Kipker/Schaar: EAID: Vernetzte medizinische Forschung und Datenschutz	ZD-Aktuell 2017, 04263

EAID: Vernetzte medizinische Forschung und Datenschutz

Dr. Dennis-Kenji Kipker ist wissenschaftlicher Geschäftsführer am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen und Mitglied im Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin. Peter Schaar ist Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) und ehemaliger Bundesdatenschutzbeauftragter.

Workshop der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) am 6.7.2017 in der Europäischen Akademie Berlin (EAB): „Vernetzte medizinische Forschung und Datenschutz"

Am 6.7.2017 fand in der *Europäischen Akademie Berlin (EAB)* ein weiterer Workshop der *Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID)* begleitend zum Einführungsprozess der Europäischen Datenschutzgrundverordnung (DS-GVO) statt. Im Mittelpunkt stand dieses Mal das Thema „Vernetzte medizinische Forschung und Datenschutz". Nach einer Begrüßung durch den Vorsitzenden der EAID, *Peter Schaar*, führte der Tagungsleiter *Dr. Alexander Dix* in die Thematik des medizinischen Datenschutzes ein. Die neuen datenschutzrechtlichen Vorschriften der EU verdeutlichten die Notwendigkeit, sich verstärkt dem medizinischen Datenschutz sowie dem Datenschutz in der Forschung mit medizinischen Daten zuzuwenden. Dies nicht zuletzt auch deshalb, weil zahlreiche Vorschriften in diesem Bereich in ihrer konkreten Anwendung noch unklar seien, was zu Schwierigkeiten bei deren praktischer Umsetzung führen könne.

Den einführenden Vortrag der Veranstaltung hielt *Irene Schlünder*, wissenschaftliche Referentin, von der Geschäftsstelle „Technologie- und Methodenplattform für die vernetzte medizinische Forschung" (TMF) e. V., Berlin, zum Thema „Datenschutz in medizinischen Forschungsprojekten". Einleitend stellte sie zunächst den von der *TMF* erarbeiteten selbstregulierenden Ansatz des Leitfadens zum Datenschutz in medizinischen Forschungsprojekten sowie die Arbeit der *AG Datenschutz* bei der *TMF* vor. Die *AG Datenschutz* bewerte für spezielle Forschungsvorhaben, ob deren datenschutzrechtliches Vorgehen den Anforderungen des Leitfadens entspreche. Zudem bestehe ein Beratungsangebot der *AG Datenschutz*. Die medizinische Forschung ließe sich in vier Bereiche untergliedern, deren Probleme und Herausforderungen *Schlünder* im Einzelnen vorstellte: Versorgungsnahe klinische Forschung, kontrollierte klinische Studien, patientenferne Forschung und Biobanken. Hierauf basierend sei auch das Datenschutzkonzept des Leitfadens entwickelt worden, das auf einem modularen System aufbaue, welches sich wiederum aus vier Einzelmodulen zusammensetze: Im klinischen Modul stehe die Behandlung im Mittelpunkt. Für die Forschung mit Patientendaten würden identifizierende Daten der Patienten noch im Krankenhaus von den zu beforschenden Daten getrennt, sodass sich der Zugriff für wissenschaftliche Zwecke auf pseudonymisierte Datensätze beschränke. Ein solches Konzept habe sich noch nicht in allen Krankenhäusern in Deutschland durchgesetzt. Im Studienmodul würden die Daten sogleich pseudonym erfasst, derselbe Grundsatz finde sich auch im Forschungsmodul, bei dem es um die Langzeitspeicherung von Daten und um die Herausgabe von Patientendaten an verschiedene Forschungsprojekte gehe. Von zentraler Bedeutung sei das Identitätsmanagement, also der Umgang mit den Daten, die eine direkte oder indirekte Zuordnung der Forschungsdaten zu

einzelnen Personen ermöglichten. I. E. sei festzustellen, dass die Pseudonymisierung in der medizinischen Forschung immer wichtiger werde, wohingegen die Anonymisierung an Bedeutung verliere, weil zu vielen Forschungszwecken die mögliche Identifizierung des Patienten immer noch erforderlich sei. Das vierte Modul des von der *AG Datenschutz* entwickelten Datenschutzkonzepts in der medizinischen Forschung sei das Biobankmodul, welches sich inhaltlich vornehmlich mit Labor- und Genomdaten befasse. Hier stellte *Schlünder* die Frage, ab wann einzelne Abschnitte eines Genoms personenbezogene Daten sind. Das TMF-Datenschutzkonzept erfordere zudem klare Verantwortlichkeiten: Eine juristische Person als verantwortliche Stelle müsse festgelegt werden, die Verantwortungsbereiche zentraler und dezentraler Stellen seien zu klären, insbesondere bei Förderprojekten müsse frühzeitig auch an die Rechtsnachfolge gedacht werden. Für künftige, heute noch nicht absehbare Forschungsprojekte sei nach Auffassung von *Schlünder* die datenschutzrechtliche Einwilligung zudem an besondere Anforderungen zu knüpfen, die den Zweckbindungsgrundsatz berücksichtigten. Hierzu stellte die *Referentin* die Lösung einer „abgestimmten Einwilligungserklärung" vor, innerhalb derer das Prinzip der Datenweitergabe von vornherein festgelegt sei und eine verbindliche Vereinbarung mit dem Empfänger getroffen werde, sodass dieser keine Dauerspeicherung von Daten „auf Vorrat" über das konkrete Forschungsvorhaben hinaus und ebenso keine Reidentifizierungsversuche betreibt.

Den zweiten Vortrag hielt *Martin Peuker*, Chief Information Officer bei der Charité Universitätsmedizin Berlin. *Peuker* referierte über den Einsatz von Datenbanktechnologien in der medizinischen Forschung und in der Therapie. Die IT-Infrastruktur der *Charité* umfasse insgesamt 12.000 PCs und über 2.000 Serversysteme, wobei ein Nutzerzugriff von über 13.000 Personen täglich erfolge. Die IT-Strategie des Klinikums verfolge einen zweigeteilten Ansatz, der sich in „Digital" (papierlos, elektronische Patientenakte, etc.) sowie „Mobil" (wichtige Informationen orts- und zeitunabhängig) untergliedere. Das Thema Datenschutz und IT-Sicherheit werde dabei bis in die Vorstandsebene des Krankenhausbetriebs eingeführt. Die Datenbanktechnologie der *Charité* basiere auf einer technischen Plattform, welche die schnelle Transformation und Extraktion von Daten ermögliche. Dabei werde versucht, sämtliche Krankenhausprozesse auf die Datenbanktechnologie zu stützen. Im Hinblick auf die Verwendung medizinischer Daten für Forschungszwecke messe die *Charité* der Berlin Health Data Platform zentrale Bedeutung zu, die das gewünschte enge Zusammenspiel von Forschung und Klinik koordinieren soll. Grundlage der Plattform sei ein dreiphasiges IT-Infrastrukturmodell. Die klinischen, aus Krankenhausinformationssystemen stammenden Daten sollen in einer gesicherten klinischen Domäne, dem Plain Data Repository (PDR), zusammengeführt werden. Für Forschungszwecke sollen im PDR gespeicherte Daten in ein Science Data Repository (SDR) überführt werden. Dabei würden die Daten anonymisiert bzw. pseudonymisiert. Dies erfolge unter Kontrolle eines Trustcenter. Der Forschungszugriff solle sich auf die anonymisierten bzw. pseudonymisierten Daten beschränken. Eine in Einzelfällen erforderliche De-Pseudonymisierung von Forschungsdaten für klinische Zwecke solle nur unter Einschaltung des Trustcenter möglich sein.

Dr. Annette Reinecke, Geschäftsführerin des TumorZentrums Berlin (TBZ) e. V., referierte über Fragen des datenschutzkonformen Umgangs mit Patientendaten im *TBZ*. Das *TBZ* verfolge das Ziel, eine neutrale Kooperationsplattform zum Austausch aller onkologischen Abteilungen und Kliniken in Berlin zu schaffen. Hierzu würden interdisziplinäre Projektgruppen und Qualitätszirkel mit Patientenbeteiligung angeboten, ebenso Fortbildungen, Schulungen und Veranstaltungen für Ärzte, Patienten sowie für medizinisches Fachpersonal. Derzeit würden die Daten aus fünf

onkologischen Datenbanken der Stadt zusammengeführt. Datenschutzrechtliche Anforderungen hätten zunächst zu einem erheblichen Mehraufwand bei der i. R. d. Dublettenbereinigung zum Ausschluss von Mehrfachmeldungen aus mehreren Krankenhäusern stammenden Meldungen geführt. Auf Grund der geringen Anzahl der Mehrfachmeldungen werde inzwischen jedoch auf den aufwändigen Abgleich der Identifizierungsdaten verzichtet. Die Zusammenarbeit mit den Kliniken sei schwieriger geworden, da sich nach Einführung verbindlicher Datenschutzstandards verschiedene Krankenhäuser zwischenzeitlich nicht mehr an der Kooperationsplattform beteiligt hätten. Das auf Grund gesetzlicher Vorgaben im Jahr 2016 aufgebaute gemeinsame Krebsregister von Berlin und Brandenburg beziehe sämtliche an der onkologischen Behandlung beteiligten Akteure ein. Die Vorteile eines solchen gemeinsamen klinischen Krebsregisters lägen im Wegfall der zuvor bestehenden Dublettenprobleme wie auch in der gesetzlichen Verpflichtung, den Vitalstatus einmal jährlich zu melden. Mittlerweile sei durch das *TBZ* zudem ein webbasiertes Nachsorge-Tool eingerichtet worden, das den Patienten auf der Basis seiner datenschutzrechtlichen Einwilligungserklärung regelmäßig an die Eintragung seiner Vitalparameter im Nachgang an die onkologische Behandlung erinnere.

Anschließend referierte *Torben Herber*, Unabhängiges Landeszentrum für Datenschutz (ULD) Kiel, über das Forschungsprojekt PARADISE, das einen datenschutzgerechten Ansatz bei der Dopingbekämpfung zum Gegenstand hat. Zunächst stellte er das gegenwärtige Verfahren der *Welt-Anti-Doping-Agentur (WADA*) zur Durchführung von Dopingtests dar. In dessen Zentrum stehe die Datenbank ADAMS, ein internationales Online-Meldesystem, das auch von der deutschen *Nationalen Anti-Doping-Agentur (NADA)* verwendet werde. Zehntausende Spitzensportler müssten ihre sämtlichen Aufenthaltsorte („WhereAbouts") in ADAMS eintragen, für jeden Tag, drei Monate im Voraus. Jeder Standortwechsel, jede Übernachtung und jede Reise müssten angegeben werden und blieben dauerhaft gespeichert. Anhand dieser Informationen führten Kontrolleure unangekündigte Dopingtests durch, bei denen sie die Athleten außerhalb von Wettkämpfen aufsuchten. Die so entstandene umfassende Datenbank ermögliche Rückschlüsse auf sensibelste Daten, etwa zur Religionszugehörigkeit, zu medizinischen Behandlungen und zu Liebesbeziehungen. Das vom BMBF geförderte und vom ULD zusammen mit Partnern aus Wirtschaft und Wissenschaft entwickelte Alternativmodell PARADISE solle die Aufenthaltsdaten auf einen Bruchteil der jetzigen Menge reduzieren. Es folge dem von den deutschen Datenschutzbehörden favorisierten „Standard-Datenschutz-Modell" und gestatte ein differenziertes Management der WhereAbouts. Ausgangspunkt sei ein GPS-Sender, den die Sportler mit sich führten. Die Aufenthaltsbestimmung durch die Anti-Doping-Agenturen erfolge nach einem abgestuften Modell mit differenziertem Genauigkeitsgrad, wobei der Zugriff auf die genauen Koordinaten nur dem für den jeweiligen Test zuständigen Kontrolleur möglich sei. Die WhereAbouts würden – ebenso wie die Ergebnisse der Tests und andere sensible Daten der Sportler – verschlüsselt in einer geschützten Cloud-Plattform gespeichert, auf die nur Berechtigte im Rahmen konkreter Aufträge zugreifen könnten. Wegen der jederzeitigen Ortungsmöglichkeit könnten die derzeitigen umfassenden Vorab-Speicherungen der WhereAbouts entfallen. Durch ein Logging-System sei es zudem nachprüfbar, wer wann auf welche personenbezogenen Daten zugegriffen habe.

Das letzte Referat des Tages hielt *Dr. Katrin Schaar*, Max-Planck-Institut für Bildungsforschung, Berlin und Projektkoordinatorin „Datenschutzkonforme Probandendatenbank MPG". Sie referierte über die datenschutzrechtlichen Anforderungen an die Verwendung von Gesundheitsdaten in der Forschung. Ausgehend von der wachsenden Bedeutung von Gesundheitsdaten für die medizinische, genetische und sozialwissenschaftliche Forschung

erläuterte sie den durch die DS-GVO gesetzten rechtlichen Rahmen. Medizinische Daten seien als „besondere Kategorien personenbezogener Daten" besonders schutzwürdig. Art. 89 DS-GVO enthalte allerdings recht weitgehende Ausnahmen für die Verarbeitung für Forschungszwecke. Zur Kompensation der damit einhergehenden Risiken müssten jedoch zusätzliche Maßnahmen ergriffen werden. Neben der Verschlüsselung und Anonymisierung komme auch die Pseudonymisierung in Frage. Nach wie vor komme der Einwilligung bei der Verarbeitung für Forschungszwecke erhebliche Bedeutung zu. Neu sei allerdings die Möglichkeit zur Einholung eines „Broad Consent", mittels dessen der Proband in „bestimmte Bereiche wissenschaftlicher Forschung" einwilligen könne, sofern anerkannte forschungsethische Standards eingehalten würden. Auch für die Betroffenenrechte auf Information, Auskunft, und Löschung bestünden bei der Forschung besondere Bedingungen. Die DS-GVO erlaube hier ausdrücklich Ausnahmen im nationalen Recht, wenn die wissenschaftlichen Zwecke sonst nicht erreicht werden könnten. Der Bundesgesetzgeber habe hiervon bei der gerade beschlossenen Neuformulierung des BSDG ausgiebig Gebrauch gemacht. Nach der deutschen Regelung sei die Einschränkung der Rechte zulässig, wenn die Verwirklichung der Forschungs- und Statistikzwecke ansonsten unmöglich oder zumindest stark beeinträchtigt würde. Kritisch sah es die *Referentin*, dass die Verarbeitung von sensiblen Daten zu Forschungszwecken auch ohne Einwilligung zulässig würde, wenn die Interessen des Verantwortlichen die der betroffenen Person erheblich überwögen. Diese Bestimmung sei stark interpretationsbedürftig und entbehre einer europarechtlichen Grundlage. Abschließend gab die *Referentin* Empfehlungen für den datenschutzgerechten Umgang mit Forschungsdaten. Neben den rechtlichen Vorgaben müssten auch die entsprechenden Ethikanforderungen beachtet werden.

Diskussion

In der lebhaften Diskussion zwischen den Vorträgen und im Anschluss der Veranstaltung offenbarten sich mehrere zentrale Themen. Immer wieder wurde problematisiert, wo die Grenzen zwischen personenbezogenen und anonymen Daten verlaufen. Immer größere Datenmengen und neue Auswertungskonzepte (Big Data) stellten das Konzept der „faktischen Anonymität" in Frage, das auch der DS-GVO zu Grunde läge. Die in Biobanken aufbewahrten Präparate und vollständig sequenzierte Genomdaten seien stets personenbezogen. Dagegen könnten genetische Teilsequenzen durchaus anonym verarbeitet werden, soweit sie keinen Rückschluss auf eine Person zuließen. Angesichts der technischen Möglichkeiten stießen Anonymisierungskonzepte im Forschungsbereich an ihre Grenzen. Von zunehmender Bedeutung seien hingegen die Pseudonymisierung und die Abschottung von Identifikations- und Inhaltsdaten. Stärkere Beachtung verdiene auch die Frage, für welche Zwecke personenbezogene Daten genutzt würden. Einvernehmen bestand darüber, dass der Datenschutz nicht als Hindernis für die Forschung gesehen werden dürfe, sondern die Vertrauensbasis für den wissenschaftlichen Umgang mit personenbezogenen Daten stärken könne.