Weichert ZD 2020, 20.*
3 *BT-Drs. 19/13438, S. 71.*
4 *BT-Drs. 19/13438, S. 72.*
5 *Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF), Stellungnahme v. 09.10.2019, BT-Ausschuss f. Gesundheit, Ausschussdrucksache 19(14)105(12), S. 5.*
6 *BT-Drs. 19/13438, S. 74.*
7 *Weichert, Big Data im Gesundheitsbereich, 2018, https://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf, S. 45 f., 163 f.*
8 *BVerfG 15.12.1983 – 1 BvR 209/83 u. a. (Volkszählung), Rn. 105, NJW 1984, 423.*
9 *BVerfG 15.12.1983 – 1 BvR 209/83 u. a., LS. 2, NJW 1984, 419.*
10 *Weichert/Bernhardt/Ruhmann, Die Forschungsklauseln im neuen Datenschutzrecht, 18.10.2018, https://www.netzwerk-datenschutz-expertise.de/sites/default/files/gut_2018_forschungklauseln_181018.pdf, S. 5.*
11 *Krawczak/Weichert, DANA 4/2017, 199.*
12 *BVerfG 15.12.1983 – 1 BvR 209/83 u. a., Rn. 109 ff., NJW 1984, 423.*
13 *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Stellungnahme vom 23.10.2019, S. 5.*
14 *Fischer, Strafgesetzbuch, 66. Aufl. 2019, § 203 Rn. 5.*
15 *BVerfG 24.03.2013 – 1 BvR 1215/07, Rn. 116 f. (Antiterrordateigesetz), NJW 2013, 1504.*
16 *Ebenso TMF (En. 5).*
17 *BVerfGE 35, 112 f. = NJW 1978, 1176; Werkmeister/Schwaab CR 2019, 85; Roßnagel, ZD 2019, 158f.; ähnlich Art. 2 lit. b Richtlinie 2005/71/EG des Rates über ein besonderes Zulassungsverfahren für Drittstaatsangehörige zum Zweck der wissenschaftlichen Forschung v. 12.10.2005, zur Erfordernis der Staatsferne Weichert, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990, 231 f.; Britz in Dreier, GG Bd. I, 3. Aufl. 2013, Art. 5 III (Wissenschaft), Rn. 74 f.*
18 *Weichert ZD 2020, 23 f*