DuD
Datenschutz und Datensicherheit

Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten

Marian Arning, Nikolaus Forgó, Tina Krügel

Die Verfasser setzen sich mit der Frage auseinander, unter welchen Voraussetzungen sich eine für eine Verarbeitung personenbezogener Daten verantwortliche Stelle das für eine Deanonymisierung erforderliche Zusatzwissen zurechnen lassen muss und unterbreiten hierzu einen Defintionsvorschlag.

Dipl. Jur. Marian Arning, LL.M.

Institut für Rechtsinformatik, Universität Hannover, www.iri.uni-hannover.de

E-Mail: arning@iri.uni-hannover.de

Prof. Dr. Nikolaus Forgó

Institut für Rechtsinformatik, Universität Hannover, www.iri.uni-hannover.de

E-Mail: forgo@iri.uni-hannover.de

Dr. Tina Krügel, LL.M.

Institut für Rechtsinformatik, Universität Hannover, www.iri.uni-hannover.de

E-Mail: kruegel@iri.uni-hannover.de

1 Einführung

Wird in der Medizin humangenetische Forschung betrieben, liegt die datenschutzrechtliche Brisanz auf der Hand: Die genetische Information eines Menschen gibt Auskunft über seine Abstammung, die ethnische Herkunft, mit einer gewissen Wahrscheinlichkeit auch über zukünftige Erkrankungen, möglicherweise auch über deren Heilungschancen und vieles mehr. Sie ist einzigartig und kann sogar für Blutsverwandte (die noch gar nicht geboren sein müssen) aussagekräftig sein. Die Verarbeitung dieser hochsensiblen personenbezogenen Daten verlangt daher in besonderem Maße die strikte Einhaltung geltender Datenschutzbestimmungen. Gleichzeitig sind die Datenschützer aufgerufen, den Wissenschaftlern einen gangbaren Weg zu weisen, der humangenetische Forschung im Rahmen der vom Gesetzgeber gesetzten Grenzen nicht behindert, sondern ermöglicht.

Der Beitrag befasst sich mit datenschutzrechtlichen Besonderheiten genetischer Daten und hier mit der Frage, ob und gegebenenfalls in welcher Form humangenetische Daten anonymisiert werden können. Er ist motiviert durch das EU – Forschungsprojekt ACGT (Advancing Clinico-Genomic Trials on Cancer), das sich zum Zwecke der Erforschung besserer und effektiverer Heilungsmöglichkeiten mit dem Aufbau einer intereuropäischen Krebsgenomdatenbank beschäftigt.[1] Die Verfasser sind im Rahmen dieses Projektes für rechtliche, insbesondere datenschutzrechtliche, Belange verantwortlich.

2 Verarbeitung genetischer Daten

Genetische Daten sind alle Daten über die Erbmerkmale einer Person oder über das für diese Merkmale typische Vererbungsmuster innerhalb einer miteinander verwandten Gruppe von Personen.[2] Die Verarbeitung von genetischen Daten wirft datenschutzrechtlich eine Reihe von Schwierigkeiten auf.

Zunächst sind genetische Daten aufgrund ihrer Aussagekraft hinsichtlich Gesundheitszustand, Herkunft und Abstammung als hoch sensibel einzuschätzen. Das europäische Datenschutzrecht zählt Daten über die Gesundheit, zu denen die genetischen Daten gehören,[3] daher folgerichtig auch zu den besonders schutzwürdigen Daten (vgl. Art. 8 Abs. 1 DSRL).[4] Die Verarbeitung dieser Daten ist nur unter engen Voraussetzungen möglich.

Die wohl relevanteste Ausnahme zu dem Verarbeitungsverbot von sensiblen Daten stellt die ausdrückliche Einwilligung der betroffenen Person in die jeweilige Verarbeitung dar (Art. 8 Abs. 2 lit. a). Für die Forschung mit genetischen Daten ist die Einwilligung des betroffenen Patienten jedoch nicht unproblematisch: Eine Einwilligung für jeden einzelnen Datenverarbeitungsvorgang in einem Forschungsprojekt einzuholen, ist praktisch unmöglich. Wird die Einwilligungserklärung des Betroffenen

[1] http://www.eu-acgt.org.

[2] Artikel 29 Datenschutzgruppe, Arbeitspapier über genetische Daten, S. 4, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp91_de.pdf.

[3] Ausführlich hierzu Schladebach, Genetische Daten im Datenschutzrecht, CR 2003, 225, 227; Weichert in: Kilian / Heussen (Hrsg.): Computerrechts-Handbuch, München 2006, Nr. 137 Rn. 28; Artikel 29 Datenschutzgruppe: Arbeitspapier über genetische Daten, S. 6, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp91_de.pdf; differenziert: Antonow, Der rechtliche Rahmen der Zulässigkeit für Biodatenbanken zu Forschungszwecken, Baden-Baden 2006, S. 84, die zwischen genetischen Informationen den Gesundheitszustand betreffend (dann sensibel i.S.d. Art 8 DSRL) und solchen, die die Haarfarbe, Augenfarbe und das Geschlecht betreffen (dann keine sensiblen Daten) unterscheidet.

[4] Europäische Datenschutzrichtlinie 95/46 EG.

deshalb sehr weit gefasst, um möglichst viele Datenverarbeitungsvorgänge zu erfassen, ist deren rechtliche Zulässigkeit zumindest zweifelhaft, da sich im Projektverlauf i.d.R. neue Forschungsmethoden ergeben und neue Partner hinzukommen. Fasst man sie hingegen enger, wären neue Forschungsmethoden beispielsweise nicht erfasst, müssten auch nach Jahren neue Einwilligungen von den betroffenen Patienten eingeholt werden. Der damit verbundene organisatorische Aufwand und die sich hieraus ergebenden rein praktischen Probleme (ist der Patient noch einwilligungsfähig?) liegen auf der Hand. Der medizinische Fortschritt und die Heilungschancen der Patienten wären letztlich gefährdet.

Weitere möglicherweise einschlägige Ausnahmen für die Forschung mit genetischen Daten finden sich in Art. 8 Abs. 3 und Abs. 4 DSRL. Nach Abs. 3 dürfen die Mitgliedstaaten die Verarbeitung sensibler Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung bzw. Behandlung und der Verwaltung von Gesundheitsdiensten erlauben, soweit die Verarbeitung durch Personen erfolgt, die der ärztlichen Schweigepflicht oder einer entsprechenden Geheimhaltungsverpflichtung unterliegen. Nach Art. 8 Abs. 4 DSRL können die Mitgliedstaaten vorbehaltlich angemessener Garantien bei wichtigen öffentlichen Interessen, wie z.B. der wissenschaftlichen Forschung i.S.d. Erwägungsgrundes (34) DSRL, weitere Ausnahmen von dem Verarbeitungsverbot sensibler Daten vorsehen.

Gem. Art. 6 Abs. 1 lit. e DSRL gilt grundsätzlich, dass genetische Daten, sobald es der Forschungszweck zulässt, zu anonymisieren sind, das heißt, dass die betroffene Person nicht mehr identifizierbar sein darf (vgl. EG (26)).[5] Ist eine Anonymisierung der Daten einmal erfolgt, besteht für die betroffene Person kein Schutzbedürfnis mehr, da ein Rückschluss auf ihre Identität nicht mehr möglich ist, indem der Personenbezug der Daten aufgehoben wurde. Da die Verarbeitung anonymer Daten folglich für die betroffenen Personen den weitaus besten Schutz bietet, ist ihr auch gegenüber den möglicherweise einschlägigen Ausnahmen zum Verarbeitungsverbot nach Art. 8 DSRL Vorrang zu gewähren. Deswegen muss bei Planung einer Datenverarbeitung von genetischen Daten sorgfältig erwogen werden, ob eine anonymisierte Datenverarbeitung möglich ist. In diesem Fall ist es dann nicht mehr erforderlich, über eine Einwilligung der betroffenen Person zu verfügen, da der Anwendungsbereich der Datenschutzrichtlinie gar nicht eröffnet ist.[6] Der Verarbeitung anonymer Daten sind demnach datenschutzrechtlich keine Grenzen gesetzt. Sie können zumindest aus datenschutzrechtlicher Sicht mangels Personenbezug beliebig gesammelt, gespeichert und veröffentlicht werden.[7]

3 Faktische Anonymisierung genetischer Daten

Für die medizinische Forschung sind anonymisierte Daten in vielen Fällen jedoch wenig hilfreich. Um den Krankheitsverlauf eines Patienten verfolgen und um ihm erforschte Heilbehandlungen zugute kommen lassen und seine Reaktion auf die Behandlung beurteilen zu können, muss der Patient identifizierbar bleiben. Aus diesem Grund wird im Forschungsbereich, soweit der direkte Personenbezug für die jeweilige Verarbeitung nicht unerlässlich ist, vornehmlich mit Pseudonymen[8] gearbeitet, das heißt mit Kennzeichen, die mit dem entsprechenden Schlüssel nach wie vor eine Identifizierung zulassen.

Zudem zeigen die hier untersuchten genetischen Daten eine weitere Besonderheit: Man stelle sich vor, dass eine für die Identifizierung einer Person ausreichend große Gensequenz ohne jeden weiteren Personenbezug im Rahmen einer Studie über das HIV-Virus im Internet veröffentlicht wird. Ist die genetische Information dieser Person in anderem Zusammenhang bereits als Referenzdatensatz gespeichert, sei es im Rahmen eines flächendeckenden Speicheltests oder als Voraussetzung für eine Lebensversicherung mit hoher Deckungssumme,[9] wäre für alle Personen, die Zugriff auf diese Datenbanken haben, nunmehr eine Identifizierung der betroffenen Person und seiner HIV-Erkrankung im Wege eines Matchingverfahrens möglich. Zwar mag dieses Szenario nicht unmittelbar bevorstehen, doch zeigt es, dass die Einzigartigkeit von genetischen Daten das Problem mit sich bringt, dass trotz umfassender Anonymisierung mit entsprechendem Zusatzwissen grundsätzlich ein Rückschluss auf die jeweilige Person möglich bleibt.[10] Ist dies der Fall, stellt sich die Frage, ob genetische Daten überhaupt im Sinne des Datenschutzrechts anonymisiert werden können oder grundsätzlich als personenbezogene Daten einzustufen sind.[11]

Die europäische Datenschutzrichtlinie definiert anonymisierte Daten in einem Erwägungsgrund als Daten, *die eine Identifizierung der betroffenen Person nicht mehr zulassen.*[12] Nach dem Wortlaut der europäischen Normgebung sind mithin nur solche Daten als anonym einzuordnen, deren Anonymisierung irreversibel erfolgt ist, ein Rückschluss auf die Person also für jedermann dauerhaft ausgeschlossen ist.

Die deutsche Umsetzung der Richtlinie hat hingegen eine weiter gefasste Definition statuiert. Diese Definition ist angelehnt an die Definition im ersten Kommissionsvorschlag zur Datenschutzrichtlinie.[13] Nach § 3 Abs. 6 Bundesdatenschutzgesetz (BDSG) sind personenbezogene Daten anonymisiert, die derart verändert worden sind, *dass die*

[5] Im BDSG ist diese Pflicht für wissenschaftliche Forschung in § 40 Abs. 2 S. 1 geregelt.

[6] Vgl. EG (26) S. 2 DSRL. Anders hinsichtlich des Löschens des Personenbezuges, dieses stellt noch ein Verarbeiten i. S. d. BDSG dar.

[7] Weichert, Thilo: Rechtsquellen und Grundbegriffe, in: Kilian / Heussen (Hrsg.): Computerrechts-Handbuch, München 2006, Nr. 131 Rn. 59.

[8] Im Gegensatz zur europ. Gesetzgebung wird „pseudonymisieren" in § 3 lit. 6 a BDSG legal definiert.

[9] Die Verwendung bzw. Einforderung genetischer Untersuchungen in Arbeits- und Versicherungsverhältnissen kann nicht mehr als Schreckgespenst abgetan werden, sie ist bereits beispielsweise in den USA und England in bestimmten Bereichen Realität, vgl. Weichert, DuD 2002, 133, 134.

[10] Weichert, DuD 2002, 133, 134.

[11] Genau genommen stellt sich diese Problematik auch nicht nur bei genetischen Daten. Es wird vielmehr bereits seit Anfang der 80er Jahre daraufhin gewiesen, dass sich das Vorhandensein von personenbezogenen Daten und absoluter Schutz vor einer Deanonymisierung gegenseitig ausschließen. Eine scharfe Trennung zwischen personenbezogenen und anonymen Daten für einen bestimmten Datenbestand sei daher a priori nicht möglich. Die Einordnung hänge vielmehr von dem konkreten Umfeld ab.
Vgl. hierzu Brennecke, Kriterien zur Operationalisierung der faktischen Anonymisierung, in: Kaase u.a., Datenzugang und Datenschutz, Königstein 1980, S. 158, 159; Burkert, Das Problem des Zusatzwissens, in: Kaase u.a. (Fn. 11). S. 143; Gebhardt, Anonymisierung als Weg aus der Mitbestimmung bei elektronischer Datenverarbeitung gemäß § 87 I Nr. 6 BetrVG?, NZA 1995, S. 103, 108.

[12] Erwägungsgrund 26 der DSRL 95/46 EG.

[13] Art. 2 lit. b Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten vom 18.7. 1990.

Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Das BDSG kennt mithin zwei Gruppen von anonymen Daten: erstens Daten, bei denen eine Deanonymisierung vollständig ausgeschlossen ist und zweitens Daten, bei denen eine Deanonymisierung einen unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft erfordern würde, die mithin faktisch anonym[14] sind.

Da sich genetische Daten, wie bereits erwähnt, durch ihre Einzigartigkeit auszeichnen und eine Identifikation der betroffenen Person daher theoretisch bei entsprechendem Aufwand immer möglich ist, können genetische Daten dem Wortlaut nach nur im Sinne der deutschen Definition anonymisiert werden. Trotzdem scheint die Anonymisierung von genetischen Daten auch auf europarechtlicher Ebene möglich, akzeptiert und unbeanstandet zu sein. So sieht beispielsweise die Artikel 29 Datenschutzgruppe gerade in der Anonymisierung von genetischen Daten, die sich dem Wortlaut der Datenschutzrichtlinie nach gar nicht anonymisieren lassen, eine Möglichkeit, das Gefahrenpotential genetischer Forschung einzugrenzen.[15] Auch ist die deutsche Umsetzung der Richtlinie im Hinblick auf die Definition anonymer Daten, soweit ersichtlich, europarechtlich nie beanstandet worden. Im Gegenteil: Bewertete der Wirtschafts- und Sozialausschuss die Streichung des „unverhältnismäßig großen Aufwandes" aus dem Richtlinienvorschlag noch als positiv, da die jetzige Definition von anonymen Daten in der DSRL die Tragweite der Definition begrenze und der Begriff „unverhältnismäßig großer Aufwand" im Bereich der EDV aufgrund der rasanten Entwicklung verfehlt sei,[16] zeigt sich mittlerweile ein Wandel dieser Sichtweise. So stellt die Kommission in ihrem ersten Bericht über die Durchführung der Datenschutzrichtlinie[17] fest, dass die Auslegung der Richtlinie vernünftig und flexibel zu erfolgen habe und verweist in diesem Zusammenhang explizit auf einen Beitrag des European Privacy Officers Forum (EPOF)[18], in dem gerade die deutsche Definition des Anonymisierens als praxisnah und vorbildlich hervorgehoben wird.

4 Zurechenbares Zusatzwissen

Obwohl der Wortlaut des EG (26) DSRL es nicht unmittelbar nahe legt, ist nach heutigem Verständnis folglich davon auszugehen, dass auch nach der europäischen Datenschutzrichtlinie Daten, deren Deanonymisierung zwar möglich, aber nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft durchführbar ist, als anonym bewertet werden können.[19] Es stellt sich weiter die Frage, auf welchen Personenkreis bei der Bewertung des unverhältnismäßigen Aufwands abzustellen ist. Mit anderen Worten: Können genetische Daten für einen Forscher anonym, für einen anderen aber personenbezogen sein; ist bei der Bewertung des unverhältnismäßigen Aufwandes auf die jeweilige verantwortliche Stelle oder auf jede beliebige dritte Person abzustellen?

Die europäische Datenschutzrichtlinie führt hierzu in EG (26) aus: „Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von den Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen." Allerdings wird darauf hingewiesen,[20] dass nach dieser Sichtweise ein Restrisiko der Deanonymisierung immer bestünde, weshalb in der Literatur zum BDSG inzwischen ganz überwiegend eine neuere Ansicht vertreten wird.[21] Diese Sichtweise hält es trotz EG (26) für maßgeblich, ob die Deanonymisierung für die verantwortliche Stelle möglich ist. Ausgangspunkt ist hiernach, dass für denjenigen, der über das zur Identifikation erforderliche Zusatzwissen verfügt, die betroffene Person bestimmbar ist, für diejenigen, die keinen Zugang zu diesem Wissen haben, aber nicht. Der Begriff des personenbezogenen Datums sei daher relativ.[22]

Erkennt man an, dass der Begriff des personenbezogenen Datums relativ ist, das heißt abhängig vom Zusatzwissen der jeweiligen verantwortlichen Stelle, führt dies unweigerlich zu der Frage, wie pseudonyme Daten, also Daten bei denen die Identifikationsmerkmale durch ein Kennzeichen ersetzt wurden, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren, für diejenige verantwortliche Stelle zu behandeln sind, die nicht über das erforderliche Zusatzwissen verfügt. Wie bereits oben ausgeführt, sind im Rahmen von medizinischen Forschungsprojekten pseudonyme Daten von erheblich höherem Nutzen. Nur wenn die Identifikation des betroffenen Patienten grundsätzlich möglich bleibt, kann dieser auch von den Forschungsergebnissen profitieren. Rein tatsächlich sind diese Daten für die datenverarbeitende Stelle anonym, soweit sie nicht über den Schlüssel verfügt, der die Zuordnung zu dem jeweiligen Patienten zulässt. Die Gefährdungslage für die betroffene Person ist die gleiche. Genau betrachtet ist nämlich der Schlüssel, der das Pseudonym aufhebt, auch nur verfügbares Zusatzwissen, welches anonyme oder eben pseudonyme Daten zu personenbezogen Daten macht, soweit die verantwortliche Stelle hierauf Zugriff hat. Ausreichend sicher verschlüsselte pseudonyme Daten müssen daher als anonym bewertet werden, wenn die verarbeitende Stelle nicht über den Schlüssel verfügt, mit der Folge, dass das Datenschutzrecht *für diese verarbeitende Stelle* keine Anwendung findet.[23]

[14] Metschke / Wellbrock, Datenschutz in Wissenschaft und Forschung, Berlin 2002, S. 20 ff., http://www.datenschutz-berlin.de/infomat/dateien/mat_28.pdf.

[15] Artikel 29 Datenschutzgruppe: Arbeitspapier über genetische Daten, S. 12 (Fn. 3).

[16] Amtsblatt der Europäischen Gemeinschaft Abl. C 1991/159/38 (40).

[17] Erster Bericht der Kommission über die Durchführung der Datenschutzrichtlinie von 2003, abrufbar unter: http://eur-lex.europa.eu/LexUriServ/site/de/com/2003/com2003_0265de01.pdf.

[18] EPOF, Comments on Review of the EU Data Protection Directive (Directive 95/46/EC) von 2002, abrufbar unter: http://www.html.dk/log/D25.pdf.

[19] Nicht unberücksichtigt bleiben darf zudem, dass Erwägungsgründen kein eigenständiger normativer Gehalt zukommt. Sie dienen vielmehr dazu, die Ziele des Gemeinschaftsgesetzgebers zu verdeutlichen; vgl. z.B. Redeker / Karpenstein, Über Nutzen und Notwendigkeit, Gesetze zu begründen, NJW 2001, 2825, 2830.

[20] Metschke /Wellbrock (Fn. 14).

[21] Rossnagel / Scholz, Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721, 723; Dammann, in: Simitis,. Komm zum BDSG 2006, § 3 Rn. 32; Gola / Schomerus, BDSG 2005, § 3 Rn. 44; Metschke / Wellbrock (Fn. 14), S. 21.

[22] Ebenda.

[23] So wohl auch Gola / Schomerus, BDSG 2005, § 3 Rn. 46, die feststellen, dass „pseudonymisieren […] nicht zwingend Anonymität herstellt", da die verantwortliche Stelle gegebenenfalls über eine Referenzdatei verfügt. Verfügt die verantwortliche Stelle über dies Datei nicht, wird wohl aber auch hier vom Vorliegen anonymer Daten ausgegangen.

Für die Frage, ob anonyme Daten vorliegen oder nicht, ist also das Zusatzwissen entscheidend. Zu klären gilt es daher, *welches* Zusatzwissen sich die verantwortliche Stelle als eigenes zurechnen lassen muss. Maßgeblich wird hierbei auf die Verfügbarkeit des erforderlichen Zusatzwissens abgestellt, durch das der Personenbezug wieder hergestellt werden kann.[24]

Unstrittig ist, dass sich die verantwortliche Stelle bei ihr tatsächlich vorhandenes Zusatzwissen immer zurechnen lassen muss. Verfügt die verantwortliche Stelle also über das erforderliche Zusatzwissen, hat sie beispielsweise in einer Datenbank die Geninformation einer betroffenen Person gemeinsam mit dessen Namen oder sonstigen Identifizierungsmerkmalen abgespeichert, sind die genetischen Daten als personenbezogen zu behandeln, und zwar selbst für den Fall, dass die Daten tatsächlich anonym verarbeitet werden, ein Abgleich mit der Datenbank also nicht erfolgen soll. Auf die Absicht der verantwortlichen Stelle kommt es nicht an.[25]

Unterschiedlich gehandhabt wird aber die Frage, ob und inwieweit sich die verantwortliche Stelle Zusatzwissen zurechnen lassen muss, über das sie tatsächlich nicht verfügt, das sie oder ein Dritter sich aber beschaffen könnte. Zu unterscheiden sind hier zwei Aspekte: Einerseits gilt es zu klären, ob der verantwortlichen Stelle nur *legal verfügbares* Zusatzwissen zugerechnet werden kann, andererseits, ob sich die verantwortliche Stelle auch Wissen, das ausschließlich *Dritten* zur Verfügung steht, zurechnen lassen muss.

4.1 Indirekt personenbezogene Daten nach § 4 Nr. 1 des österreichischen Datenschutzgesetzes 2000

In Österreich hat man anlässlich der Umsetzung der DSRL zur Lösung dieser Fragen[26] eine weitere Datenart eingeführt. Neben personenbezogenen (§ 4 Nr. 1 ö DSG 2000) und nicht personenbezogenen Daten kennt das österreichische Datenschutzgesetz auch so genannte indirekt personenbezogene Daten. Indirekt personenbezogen sind „Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.“[27] Bei der Verwendung von indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen des Betroffenen als nicht verletzt – und zwar weder bei nicht sensiblen (§ 8 Abs. 2 DSG 2000) noch bei sensiblen Daten. (§ 9 Nr. 2 DSG 2000). Daten, die für den Empfänger nur indirekt personenbezogen sind (was etwa durch ein Pseudonym erreicht werden kann), dürfen genehmigungsfrei ins Ausland übermittelt oder im Ausland überlassen werden (§ 13 Abs. 3 Nr. 2 DSG 2000). Datenanwendungen, die nur indirekt personenbezogene Daten enthalten, sind nicht meldepflichtig (§ 17 Abs. 2 Nr. 3 DSG 2000). Der Datenbetroffene kann bei indirekt personenbezogenen Daten kein Recht auf Auskunft (§ 26 DSG 2000), Richtigstellung, Löschung (§ 27 DSG 2000) oder Widerspruch (§ 28 DSG 2000) geltend machen (§ 29 DSG 2000). Sind die Daten für den Auftraggeber (entspricht weitgehend der verantwortlichen Stelle nach deutscher Terminologie, vgl. § 4 Nr. 4 DSG 2000) nur indirekt personenbezogen und will er sie zum Zwecke wissenschaftlicher oder statistischer Untersuchungen verwenden, die keine personenbezogenen Ergebnisse zum Ziel haben, so ist dies ohne irgendwelche weiteren Voraussetzungen möglich (§ 46 Abs. 1 Nr. 3 DSG 2000). Daten für wissenschaftliche Zwecke sind, wenn möglich, pseudonymisiert oder anonymisiert zu verarbeiten (§ 46 Abs. 5 DSG 2000). Dies gilt insbesondere im medizinischen Bereich, in dem sich aus dem österreichischen Arzneimittel- und Medizinproduktegesetz eine Pseudonymisierungspflicht ergibt.[28] Weitere Sicherheitsanforderungen für direkt personenbezogene Daten ergeben sich aus dem Medizintelematikgesetz.[29]

Die österreichische Regelung rechnet mithin nur solches Zusatzwissen zu, auf das die datenverarbeitende Stelle mit legalen Mitteln, etwa über im Internet frei zugängliche Quellen, zugreifen könnte. Die Möglichkeit Dritter, den Personenbezug wieder herzustellen, bleibt unberücksichtigt.

4.2 Rechtslage in Deutschland

Doch ist diese österreichische Regelung zur datenschutzgerechten Forschung mit genetischen Daten nicht ohne weiteres auf die anderen Mitgliedstaaten der Europäischen Union übertragbar. Die europäische Datenschutzrichtlinie (95/46/EG) hat das Datenschutzrecht in den einzelnen Mitgliedstaaten zwar harmonisiert, aber den Mitgliedstaaten auch Spielräume bei der Umsetzung der Richtlinie überlassen[30] und enthält zu bestimmten Bereichen keine Aussagen, so dass die Datenschutzregelungen in den einzelnen EU-Mitgliedstaaten teilweise immer noch relativ stark voneinander abweichen.[31]

Das BDSG enthält keine Norm, in der die Zurechnung von Zusatzwissen ausdrücklich geregelt wird. Folglich ist die Zurechnung von Zusatzwissen durch Auslegung der datenschutzrechtlichen Bestimmungen zu ermitteln.

[24] Dammann in: Simitis, BDSG 2006,§ 3 Rn. 29.

[25] Gola / Schomerus, BDSG, München 2005, § 3 Rn. 44.

[26] Vgl. Regierungsvorlage zum Datenschutzgesetz 2000, 1613 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, 37: „Um hier im Hinblick auf das Schutzinteresse eine sinnvolle Abstufung vornehmen zu können, wurde die in der Richtlinie enthaltene Unterscheidung zwischen direkter und (nur) indirekter Identifizierbarkeit nutzbar gemacht; wenn es für den konkreten Verwender der Daten nicht möglich ist, den – zB in Form einer laufenden oder sprechenden Nummer – vorhandenen Personenbezug auf eine in ihrer Identität bestimmte Person zurückzuführen, dann ist der Gebrauch solcher „nur indirekt personenbezogener” Daten durch diesen Verwender unter erleichterten datenschutzrechtlichen Bedingungen erlaubt.“

[27] § 4 Nr. 1, 2. Halbsatz DSG 2000.

[28] Vgl. §§ 46 Abs. 3, 36 Nr. 8 AMG, 55 Abs. 1 MPG; vgl. dazu Knyrim / Momeni, Datenschutz bei klinischen Prüfungen und medizinischen Studien, in: RdM 2003, 32.

[29] Art. 10 des Gesundheitsreformgesetzes 2005, BGBl I 2005 Nr. 179.

[30] Brühann, Die Veröffentlichung personenbezogener Daten im Internet als Datenschutzproblem, DuD 2004, 201, 201.

[31] Die nationale Umsetzung der RiL 95/46/EG darf dabei jedoch im Rahmen der gemeinschaftskonformen Interpretation nicht andere durch die Gemeinschaftsrechtsordnung geschützte Grundrechte oder andere allgemeine Grundsätze des Gemeinschaftsrechts, wie den Grundsatz der Verhältnismäßigkeit, verletzen; vgl. EuGH in der Sache „Lindqvist“ Urteil vom 06.11.2003, C-101/01, DuD 2003, 244: Die Mitgliedstaaten dürfen demzufolge nur Vorschriften, die über das Schutzniveau der RiL 95/46/EG hinausgehen, auf die in der Richtlinie 95/46 vorgesehenen Art und Weise erlassen, wenn diese ein Gleichgewicht zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre wahren und ihnen keine Bestimmungen des Gemeinschaftsrechts entgegenstehen.

So wird vertreten, dass es unbeachtlich sei, ob Zusatzwissen legal oder unzulässig beschafft wurde bzw. beschafft werden könnte. Es komme lediglich darauf an, ob Wissen zur Identifizierung des Betroffenen faktisch zur Verfügung stünde.[32] Dieser Auffassung ist insoweit zuzustimmen, als genetische Daten sehr sensible Informationen über den Betroffenen beinhalten und sie nach dieser Ansicht umfassend geschützt wären. Doch ist diese Auffassung nach hier vertretener Ansicht mit EG (26) der DSRL kaum vereinbar, wonach nur solche Mittel zur Bestimmung einer Person berücksichtigt werden sollten, die *vernünftigerweise* […] eingesetzt werden könnten, um eine Person zu bestimmen. Nach obiger Ansicht wäre jedoch jedes Zusatzwissen zu berücksichtigen und nicht nur solches, welches *vernünftigerweise* eingesetzt werden könnte, so dass diese Ansicht dem Wortlaut der DSRL widerspricht. Eine Unterscheidung zwischen personenbezogenen und nichtpersonenbezogenen Daten wäre in der Praxis für eine datenverarbeitende Stelle auch nicht mehr möglich, so dass der Anwendungsbereich der datenschutzrechtlichen Regelungen unkontrollierbar ausgedehnt würde. In einem rechtsstaatlichen Umfeld muss Zusatzwissen, welches einer datenverarbeitenden Stelle zugerechnet werden soll, daher vernünftigerweise dieser zur Verfügung stehen, das heißt im Regelfall: auf legalem Wege beschafft werden können.[33]

Bezüglich der Frage, ob der für die Datenverarbeitung verantwortlichen Stelle auch Wissen, das ausschließlich Dritten zur Verfügung steht, zugerechnet werden muss, wird, wie oben bereits angedeutet, in der deutschen Literatur, ähnlich wie in Österreich bereits normiert, vielfach vertreten, dass ihr lediglich das Zusatzwissen zugerechnet werden kann, über welches sie selbst verfügt oder zumindest legalerweise verfügen könnte.[34] Der verantwortlichen Stelle könnte somit lediglich jenes Wissen zugerechnet werden, welches für sie selbst, z.B. über das Internet, zugänglich ist, nicht jedoch Wissen in Datenbanken, z.B. der Strafverfolgungsbehörden, zu dem sie selbst keinen legalen Zugang besitzt. Die verantwortliche Stelle wäre somit frei, mit diesen Daten nach eigenem Belieben zu verfahren, z.B. die Daten im Internet zu veröffentlichen. Dies würde gleichzeitig aber die Strafverfolgungsbehörden in die Lage versetzen, den Personenbezug durch Abgleich der im Internet veröffentlichten Daten mit ihrer eigenen Datenbank wieder herzustellen.

4.3 Bewertung

Diese Ansicht vermag vor dem Hintergrund geltenden europäischen Rechts nicht zu überzeugen. Es kann bei der Zurechnung von Zusatzwissen nicht darauf ankommen, ob die für die Datenverarbeitung verantwortliche Stelle oder ein Dritter Zugriff auf dieses Wissen hat. Die Auslegung, welches Zusatzwissen einer für einen Datenverarbeitungsvorgang verantwortlichen Stelle zurechenbar und ob eine Person in der Folge für sie bestimmbar ist, muss sich zuvorderst im Wege der europarechtskonformen Auslegung an der europäischen Datenschutzrichtlinie (95/46/EG) orientieren. Diese besagt in dem bereits erwähnten EG 26 S. 2, dass bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden sollten, *die vernünftigerweise entweder von dem Verantwortlichen […] oder von einem Dritten eingesetzt werden könnten[…]*.

Die Auslegung des Wortlauts dieser Vorschrift lässt es als nahe liegend erscheinen, dass der verantwortlichen Stelle nicht nur die Mittel zugerechnet werden dürfen, deren Nutzung durch die verantwortliche Stelle rechtlich zulässig ist. Vielmehr besagt diese Vorschrift, dass auch die Mittel eines Dritten der verantwortlichen Stelle zugerechnet werden müssen, die dieser vernünftigerweise zur Identifikation einer Person einsetzt.

Zu solchen Mitteln, welche vernünftigerweise von einem Dritten eingesetzt werden, gehört zweifelsfrei die Nutzung von Wissen, auf welches dieser Dritte legalerweise Zugriff hat und das er mit vertretbarem Aufwand einsetzen kann. Folglich erscheint es im Wege dieser richtlinienkonformen Auslegung des BDSG zwingend, dass der verantwortlichen Stelle nicht nur das Wissen zugerechnet wird, auf welches sie selbst Zugriff hat, sondern auch solches, auf das ein Dritter zugreifen kann.[35]

Auch nach teleologischer Auslegung des § 3 Abs. 1 BDSG erscheint eine derartige Auslegung zwingend. Sinn des Datenschutzrechts ist es gem. § 1 Abs. 1 BDSG, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Dies wird verfassungsrechtlich durch das Recht auf informationelle Selbstbestimmung abgesichert, wonach die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraussetzt.[36]

Die im Rahmen eines Genomforschungsprojekts für einen Datenverarbeitungsvorgang verantwortliche Stelle verfügt regelmäßig über keine personenbezogenen Referenzdatensätze, mit Hilfe derer sie im Wege eines Matchingverfahrens die betroffene Person identifizieren könnte. Folglich würde es sich bei den Daten nach der ersten Ansicht für sie um faktisch anonymisierte Daten handeln, die nicht in den Anwendungsbereich der Datenschutzgesetze fielen.

Die verantwortliche Stelle könnte mit den von ihr zu verarbeitenden genetischen Daten nach Belieben verfahren, so z.B. diese im Internet veröffentlichen oder ins Ausland übermitteln. Auf diesem Wege könnten jedoch Dritte auf diese Daten zugreifen und den Personenbezug wiederherstellen, weil sie über personenbezogene Referenzdatensätze verfügen und ein Interesse an den damit verbundenen Informationen haben.

Strafverfolgungsbehörden oder Versicherungen, die teilweise in der Praxis über Gendatenbanken verfügen, könnten z.B. ein großes Interesse daran haben, zu erfahren, ob eine bestimmte Person, über die sie einen personenbezogenen Referenzdatensatz besitzen, eine bestimmte Krankheit hat. Der Bürger würde dadurch in seiner Freiheit verletzt, selbst zu entscheiden, wann er wem welche Daten zugänglich macht, so dass der Sinn des Datenschutzrechts unterlaufen würde.

Folglich ist der für einen Datenverarbeitungsvorgang verantwortlichen Stelle gemäß des Wortlauts der europäischen Datenschutzrichtlinie und des Sinns des Datenschutzrechts auch das Zusatzwissen Dritter zuzurechnen. Hat somit ein Dritter legalerweise Zugang zu Wissen, mit Hilfe dessen

[32] Weichert (Fn. 7), Rn. 58.

[33] Saeltzer, Sind die Daten personenbezogen oder nicht?, DuD 2004, 218, 220; Dammannin: Simitis, BDSG 2006, § 3 Rn. 37; Sieber in: Hoeren / Sieber (Hrsg.), HdB Multimedia 2006, Nr. 19 S. 206, Rn. 552.

[34] Vgl. z.B. Dammann in: Simitis, BDSG 2006, § 3 Rn. 37 ff.; Saeltzer, DuD 2004, 218, 222; Roßnagel / Scholz, MMR 2000, 721, 723

[35] Im Ergebnis so auch Schaar, Datenschutz im Internet, München 2002, S. 55 f., Rn. 153 und Metschke /Wellbrock (Fn. 14).

[36] BVerfGE 65, 1, 45.

die betroffene Person identifiziert werden kann, so handelt es sich bei den genetischen Daten auch für die verantwortliche Stelle um personenbezogene Daten, obwohl sie selbst die betroffene Person gar nicht identifizieren kann. Da sie in der Praxis aber gar nicht wissen kann, für welche der von ihr verwendeten Genomdatensätze ein personenbezogener Referenzdatensatz existiert, müsste sie alle Genomdatensätze als personenbezogene Daten betrachten, um einer etwaigen Verantwortlichkeit zu entgehen. Sie bräuchte folglich für jeden Datenverarbeitungsvorgang und somit auch für die Übermittlung und Veröffentlichung eine Erlaubnis durch eine Rechtsvorschrift oder eine Einwilligung des Betroffenen. Dieser wäre dadurch wirksam in seiner Privatsphäre und seinem Recht auf informationelle Selbstbestimmung geschützt. Auf der anderen Seite würde diese Auslegung die medizinische Forschung aber stark beeinträchtigen: Die Wirksamkeit einer allumfassenden, auch zukünftige, im Erklärungszeitpunkt nicht bekannte Verarbeitungsvorgänge erfassenden Einwilligung der betroffenen Person ist, wie oben bereits erläutert, rechtlich zweifelhaft. Ähnlich weit reichende (europaweit einigermaßen harmonisierte) Ermächtigungsgrundlagen für die Datenverarbeitung sind nicht ersichtlich. Die transnationale medizinische Forschung an genetischen Daten wäre ausgebremst.

4.4 Unterscheidung nach Verarbeitungsschritten

Deshalb muss die hier vertretene Auslegung restriktiv gefasst werden. Es besteht nämlich immer dann keine Gefährdung für die Privatsphäre des Betroffenen, wenn die verantwortliche Stelle erstens legalerweise nicht auf das Zusatzwissen Dritter zugreifen kann und zweitens die Dritten nicht auf die Daten der verantwortlichen Stelle zugreifen können. Eine Identifizierung der betroffenen Person ist zumindest dann mit der heute verfügbaren Technik schlechthin nicht zu realisieren oder nur mit unverhältnismäßigem Aufwand möglich. Die Zurechnung von Zusatzwissen Dritter auch in diesen Fällen würde die Anwendbarkeit datenschutzrechtlicher Vorschriften deshalb zu sehr ausweiten und dem Sinn des Datenschutzes widersprechen.

Folglich muss die Zurechnung des Zusatzwissens Dritter von der konkreten Situation der jeweiligen Datenverarbeitung abhängig gemacht werden.[37] Besteht also die Gefahr, dass ein Dritter die von der verantwortlichen Stelle zu verarbeitenden Daten einsehen (z.B. infolge einer Veröffentlichung oder Übermittlung dieser Daten) und die betroffene Person identifizieren kann, so müssen die Datenschutzgesetze den Betroffenen wirksam in seiner Privatsphäre schützen. Daraus folgt, dass bei Verarbeitungsvorgängen, bei denen diese Gefahr für die Privatsphäre des Betroffenen besteht, also insbesondere im Falle der Übermittlung und Veröffentlichung von Daten, das Zusatzwissen Dritter der verantwortlichen Stelle zugerechnet werden muss.[38]

Diese braucht folglich für jede Übermittlung oder Veröffentlichung der faktisch anonymisierten Daten eine Erlaubnis (durch eine Rechtsvorschrift oder Einwilligung), da sie nicht wissen kann, für welche der von ihr zu verarbeitenden Genomdatensätze Zusatzwissen existiert.

Verarbeitungsvorgänge, die eine solche Gefährdung des Persönlichkeitsrechts nicht beinhalten, wie z.B. die adäquat gesicherte Speicherung oder Nutzung der faktisch anonymisierten Daten, bedürfen hingegen keiner Einwilligung des Patienten oder einer gesetzlichen Erlaubnis. Diese Lösung bietet somit einen ausreichenden Schutz des verfassungsrechtlich verankerten Rechts des betroffenen Bürgers auf informationelle Selbstbestimmung, ohne die medizinische Forschung zu behindern.

Die hier vertretene Ansicht steht zudem im Einklang mit EG 26 S. 2 DSRL, da dieser sogar explizit aussagt, dass nur die Mittel eines Dritten bei der Bestimmung einer Person berücksichtigt werden sollen, die *vernünftigerweise* von ihm eingesetzt werden könnten. Vernünftigerweise setzt ein Dritter aber nur Mittel zur Identifikation einer von einem Datenverarbeitungsvorgang betroffenen Person ein, wenn er auch auf die zu verarbeitenden Daten Zugriff hat. Hat er dies nicht, setzt er auch vernünftigerweise keine Mittel zur Identifikation ein, so dass der für den Datenverarbeitungsvorgang verantwortlichen Stelle diese Mittel, also z.B. auch das Wissen dieses Dritten, auch bei richtlinienkonformer Auslegung des § 3 Abs. 1 BDSG nicht zugerechnet werden können.

5 Fazit

Bei der Frage, ob eine datenverarbeitende Stelle personenbezogene Daten verarbeitet oder nicht, ist auf das verfügbare Zusatzwissen abzustellen. Der datenverarbeitenden Stelle ist dabei Zusatzwissen zuzurechnen, über welches sie selbst tatsächlich verfügt oder zumindest legalerweise verfügen könnte. Darüber hinaus muss sie sich ebenso Wissen, über das ausschließlich Dritte legalerweise verfügen können, zurechnen lassen. Da dies aber zu einer zu extensiven Anwendung der Datenschutzgesetze führen würde, muss diese Auslegung restriktiv erfolgen.

Der vorliegende Beitrag schlägt eine Unterscheidung nach der Gefahrenlage bei der jeweiligen Verarbeitungsart vor. Bei der Übermittlung und Veröffentlichung von faktisch anonymen genetischen Daten sollen die Datenschutzgesetze hiernach immer Anwendung finden. Bei der Speicherung und Nutzung faktisch anonymer genetischer Daten jedenfalls dann nicht, wenn die verantwortliche Stelle erstens legalerweise selbst nicht auf das Zusatzwissen Dritter zugreifen kann und zweitens die Dritten nicht auf die Daten der verantwortlichen Stelle zugreifen können.

Somit bietet die hier vorgestellte und vertretene Ansicht eine richtlinienkonforme und dem Sinn des Datenschutzes entsprechende, aber auch praxistaugliche Lösung für die Zurechnung von Zusatzwissen, die auch den medizinischen Fortschritt unterstützt.

[37] Vgl. für biometrische Daten: Hornung, Die digitale Identität, Baden-Baden 2005, S. 147 ff. und ders., Der Personenbezug biometrischer Daten, DuD 2004, 429, 430, der den Personenbezug von biometrischen Daten ebenfalls von den unterschiedlichen Verfahrensschritten abhängig macht.

[38] Vgl. dazu auch Schaar, Datenschutzrechtliche Schranken der Genanalysen, in: Ronellenfitsch / Kartmann (Hrsg.), Genanalysen und Datenschutz 2005, S. 75, abrufbar unter: http://www.datenschutz.hessen.de/Forum/Forum2004.pdf.