

Anspruch der sozialwissenschaftlichen Komplexitätsansätze sehe ich auf der Ebene einer Theorie mittlerer Reichweite, die empirische Forschung anleiten kann. Eine Soziologie, die am Auffinden sozialer Mechanismen zur Erklärung sozialer Prozesse interessiert ist, kann neue Impulse durch die Komplexitätstheorie erhalten.

Zum möglichen Nutzen der Komplexitätstheorie für die (interne oder externe) Governance von LTS kann dreierlei gesagt werden. Zum einen sensibilisiert ein Verständnis von Komplexität für die Grenzen direkter Steuerung und Kontrolle. Darüber hinaus lassen sich zweitens auch durchaus Managementregeln auf Organisationsebene herausarbeiten. Drittens kann auf Basis der Komplexitätstheorie das Verhalten soziotechnischer Systeme möglicherweise auch (computergestützt) für bestimmte Anwendungsbereiche (man denke etwa an Stauvermeidung im Straßenverkehr oder den Datenfluss im Internet) so genau modelliert werden, dass sich konkrete Regulierungsmaßnahmen darauf stützen können. An dem Umstand, dass man Systeme, wenn sie wirklich komplex und nicht nur kompliziert sind, letztlich eben nicht planen und managen kann, ändert das nichts.

### Anmerkungen

- 1) Präsentationen sind auf der Konferenzwebsite mit den Präsentationen abrufbar unter <http://www.uni-konstanz.de/FuF/Verwiss/Schneider/largetech/index.php?pg=6&lan=1> (download 18.11.08).
- 2) Ein ausführlicherer Tagungsbericht des Autors kann von der Website des Arbeitskreises für Politik und Technik der Deutschen Vereinigung für Politische Wissenschaft abgerufen werden unter: [http://www.uni-konstanz.de/FuF/Verwiss/Schneider/Akpt/files/Boehle\\_2008CTS.pdf](http://www.uni-konstanz.de/FuF/Verwiss/Schneider/Akpt/files/Boehle_2008CTS.pdf) (download 15.12.08).

« »

## Mehr Standard, weniger Vielfalt Bericht vom Workshop „Die datenschutzrechtliche Auditierung von Biobanken“

Kiel, 4. Juli 2008

von Imme Petersen, Universität Hamburg  
(BIOGUM)

### 1 Einleitung

Sammlungen von Blut- und Gewebeproben werden in der biomedizinischen Forschung zur Aufklärung von Krankheitsursachen und für die Entwicklung neuer Therapien immer wichtiger. Spender stellen der Forschung diese Proben häufig zusammen mit klinischen, biologischen, soziodemographischen und lebensstilbezogenen Daten zu ihrer Person zur Verfügung. Dabei haben sie ein Recht auf wirksamen Schutz ihrer Daten und Proben und der Informationen, die mit diesen im Zusammenhang stehen. Während die personenbezogenen Daten verschlüsselt werden können, ist Körpermaterial, das genetische Informationen enthält, de facto nicht anonymisierbar. Gleichzeitig wächst das Risiko von Datenmissbrauch, da sich (insbesondere genetische) Referenz-Informationen durch das Internet immer mehr verbreiten, Testverfahren zur Gesundheitsvorhersage aussagekräftiger werden und Begehrlichkeiten staatlicher und privater Institutionen entstehen.

Bislang existieren jedoch kaum spezifische ethische und datenschutzrechtliche Standards für Biobanken, die Proben und Daten der Spender sammeln, speichern und für Forschung freigeben. Aus diesem Grund hat sich der vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Forschungsverbund „Biobank Data Custodianship \ Audit Methodology and Criteria (bdc-AUDIT)“ zum Ziel gesetzt, Methoden, Kriterien und Handlungsempfehlungen für ein datenschutzrechtliches Auditierungsverfahren von Biobanken zu erarbeiten, das erstmals die Einhaltung datenschutzrechtlicher Standards überprüfbar machen soll. Auf dem Workshop „Die datenschutzrechtliche Auditierung von Biobanken. Voraussetzung, Kriterien, Vorgehensweisen“ im Landeshaus Kiel

stellten die Verbundpartner Regine Kollek (Forschungsschwerpunkt Biotechnik, Gesellschaft und Umwelt, Universität Hamburg), Thilo Weichert (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) und Norbert Luttenberger (Institut für Informatik, Christian-Albrechts-Universität Kiel) mit ihren Mitarbeitern ein allgemeines Modell für ein datenschutzrechtliches Audit von Biobanken vor. Das Modell, das auf Grundlage einer empirischen Analyse der Strukturen und Prozesse in deutschen Biobanken entwickelt wurde, soll verdeutlichen, wie eine Biobank sich selbst organisieren und beschreiben muss, damit sie erfolgreich ein Datenschutz-Audit bestehen kann. Mehr als 50 Datenschützer, Informatiker, Biobank-Betreiber und Mediziner diskutierten anhand der präsentierten Forschungsergebnisse, wie die Vertraulichkeit und Integrität von Proben und Daten in Biobanken gewährleistet werden kann.

## 2 Analyse und Klassifikation von Biobanken

*Erich Wichmann* vom Helmholtz-Zentrum in München zeigte in seinem Eingangsreferat zunächst die aktuellen Trends in der epidemiologischen Biobank-Forschung auf. Die medizinische Forschung habe ein großes Interesse an Biobanken, insbesondere an Proben- und Datensammlungen mit großen Probandenzahlen. Im Fokus der Forschung stünden weit verbreitete Krankheiten wie Herz-Kreislauf-Erkrankungen, Krebs oder Diabetes und deren genetische und umweltbezogene Ursachen. Laut Wichmann, der sich auf Zahlen von „Public Population Projects in Genomics“ bezog, existierten im Sommer 2007 weltweit bereits 91 bevölkerungsbezogene Biobanken mit rund zehn Mio. registrierten oder angestrebten Probanden. Während in Europa die skandinavischen Länder mit insgesamt drei Mio. und die „UK Biobank“ in Großbritannien mit 600.000 anvisierten Proben bereits große Biobank-Projekte verwirklicht haben, sind derzeit in Deutschland regional orientierte Biobanken mit vergleichsweise geringen Probandenzahlen vorhanden wie „KORA“ in der Region Augsburg (20.000) oder „Popgen“ in Schleswig-Holstein (25.000). Wichmann betonte die Notwendigkeit einer nationalen Neugründung, die unter dem Namen „Helmholtz Cohort“ mit 200.000 prospektiven Spendern in fünf deutschen Regionen

in der Nähe von Helmholtz-Zentren bereits geplant ist und voraussichtlich 2010 mit der Rekrutierungsphase beginnen wird. Parallel zu nationalen Bestrebungen vernetzen sich bereits bestehende Biobanken international zunehmend. In der „Pan-European Biobanking and Biomolecular Resources Research Infrastructure“ sollen beispielsweise 104 europäische Biobanken mit 12,5 Mio. Proben vernetzt werden. Angesichts dieser Entwicklungen seien einheitliche Standards zur Sicherung des Datenschutzes bei nationalen Biobanken und internationalen Biobankinfrastrukturen zwingend notwendig, betonte Wichmann.

Um ein auditierbares Datenschutzkonzept für Biobanken unabhängig von ihrer Größe, Struktur und Vernetzung entwickeln zu können, analysierten *Regine Kollek* und *Rainer Paslack* vom Forschungsschwerpunkt „Biotechnik, Gesellschaft und Umwelt“ der Universität Hamburg (BIOGUM) in zwei Interviewrunden acht deutsche Biobanken. Die empirischen Ergebnisse machten deutlich, dass die Biobanken sich historisch eigenständig entwickelt haben und in Organisation, Datenbeständen, Abläufen und Strukturen teilweise deutlich voneinander abweichen. Trotz dieser Heterogenität konnten bei der Prozessanalyse insgesamt 13 datenschutzrelevante Prozesskomplexe (wie die Spender-Rekrutierung, die Proben- und Daten-Erhebung, das Proben- und Daten-Handling oder die Weitergabe von Daten und Proben an externe Institutionen) typisiert werden. Insbesondere die Analyse der Verantwortlichkeiten in den einzelnen Einrichtungen offenbarte, dass die Biobanken aufgrund fehlender verbindlicher datenschutzrechtlicher Standards eigene betriebliche Lösungen für den Daten- und Spenderschutz entwickeln müssen, was den Aufbau von Biobanken aufwendig und kostenintensiv mache, dabei Probleme bei der Überprüfung und Vernetzung schaffe und dadurch die Effektivität von Forschung behindere. Regine Kollek betonte in ihrem Vortrag damit die Nachteile für Biobanken durch die bislang fehlende Standardisierung und machte deutlich, dass Biobanken von einer Auditierung profitieren könnten. Ausgehend von den erhobenen empirischen Ergebnissen schlussfolgerte Kollek, dass trotz des insgesamt konstatierten Bemühens um den Daten- und Spenderschutz Handlungsbedarf für eine Standardisierung

bestehe – zum Beispiel bei der Formulierung der Einwilligungserklärung der Probengeber, bei der Transparenz der Verarbeitung, bei der Dokumentation sowie bei der Sicherheit der pseudonymen Nutzung von Proben und Daten.

### 3 Das Modell der internen Datentreuhänderschaft

*Rainer Paslack* wies daraufhin den Biobanken die De-facto-Funktion eines „Datentreuhänders“ zu. Sie seien verpflichtet, den sicheren Umgang mit den Daten und Proben zu gewährleisten; insbesondere sollten sie unzulässige Re-Identifikationen des Spenders verhindern sowie die Verwendung der Proben und Daten ohne Einwilligung des Spenders ausschließen. In diesem Zusammenhang benannte Paslack drei Risikobereiche und zwei zentrale Risikoschwellen, die vom Verbundprojekt identifiziert worden seien und für alle Biobanken trotz der Vielfalt ihrer möglichen Nutzungszwecke bestünden: (1) die Erhebung von Daten und Proben (Risikoschwelle Eingang), (2) die Weiterverarbeitung der Daten und Proben, (3) die Weitergabe an die Forschung (Risikoschwelle Ausgang). Um den Spenderschutz zu garantieren, müssten grundsätzlich beim Überschreiten einer Risikoschwelle die Kennzeichnungen (die Pseudonyme) der Probe und der dazugehörigen Daten geändert werden. Wenn Daten und Proben also getrennt voneinander zu kennzeichnen sind, dann wechselt eine Probe bzw. ein Datensatz demnach idealtypisch von der Erhebung bis zur Herausgabe zweimal sein Pseudonym: vom Erhebungspseudonym zum Vorhaltungspseudonym und vom Vorhaltungspseudonym zum Herausgabepseudonym<sup>1</sup>. Gerade die Pseudonymersetzungen wurden in den untersuchten Biobanken sehr unterschiedlich gehandhabt. Paslack konstatierte deshalb einen zum Teil erheblichen Nachbesserungsbedarf für das Niveau des Spenderschutzes.

*Wolfgang Zimmermann* vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) definierte für die einzelnen Risikoschwellen rechtliche Datenschutzerfordernisse und machte Vorschläge für ein Datentreuhändermodell auf der Basis mehrfacher Pseudonymisierung. Er betonte, dass das klassische Modell eines externen Datentreuhänders, der als unabhängige Person zwischen der daten-

besitzenden Stelle und dem Forscher die erforderlichen Daten vermittelt, bei Biobanken nicht möglich sei. Diese externe Datentreuhänderschaft zum Schutz des Spenders sei für reine Datenregister wie das Krebsregister entwickelt worden. Biobanken hätten dagegen aufgrund der besonderen Doppelstruktur wechselbezoglicher Daten und Proben das Problem, dass die Relation zwischen Probe und Daten – wenn auch verschlüsselt – über die Risikoschwellen hinweg erhalten bleiben muss. Dem kann laut Zimmermann der externe Datentreuhänder nur gerecht werden, wenn er nicht nur mit den Daten, sondern auch mit den Proben umgehe und dafür eine entsprechende Infrastruktur unterhalte. Da ein solcher externer Biobank-Datentreuhänder zudem nicht nur rechtlich sondern auch ökonomisch unabhängig sein müsse, sei das Modell des externen Biobank-Datentreuhänders nicht praxistauglich. Als Alternative entwickelte Zimmermann ein Modell, das den Datentreuhänder in die betriebsinternen Abläufe der Biobank integriert. Voraussetzung für diese Datentreuhänderschaft seien aber umfassende Auditierungen, um die Zuverlässigkeit und Vertrauenswürdigkeit des internen Datentreuhänders für Dritte nachvollziehbar zu machen.

### 4 Prozessorientierte Biobank-Modellierung

*Ralf Herkenhöner* (Institut für Informatik, Christian-Albrechts-Universität Kiel) stellte daraufhin ein computergestütztes Verfahren zur modellhaften Darstellung von Biobanken vor, mit dem Auditierungen einfacher durchgeführt werden könnten. Den internen Datentreuhänder berücksichtigend, wurden Prozesse, Rollen und deren Aktivitäten formalisiert mittels der Modellierungssprache UML dargestellt. Herkenhöner betonte, dass die Anforderungen an das Sicherheitssystem einer Biobank hoch seien angesichts möglicher Sicherheitsrisiken (wie unbefugter Zugriff, Systemfehler oder -absturz, Manipulationen, Fehlbedienungen oder unbefugte Re-Identifizierungen). Er definierte notwendige Sicherheitsanforderungen, die eine Biobank zu erfüllen habe. Neben der Dokumentation und Transparenz der internen Prozesse müsse der Spender vor allem vor unzulässigen Re-Identifikationen geschützt werden. Herkenhöner beschrieb daraufhin die technischen Anforderungen an Pseudonymisierungsverfahren. Bei

Einhaltung dieser Sicherheitsanforderungen können Biobanken laut Herkenhöner die Vertrauenswürdigkeitsstufe EAL 4 nach dem ISO-Standard 15408 erreichen.<sup>2</sup> Biobanken wären dann so sicher wie EC-Karten, die die Voraussetzung für dasselbe Sicherheitsniveau erfüllen.

## 5 Fazit und Ausblick

*Thilo Weichert* zeichnete in seinem Schlussvortrag die Fortschritte von Genomanalyse und Gendiagnostik nach und unterstrich deren potenzielle Risiken für Persönlichkeitsrechte. Die Gendiagnostik sei bereits heute ein selbstverständlicher Bestandteil der medizinischen Diagnostik, der genetische Fingerabdruck zähle zur forensischen Standard-Maßnahme und die sogenannte Life-Style-Genetik sei ein expandierender Wirtschaftszweig. Weichert prognostizierte, dass Biobanken zu der Standard-Datenbasis der medizinischen Forschung avancieren und dass neue Begehrlichkeiten für genetische Daten im Alltag – zum Beispiel von Versicherungen und Arbeitgebern – erwachen werden. Auch wenn bei der bisherigen Nutzung solcher Daten und Proben in der Forschung bislang noch kein Missbrauch für Betroffene bekannt geworden sei, sei eine vertrauenswürdige und integre Forschungsinfrastruktur zwingend, um Risiken wachsender Datennutzung auch in Zukunft zu bewältigen und die Kooperationsbereitschaft der Bevölkerung zu wahren. Der Gesetzgeber hat den Datenschutz bei Biobanken allerdings bislang nicht reguliert; auch der im Juni 2008 in den Bundestag eingebrachte Gendiagnostikgesetzentwurf klammert den Bereich der Forschung explizit aus. Nicht zuletzt wegen dieser gesetzlichen Regelungslücke konstatierten die Veranstalter dringenden Handlungsbedarf. Das zur Diskussion gestellte Auditierungsmodell soll die selbstgestrickten Einzellösungen beenden und eine Standardisierung des Daten- bzw. Spenderschutzes ermöglichen. Auch wenn für eine bundesweit rechtsverbindliche Auditierung ebenfalls bis dato die rechtlichen Voraussetzungen fehlen, betonte Weichert, dass die Biobanken von einer freiwilligen Auditierung profitierten. Das präsentierte Auditierungsmodell ziele – zum Nutzen aller – mittelfristig auf eine Standardisierung auf hohem Datenschutzniveau.

In der Diskussion betonten Vertreter von Biobanken ihr Interesse und den Bedarf an ver-

bindlichen Datenschutzstandards, um für Biobank-Betreiber Rechtssicherheit und für Probanden Gewissheit eines vertraulichen Umgangs mit den hochsensiblen Daten und Proben zu gewährleisten. Das Publikum befürwortete die Auditierung und damit eine datenschutzrechtliche Überprüfung als geeignetes Instrument der Standardisierung. Insbesondere die empirische Herangehensweise, das Auditierungsmodell aus den Strukturen und Prozessen der bereits existierenden Biobanken zu entwickeln, wurde positiv bewertet. Thematisiert wurden in diesem Zusammenhang aber auch praktische Probleme wie etwa das notwendige Umetikettieren der Proben bei jedem Pseudonymisierungsschritt. Bedenken wurden hinsichtlich der Selbstregulierung geäußert. Einige Stimmen bezweifelten, ob sich eine freiwillige Auditierung bundesweit durchsetzen könne oder ob – wegen der fehlenden rechtlichen Implementation – nicht doch wieder Inselösungen auf Länderebene entstehen würden.

Zusammenfassend ist festzustellen, dass es den Veranstaltern gelang, ein überzeugendes Modell sowie Musterprozesse und Kriterien vorzustellen, wodurch der Datentreuhänder in Biobanken betrieblich integriert und gleichzeitig durch das Datenschutz-Audit wirksam überwacht werden kann. Damit haben die Veranstalter einen konstruktiven Beitrag zur Diskussion über verantwortungsvolle Forschung mit genetischen Daten und Biomaterial geleistet. Es bleibt zu hoffen, dass die Diskussion über die datenschutzrechtliche Auditierung von Biobanken weitergeführt wird.<sup>3</sup>

## Anmerkungen

- 1) Dabei soll für jeden Fall einer Herausgabe ein neues Pseudonym verwendet werden, weshalb präziser von „Herausgabefallpseudonymen“ die Rede ist.
- 2) Die ISO ist die Internationale Organisation für Normung. Die Common Criteria sind seit 1999 eine ISO-Norm der technischen Standardisierung (vgl. Norm ISO 15408; <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>).
- 3) Weitere Informationen über den Workshop (inkl. der Präsentationen) sind unter <http://www.datenschutzzentrum.de/biobank/> abrufbar.

« »