

Karl-Heinz Ladeur

„Big Data“ im Gesundheitsrecht – Ende der „Datensparsamkeit“?

Die Nutzung von Big Data in der Medizin führt zu neuen Herausforderungen für den Datenschutz. Dies hängt nicht nur mit der Menge der Daten zusammen, die benutzt werden können und deren Nutzung mit dem Grundsatz der „Datensparsamkeit“ kollidiert. Die sich herausbildende „datenbasierte Medizin“ wirft auch Probleme im Hinblick auf die Zweckbindung der erhobenen und gespeicherten Daten auf. Andererseits lässt die gesteigerte Komplexität der immer neuen Durchsuchung von Daten nach bemerkenswerten Mustern auch neue Formen der Anonymisierung zu, die informationstechnologisch gut durchsetzbar erscheinen.

1 „Big Data“ ... und die „datenbasierte Medizin“

Das Ziel der Nutzung von Big Data im Gesundheitsrecht lässt sich schlechthin als „datenbasierte Medizin“ bezeichnen. Damit wäre ein grundsätzlicher Wandel von Wissenschaft und Praxis der Medizin verbunden. D. h. anders als bei der erfahrungs- oder der (neueren) evidenzbasierten Medizin (EBM), die an der methodisch kontrollierten Krankenhauspraxis orientiert ist, wird nicht ein bestimmtes Untersuchungsdesign mit einer fest vorgegebenen Fragestellung entworfen, sondern es werden *Daten ohne einen bestimmten Zweck*¹, jedenfalls ohne feste Verknüpfung mit einem Zweck, gesammelt, die über unterschiedliche, auch jeweils selbst auf Wandel, also Lernen angelegte „Algorithmen“ nach produktiven Verknüpfungsmustern abgesucht werden, die selbst allerdings Aussagen insbesondere über Krankheitsverläufe oder Therapien ermöglichen sollen.

In den neuen Konstellationen geht es statt um Genauigkeit der Bestimmung von Ursache-Wirkungs-Beziehungen, die für die Behandlung im *Einzelfall* sicher noch so wichtig sind wie vorher, eher um die Brauchbarkeit der Relationen.² Es geht um die Suche

nach Verteilungen von „Knoten“ und die Musterbildung in großen Datenmengen. Damit können auch komplexe Kausalitäten erfasst werden, d. h. individuelle Krankheitsbilder, in die multi-kausale Zusammenhänge eingehen, aber auch die Verteilung von Krankheiten innerhalb größerer Populationen.

Dies kollidiert mit dem Grundsatz der „Datensparsamkeit“, § 3a BDSG, und dem Grundsatz der Zweckbindung von Daten, § 40 Abs. 1 BDSG. Auch wenn durch die damit verbundene Begrenzung der Nutzung von Big Data nicht in die Wissenschaft eingegriffen wird, so erscheint es verfassungsrechtlich bedenklich, dass z. B. nach dem GenDG (§§ 1, 12 Abs. 1 S. 3) der objektiv-rechtliche Schutz der Wissenschaftsfreiheit weder zu den Zwecken des Gesetzes gehört (anders als die Menschenwürde und das Recht auf informationelle Selbstbestimmung) noch bei der Entscheidung über die Aufbewahrung von Daten (einschließlich der Nebeninformationen) zu berücksichtigen ist. Es zeichnet sich im Bereich der Gendiagnostik, deren Nutzung in der medizinischen Praxis an Grenzen stößt, die Möglichkeit ab, diese Verknüpfung durch die Auswertung von Big Data zu verbessern. Das kollidiert aber mit dem datenschutzrechtlichen Grundsatz der „Datensparsamkeit“, § 3a BDSG. Der Menschenwürde scheint besser gedient zu sein, wenn Daten, die für die medizinische Forschung von hohem Wert sein können, vernichtet werden.³

Die Bezeichnung „Big Data“ für einen wesentlichen Aspekt des weiteren Wandels des gesellschaftlichen Wissens ist allerdings insofern irreführend, als die reine Steigerung der Quantität des Wissens, die über die Möglichkeiten der systematischen klinischen Forschung hinausweist, nicht charakteristisch für den Wandel des Wissens ist, sondern nur einen Aspekt neben anderen betrifft. Entscheidend ist vielmehr die Emergenz des neuen Phänomens der Verknüpfbarkeit zwischen Daten jenseits fester Kausalitätsmuster, die bisher in der klinischen Forschung immer weiter verfeinert worden sind – die offene, nicht-lineare „Relationalität“ der Daten, wie man formulieren könnte. Wenn die Daten

¹ W. Opaschowski, in: A. Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.1, S. 219.

² S. Leonelli, What Difference Does Quantity Make? On the Epistemology of Big Data in Biology, Big Data and Society, Juni 2014 <http://bds.sagepub.com/content/1/1/2053951714534395>.



(em.) Prof. Dr. Dr. h.c. Karl-Heinz Ladeur

Universität Hamburg;
Arbeitsschwerpunkte: Verfassungs- und Rechtstheorie, Medienrecht, globales Recht
E-Mail:
karl-heinz.ladeur@uni-hamburg.de

³ Vgl. zur Kritik den Bericht im Handelsblatt, Nr. 165, v. 28./29./30.8.2015, S. 7.

„dekontextualisiert“ werden, weil der Zusammenhang mit den „Spuren“ der faktischen Kausalketten gelockert wird⁴, bedeutet dies nicht, dass die Verknüpfungen zwischen ihnen rein empirisch⁵ – ohne Anleitung einer Theorie – erfolgen und dass dies den Übergang zu einer neuen empiristischen Wissenschaft darstellt.⁶ Deshalb darf man die Reichweite der Dekontextualisierung nicht überschätzen. Sie bedeutet nur, dass die Daten nicht mit bestimmten Zwecken verknüpft sind. Sie unterliegen der permanenten Rekontextualisierung durch *neue Zwecke* (Bottom up) oder durch spontan generierte Korrelationen und Muster, die eine Dynamik des Wissens in Anschlag bringen, die über variable Konstellationen prozessiert wird, nicht aber „die“ Wirklichkeit abbilden.⁷

Die Analyse von Big Data kann mit klinischen Untersuchungen verknüpft werden⁸, auf diese Weise können die Behandlungsmethoden verglichen werden. Zugleich können Risikopatienten besser bestimmt werden.⁹ Big Data kann partiell auch den einzelnen Ärzten einen offenen Referenzrahmen bereitstellen, über den strukturiertes Lernen erst ermöglicht wird. Aus der bloßen Beobachtung kann allein nicht gelernt werden, weil das praktische Wissen sich immer an vorhandenen Wissensstrukturen „an-kristallisieren“ muss.¹⁰

2 Probleme der Definition einer neuen „Regulierungsphilosophie“

Wie in anderen Teilen der „verflüssigten Wirklichkeit“¹¹, die eher in eine multiple Welt, eine Pluralität der Möglichkeiten transformiert worden ist, hat der Wandel Konsequenzen auch für das medizinische Wissen. Die neuen offenen Methoden der Suche nach immer neuen relevanten „Knoten“ im Netzwerk des Wissens ermöglichen eine neue relationale „Intelligibilität“ und erlauben eine Verknüpfung der Relationierungen innerhalb von Big Data mit dem in Kliniken „am Fall“ generierten Wissen¹², aber auch mit dem Wissen der praktizierenden Ärzte. Die Sammlungen von Big Data sind „sense making systems“¹³ mit offenen Zie-

len, die zu variablen Kontexten aggregiert werden, nicht aber bei der Anlage der Datensammlungen vorausgesetzt werden. „Daten finden Daten“, die Relevanz findet den Nutzer, nicht aber sind es die beteiligten Individuen oder Organisationen, die die Ziele vorformulieren.¹⁴ Deshalb bedarf es vielfach für „data driven“ Verknüpfungen und ihre Remodellierungen auch der Interoperabilität verschiedener Datenbanken, ein Problem, das z.Zt. noch schwer lösbar erscheint.¹⁵

Es vollzieht sich in der Relationierung von Wissens-elementen ständig eine Art „Umbesetzung“: D. h. obwohl oder gerade weil die „Daten“ nicht mehr für die Beantwortung bestimmter Fragen gesammelt werden (für eine vorher feststehende Art und Zahl von Fragestellungen), stellen sich jetzt nicht zuletzt methodische Probleme des „Data Cleansing“.¹⁶ Die Daten müssen standardisiert so erhoben werden, dass sie kontextfrei prozessiert werden können, während zugleich durch Rekombination mit anderen Daten ein artifizierender Kontext generiert wird, der das Ablesen von Musterbildungen erlauben soll.¹⁷ Damit wird auch die Regulierung erschwert, eben weil die Fragestellungen nicht feststehen. Deshalb ist auch vorab ein Ziel-Mittel-Verhältnis kaum zu beschreiben. Eine neue „Regulierungsphilosophie“ wird deshalb erforderlich. Sie wird vor allem eher abstrakt nach „laws of complexity“ suchen, d. h. nach Regeln der Verknüpfung zwischen Parametern, deren Muster im einzelnen ex ante schwer abschätzbar sind und ihrerseits als „evolutionary algorithms“ auf Veränderung durch Lernen angelegt sind.

„Datenzentrierte Medizin“ erscheint als eine zutreffende Beschreibung für eine Wissensbasierung, die sich weiter von der Anschauung entfernt, als dies bei der EBM der Fall ist. Die so plausibel gemachte Komplexität von Big Data, die Vielzahl der ex ante kaum abschätzbaren Verknüpfungen und Relevanzen wirft im Gesundheits- und Sozialrecht neue Fragen der Regulierung auf. Auch hier stellt sich die Frage der Kontrolle, aber auf eine neue Art: Führt Big Data wegen der zunächst über die Mittel, nicht über Zwecke gesteuerte Wissensaggregation zu „Big Government“? Wegen der konzentrierten Form der Aggregation der Daten und der Komplexität der Suchverfahren könnte diese Annahme naheliegen.

Wenn andererseits die Kombinatorik der Datenverknüpfung offen bleibt, könnte dies aber auch zu einer Pluralisierung der Recherche führen, die Datenbanken könnten dann doch einen „Varietätspool“ der Gesellschaft bilden, der die Entwicklung unterschiedlicher Lesarten und Strategien erlaubt. Dann ist zu fragen nach den Zugangsmöglichkeiten. Immer häufiger stellt sich im Bereich des – im weiteren Sinne – „geistigen Eigentums“ heute die Frage nach dessen Schutz einerseits, aber zugleich nach der *Eröffnung des Zugangs* andererseits. „Zugang“ ist das neue Problem des Status der Daten.

4 Vgl. dazu H. J. Rheinberger, Wie werden aus Spuren Daten, und wie verhalten sich Daten zu Fakten?, in: Nach Feierabend. Zürcher Jahrbuch für Wissenschaftsgeschichte 3, 2007, S. 117.

5 Vgl. allg. C. Anderson, The End of Theory. The Data Deluge Makes the Scientific Method Obsolete, WIRED 23 (2008), Juni – http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory. Auch wenn diese Auffassung zu weit geht, erfasst sie doch die grundlegende Veränderung der Konzeption der Naturwissenschaften.

6 So Anderson, ebd.; kritisch dazu und differenzierter R. Kitchin, Big Data, New Epistemologies, and Paradigm Shifts, Big Data & Society, Juni 2014 <http://bds.sagepub.com/content/1/1/2053951714528481>.

7 D. Boyd/K. Crawford, Six Provocations for Big Data, A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011 – http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431; auch Anderson, ebd.

8 M. Herland u. a., A Survey of Data Mining Using Big Data in Health Informatics, Journal of Big Data 1 (2014), Nr. 2 – <http://www.journalofbigdata.com/content/pdf/2196-1115-1-2.pdf>.

9 N. Brennan u. a., Leveraging the Big-Data Revolution. CNS is Expanding Capabilities to Spur Health System Innovation, Health Affairs 33 (2014), 1195.

10 Das hat das BVerfG, MedR 2006, 164, in seinem berühmten „Nikolaus“-Beschluss verkannt; vgl. auch die Besprechung von R. Francke/D. Hart, Die Leistungspflicht der gesetzlichen Krankenversicherung für Heilveruche, MedR 2006, 131.

11 H. Bahrami/S. Evans, Super-Flexibility for Real-Time Adaptation: Perspectives From Silicon Valley, California Management Review 2011, Heft 2, 21.

12 M. Viceconti u. a., Big Data, Big Knowledge: Big Data for Personalized Healthcare, IEEE Journal of Biomedical and Health Informatics 19 (2015), 1209.

13 A. Cavoukian/J. Jones, Privacy by Design in the Age of Big Data, 8.6.2012 – http://privacybydesign.ca/content/uploads/2012/06/pdb-big_data.pdf.

14 A. Cavoukian/D. Castro, Big Data and Innovation. Setting the Record Straight: De-Identification Does Work, 2014 <http://www2.itif.org/2014-big-data-deidentification.pdf>. Ann Cavoukian ist Datenschutzbeauftragte des Staates Ontario.

15 Sh. Hoffman/A. Podgurski, Big Bad Data: Law, Public Health, and Biomedical Databases, Journal of Medical Ethics 41 (2013), Suppl. 1, 56.

16 Hoffman/Podgurski, ebd.

17 R. Pivovarov/N. Elhadad, Automated Methods for the Summarization of Electronic Health Records, Journal of the American Medical Informatics Association (22) 2015, S. 938: Die Kehrseite der Schwierigkeiten der Gewährleistung der Interoperabilität der Datensysteme und ihrer Führung durch die Ärzte bildet die ernüchternde Einsicht, dass die Vielzahl der Daten, die vor allem über chronisch Kranke entsteht, vielleicht schwer digital zu verwalten ist, aber vom behandelnden Arzt wegen Überkomplexität erst recht nicht verarbeitet werden kann.

3 Der Wandel des „geistigen Eigentums“ an Big Data – Die Gewährleistung des Zugangs zu Gesundheitsdaten

Das „geistige Eigentum“, das auch an Datenbanken bestehen kann, ist nicht mehr nur durch seine rezeptive Nutzung durch Dritte geprägt, die sich durch Lizenzierungen sichern lässt, sondern durch seine *Verknüpfung* mit anderen Nutzungsformen wie z. B. im „Remix“ bei Musikstücken oder Videos.¹⁸ Die Verfügung über die Verknüpfungsformen von Daten ist auch eine Problematik, die sich jenseits des Datenschutzes in der Diskussion um die Stellung von „Google“ innerhalb der Medien stellt. Hier wie dort stellt sich die Frage nach der Notwendigkeit, neue Institutionen für die Informationsnetze zu entwickeln. So wäre daran zu denken, ob es nicht neuer „information broker“ bedarf, die das Recht haben könnten, über die Zugänglichkeit von Datenbanken für Dritte zu entscheiden.

Eine andere Überlegung könnte darauf zielen, diesen Datenbrokern ex post auf der Grundlage von Anregungen aus der Öffentlichkeit zu Kontrollzwecken eine Überprüfung von Ergebnissen aus der „datenzentrierten Medizin“ durch EBM-Methoden oder erfahrungsbasierte Beobachtungen zu ermöglichen. Eine weitere Möglichkeit der Kontrolle könnte darin bestehen, Methoden der Bildung und Erprobung „evolutionärer Algorithmen“ offenzulegen und einer Kontrolle durch Dritte zu unterwerfen oder zu prüfen, ob und wieweit wirtschaftliche Interessen in legitimer Weise eher nach Krankheitsbildern suchen, die lukrative Behandlungsstrategien eröffnen. Dies wirft sicher neue Probleme des Schutzes von Betriebs- und Geschäftsgeheimnissen auf. Die jetzige Kanalisierung der ärztlichen Versorgung über EBM-Methoden könnte teilweise durch die Analyse von Big Data abgelöst werden. Dies würde zugleich aber Kompensationsstrategien verlangen.

Vor allem muss der Gefahr der Monopolisierung der Verfügung über Big Data begegnet werden: Big Data tendiert zur Begünstigung der Herausbildung von Monopolen, die die Daten aggregieren und darüber verfügen. Ähnlich wie bei Suchmaschinen (Google) ist die Komplexität der potentiellen Nutzung so hoch, dass die Wirkung der Anwendung des klassischen Wettbewerbsrechts (Kartellrechts) kaum abzuschätzen und deshalb Vorsicht geboten ist.¹⁹ Allerdings stellt sich umso dringlicher die Frage, wie und zu welchen (finanziellen?) Bedingungen Zugang zur Nutzung von Big Data zu sichern ist.²⁰

4 Neue Probleme der Kontrolle der Nutzung von Big Data in der „datenbasierten Medizin“

Das Wissenssystem der Gesellschaft wandelt sich mit der „Gesellschaft der Netzwerke“, die immer mehr durch die Permeabilität der Grenzen zwischen Organisationen bestimmt ist. An die-

ser Stelle könnte sich auch eine Perspektive auf den Einbau *planerischer Komponenten* in die ärztliche Versorgung jenseits einer Basis von Standardleistungen eröffnen: Bestimmte Krankheiten, bei denen sich wegen der Verbreitung und der Heilungsmöglichkeiten auf der Grundlage der Analyse von Big Data vielversprechende Strategien abzeichnen, könnten vorrangig erforscht und behandelt werden. Hier stellen sich deshalb Probleme der Schwerpunktsetzung bei der Entwicklung des Designs von „evolutionary algorithms“ und als Kehrseite das Risiko des Einrastens in bestimmten Trajektorien. Dies ist ein Problem, das sich mit dem Aufstieg der „datenbasierten Medizin“ stellen wird. Immer mehr Behandlungsmöglichkeiten zwingen zu offenen Verfahren der Prioritätensetzung.

Auf Probleme der Haftung für Computerfehler²¹, Missachtung von Warnungen etc. sei nur hingewiesen. Es wird aber nicht davon auszugehen sein, dass die „datenzentrierte Medizin“ alle anderen Modelle der Ordnung des medizinischen Wissens ablösen wird. Dann bietet sich die Möglichkeit des Einsatzes z. B. von Methoden der EBM für die Kontrolle oder Erschütterung der Ergebnisse der „datenbasierten Medizin“.

Methoden der „datenbasierten Medizin“ lassen sich auch in der Pharmakovigilanz einsetzen. Zu den risikobasierten Modellen der Datenerhebung nach § 63b AMG könnten dann auch Erfordernisse der Standardisierung der Datenerhebung und ihrer Kompatibilität mit den Möglichkeiten der Aggregation und Auswertung von Big Data gehören, für deren Konkretisierung methodische Standards entwickelt werden könnten.²² Der breite Einsatz von Big Data in der Pharmakovigilanz könnte in der Nachmarktkontrolle ex post sehr viel wirksamer sein als die Durchführung von Tests ex ante.²³ Das Erfordernis der Durchführung von Tests im Zulassungsverfahren ließe sich möglicherweise für eine Reihe von Konstellationen durch differenzierte Auswertungsverfahren der anfallenden und zu Big Datasystemen zu aggregierenden Krankendateien abschwächen. Dies entspräche ebenfalls einer allgemeineren Tendenz zur Entwicklung einer „verflüssigten Realität“²⁴, die sich ex ante nur schwer abschätzen lässt, dafür aber umso mehr durch den Datenanfall und seine Auswertung in „Echtzeit“ oder ex post beobachten lässt.

Big Data erlaubt grundsätzlich auch die Entwicklung von Systemen, die die Wechselwirkung zwischen verschiedenen Medikamenten beobachten.²⁵ Dies ist einer der Schwachpunkte der bisherigen Pharmakovigilanz: Sehr viele Patienten benutzen mehrere Medikamente nebeneinander. Dies ist wegen der hohen Komplexität und Vielfalt der Kombinationsmöglichkeiten bisher kaum zu erfassen. Die Ermöglichung der Beobachtung (Monitoring) der Durchführung von Programmen in „real time“ (Echtzeit) könnte ein charakteristisches Merkmal der Analytik von Big Data werden.²⁶

21 M.-C. Gruber, Gefährdungshaftung für informationstechnologische Risiken: Verantwortungszurechnung im „Tanz der Agenten“, KritJ 2013, 356; Th. Söbbing, Rechtsfragen der Robotik, Zeitschrift für Innovations- und Technikrecht 2013, 43; J. Hanisch, Zivilrechtliche Haftungskonzepte für Roboter, in: E. Hilgenhof/J. P. Günther (Hrsg.), Robotik und Gesetzgebung, 2013, S. 109.

22 Auch hier stellten sich bisher und stellen sich in Zukunft Haftungsfragen: G. Wagner, Produktvigilanz und Haftung, VersR 2014, 916 (§ 63b AMG als Schutzgesetz i. S. v. § 823 Abs. 2 BGB).

23 R. Abbott, Big Data and Pharmacovigilance: Using Health Information Exchanges to Revolutionize Drug Safety, Iowa Law Review 99 (2013), 225.

24 Bahrami/Evans, Fn. 11, 21.

25 J. Wapner, Deadly Drug Combinations, Scientific American 2015 (Oktober), 29.

26 Brennan u. a., Fn. 9.

18 K. H. Ladeur, Kunstfreiheit, digitale Kunst und Urheberrecht. Zur Stellung des „Werks“ in transmedialen Netzwerken, Kunst und Recht 11 (2009), 181.

19 Vgl. zu Google G. A. Manne/J. D. Wright, Google and the Limits of Antitrust: The Case Against the Case of Google, Harvard Journal of Law and Public Policy (34) 2011, S. 172.

20 N. M. Richards/J. H. King, Three Paradoxes of Big Data, Stanford Law Review (66) 2013, S. 41; F. Hase, Forschung mit Sozialdaten, DuD 2011, 875 (zur Frage, wie weit Daten der Krankenkassen für Forschungszwecke genutzt werden können).

Zugleich würde dies aber verlangen, dass ein Anreiz für Dritte geschaffen werden müsste, Daten über den Gebrauch von Arzneimitteln zu erfassen und an die Aufsichtsbehörde weiterzuleiten.²⁷ Dies wäre dann mit einer Verpflichtung der Behörde zu verbinden, ein Untersuchungsverfahren zur Beobachtung der Wirksamkeit von Arzneimitteln einzurichten. Dann könnte die Behörde eher die Rolle der Moderation des Verfahrens übernehmen und eine größere Neutralität gegenüber dem Pharmaunternehmen wahren, da es weniger stark an der Zulassung des Arzneimittels ex ante beteiligt wäre.²⁸

Es mag etwas überraschend erscheinen, dass auch die Verfahren der Kostenerstattung im Krankenversicherungsrecht von Big Data nicht unberührt bleiben werden. Nach dem jetzigen „fee for service“-Modell werden Leistungen in der Form von Krankheitsbehandlungen, Arzneimitteln o. ä. vergütet. In Zukunft wäre es auch erforderlich oder jedenfalls denkbar, den Beitrag mit zu vergüten, den Versorger für die Entwicklung von Big Data erbringen. In den USA werden schon Modelle entwickelt und praktiziert, nach denen „sinnvoller Gebrauch“ von Gesundheitsdaten finanziell kompensiert wird.²⁹ Dies wäre wieder eine Erscheinungsform der sich entwickelnden „share economy“, in der einzelne Leistungen nicht mehr auf einzelne Erbringer zugerechnet werden können. Dies wäre die andere Seite der Öffnung von „geistigem Eigentum“ für den Zugang Dritter.³⁰

5 Datenschutz und Big Data

Wegen der Offenheit der Verknüpfungsmöglichkeiten verändert sich die Konstellation des Datenschutzes, insbesondere die Bedeutung des Begriffs der „Personenbezogenheit“.³¹ Die variable kontextuelle Generierung von Verknüpfungen und Verlaufspfaden innerhalb der „Datenlandschaften“ kann generell die Gefahr der Deanonymisierung von Daten über Personen, z. B. über die Inanspruchnahme ärztlicher Dienstleistungen steigern. Diese Entwicklung darf aber nicht mit einer Strategie der Ausweitung des Begriffs beantwortet werden. Dies würde eine Blockierung der Nutzungsmöglichkeiten von Big Data bedeuten. Die Antwort kann auch nicht in der Erhaltung oder gar Erweiterung der Datensparsamkeit bestehen.³² Hier entsteht eine für das neue Risikorecht charakteristische Ungewissheit, für die komplexitätsgerechte Strategien formuliert werden müssen.

Dies ist auch die Folie für die Beobachtung der Entwicklung zu Big Data. Ein Datenschutzkonzept, das vor allem beim Individuum ansetzt, genauer gesagt bei einem Individuum, das um

seine transindividuellen Bezüge verkürzt wird, wird diesen Entwicklungen nur wenig entgegenzusetzen können, weil die Verknüpfung von Daten so viele Entwicklungsmöglichkeiten zu versprechen scheint und deshalb von den meisten Menschen erst dann als bedenklich wahrgenommen wird, wenn konkrete Nachteile drohen. Das Datenschutzrecht muss genauer als „Risikorecht“ eingeordnet werden (anders als das klassische Polizei- und Ordnungsrecht), in dem es primär (allerdings nicht nur) auf die Gefährdung von natürlichen Netzwerken (Umwelt) oder gesellschaftlichen Netzwerken (Big Data) ankommt, nicht aber primär der Einzelne durch konkrete „Gefahren“ bedroht wird. (Selbstverständlich ist auch dies nicht auszuschließen.) Die Entwicklung von Big Data und der Methoden ihrer Verarbeitung verlangt letztlich auch nach einem neuen Verständnis der „kollektiven Intelligenz“, die sich von der persönlichen Intelligenz der Individuen unterscheidet.

Die Aggregation von Big Data und das kontinuierliche Experimentieren mit statistischen Modellen, die auf Identifikation von Verknüpfungsmustern angelegt sind, können möglicherweise Zusammenhänge offenlegen, über die sonst nur Vermutungen angestellt werden können.³³

Wenn Daten auf so unterschiedliche Weise codiert, recodiert, prozessiert und nach ganz unterschiedlichen Mustern und Rastern durchsucht werden können, müsste aber auch ein Konzept der „functional encryption“³⁴ denkbar sein, die Daten in unterschiedliche „Pakete“ zerlegt und verschiedene Ebenen des „unpacking“ ermöglicht und damit nur differenzierte Varianten der „decryption“ zulassen würde. Dafür hat sich die Bezeichnung „homomorphic encryption“³⁵ entwickelt: ein dieser Konzeption entsprechendes begrenztes Prozessieren von Daten würde zum Beispiel darin bestehen, dass die Daten als solche von Maschinen nach bestimmten Kriterien bearbeitet werden könnten, aber Namen und Internetadressen u. ä. persönliche Daten unlesbar wären.

Damit ist noch nicht die Sorge ausgeräumt, dass auch anonyme Daten durch Kombination mit offen zugänglichen Daten wieder deanonymisiert werden könnten. Wenn Daten aber auf eine Mehrzahl von unterschiedlichen Speichern verteilt werden, lässt sich jedenfalls der Vorgang der Kombination und Rekombination mit Daten, die auf unterschiedlichen Datenbanken gespeichert werden, dokumentieren, rekonstruieren und damit kontrollieren. Es könnte auch daran gearbeitet werden, solche Vorgänge automatisch zu dokumentieren und sie dem persönlichen Zugriff von Bearbeitern zu entziehen, damit auf diese Weise Kontrolle ermöglicht wird.

Jedenfalls kann die Zukunft von Big Data im Gesundheitsrecht nicht von dem Grundsatz der Datensparsamkeit bestimmt werden, der Datenschützern lieb und teuer ist.³⁶ Vielmehr muss sie von der Suche nach *Trennungs- und Verknüpfungsregeln* bestimmt sein, die auch technisch so abgesichert sind, dass Sperren nicht ohne weiteres von Insidern umgangen werden können. Die Vorteile der Verknüpfung der Gesundheitskarte mit einer Viel-

27 Vgl. zur Notwendigkeit dieser Umstellung der finanziellen Kompensation medizinischer Leistungen W. Raghupathi/V. Raghupathi, Big Data Analytics in Health Care: Promise and Potential, <http://www.hissjournal.com/content/2/1/3>.

28 J. Lewandowski u. a., Logic-Centered Architecture for Ubiquitous Health Monitoring, IEEE Journal of Biomedical Health Information 2014, 1525.

29 D. Blumenthal/M. Tavener, „Meaningful Use“ Regulation for Electronical Health Records, New England Journal of Medicine 363 2010, 501.

30 D. Wielsch, Relationales Urheberrecht. Die vielen Umwelten des Urheberrechts, Zeitschrift für geistiges Eigentum 2013, 274.

31 O. Tene/J. Polonetsky, Privacy in the Age of Big Data: A Time for Big Decisions, Stanford Law Review Online (64) 2012, S. 63; P. M. Schwartz/D. J. Solove, The PII Problem: Privacy and the Problem of Personally Identifiable Information, New York University Law Review 86 (2011), S. 1814.

32 Es wird vermutet, dass die Gesundheitsschädlichkeit des Medikaments „vioxx“ erst durch die Computeranalyse von 17.000 Krankenakten ermöglicht worden ist: R. Rubin, How Did Vioxx Debauch Happen?, USA Today, 12. 10. 2004, http://www.usatoday.com/news/health/2004-10-12-vioxx-cover_x.htm.

33 A. Pentland, Social Physics: How Good Ideas Spread – The Lessons from a New Science, 2014, S. 137.

34 S. Goldwasser u. a., Multi-input Functional Encryption, Cryptology ePrint Archive, Report 2013/727.

35 E. Naone, Homomorphic Encryption: Making Cloud Computing More Secure, MIT Technology Review Mai/Juni 2011 <http://www2.technologyreview.com/article/423683/homomorphic-encryption/>.

36 Vgl. zur Kritik H. P. Bull, Sinn und Unsinn des Datenschutzes. Persönlichkeitsrecht und Kommunikationsfreiheit in der digitalen Gesellschaft, 2015, S. 61f.

zahl von (personenbezogenen) Daten des einzelnen Patienten (die z. Zt. nicht praktiziert wird), bestehen nicht zuletzt in der Vermeidung von Doppeluntersuchungen. Es wäre zu erwägen, die Gesundheitskarte in größerem Umfang als bisher geplant nur mit freiwilligen Teilnehmern zu testen, damit auf der Grundlage der erhobenen Daten und ihrer Nutzung eine bessere Bewertungsgrundlage geschaffen wird. Dass die so genutzte Gesundheitskarte kommen wird, ist aber in einer Zeit der zunehmenden Ausbreitung von Computernetzwerken als den wichtigsten gesellschaftlichen Speichermedien ganz sicher.³⁷

Am 1.1.2016 ist das eHealth-Gesetz in Kraft getreten³⁸, auf das nicht im Einzelnen eingegangen werden kann. Jedenfalls wie ein großer Wurf wirkt es nicht. Nur hinzuweisen sei auf die absehbare rasante Entwicklung von Geräten zur privaten Erhebung von Gesundheitsdaten mittels tragbarer Minicomputer in Uhren, Armbändern etc., deren Brauchbarkeit in der nahen Zukunft noch zweifelhaft ist. Auch diese Daten könnten z. B. in Datenbanken von Versicherungen verarbeitet werden – auch damit werden neue Fragen nach der Zulässigkeit der Verknüpfung von Daten etwa nach einem Sanktionssystem aufgeworfen: Dürfen Beitragsreduktionen angeboten werden, wenn der Versicherte z. B. Daten von seinem „intelligenten“ Armband oder seiner Apple-Uhr übermittelt?

Probleme stellen sich auch bei der Frage, ob der Abschluss eines ärztlichen Behandlungsvertrages von der Einwilligung in die Übermittlung aller Gesundheitsdaten, die bei früheren Behandlungen angefallen sind, abhängig gemacht werden kann. Es ist nicht zu leugnen, dass es in vielen Fällen sinnvoll ist, so zu verfahren, zumal wenn die Auswertung der Daten durch Computerprogramme verbessert werden kann. Andererseits sind auch Fälle denkbar, in denen die Verweigerung der Daten durch den Patienten nachvollziehbar ist. Diese Bewertung kann aber häufig nicht durch den Patienten sinnvoll vorgenommen werden, während der Arzt (oder das Krankenhauspersonal) die Bedeutung der Daten ohne ihre Kenntnis nicht bewerten können. Es bleibt deshalb rätselhaft, wie in solchen Konstellationen eine „umfassende Abwägung der jeweiligen Interessen“ – so die Forderung von H. J. Menzel³⁹ – erfolgen soll.

37 Vgl. zu den USA die Diskussion um die eHealth-Card http://www.smartcardalliance.org/resources/lib/Smart_Card_Health_Benefits.pdf; <http://www.gemalto.com/govt/health>.

38 BGBl I 2015, Nr. 54, S. 2408; vgl. zur ersten Lesung des Bundestages am 3.7.2015 <http://www.bmg.bund.de/ministerium/meldungen/2015/e-health-bundestag.html> (dort auch der Link zum Entwurf des Gesetzes) – das Gesetz ist inzwischen in Kraft getreten: [http://www.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBI&start=//*\[attr_id=%27bgbl115s2408.pdf%27\]](http://www.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBI&start=//*[attr_id=%27bgbl115s2408.pdf%27]).

39 H. J. Menzel, Informationssysteme in Krankenhaus und Praxis und die Selbstbestimmung des Patienten, DuD 2011, 853, 858 – der Autor war stellv. Ham-

Auch in der Krankenpflege können Roboter und andere Assistenzsysteme eingesetzt werden (z. B. bei der Erhebung von Daten über den Gesundheitszustand der zu pflegenden Person).⁴⁰ Auch hier stellen sich Probleme bei der Frage nach der Weitergabe und der zentralisierten Auswertung von Daten insbesondere durch „lernende Sensorsysteme“, die in die Lebensumwelt integriert sind.⁴¹ Datenschutz wird auch hier praktisch eher bei der Prüfung der Nutzungsmuster ex post, nicht aber ex ante möglich sein.

6 Ergänzung der individuellen Grundrechte um „impersonale Grundrechte“ der Prozesse der Wissenserzeugung?

Jedenfalls ist der potentielle Nutzen von Big Data so erheblich, dass es nicht mehr nur um die möglichst weitreichende Beschränkung der Möglichkeiten zur Akkumulation von Daten gehen sollte – sondern um die Gestaltung der *Verknüpfungsregeln*. Auch hier könnte sich die Fruchtbarkeit des auf H. Ridder⁴² zurückgehenden Ansatzes der Konstruktion von „*impersonalen Grundrechten*“ bewähren, die transsubjektive, eine Vielzahl von Individuen und Interessen betreffende Bedingungen der Grundrechtsausübung durch ein System von sozialen Regeln absichern und nicht quasi-räumliche Handlungsbereiche. Diese Idee bedürfte einer Spezifizierung, aber sie ist einer solchen Spezifizierung jedenfalls auch eher zugänglich als ein vages Abwägungsgedenken.⁴³ Dies ist auch keine Alternative zum Individualschutz, sondern eine Ergänzung des Schutzes in multipolaren Handlungssystemen, die eine eigene selbstorganisierte Rationalität entwickeln (müssen), denen gegenüber – hier z. B. – die subjektive Einwilligung in das Prozessieren eines Systems funktionslos werden kann.

burgischer Datenschutzbeauftragter; diese Auffassung ist nicht ganz untypisch für den professionellen Datenschutz, der die Zwänge der Routinisierung von Entscheidungen in einer auf schnelles Handeln angelegten Praxis ignoriert; vgl. auch B. Hausteil, Herausforderung des Datenschutzes vor dem Hintergrund aktueller Entwicklungen in der Robotik, in: Hilgendorf/Günther (Hrsg.), Fn. 21, S. 93.

40 Vgl. Hausteil, ebd.

41 S. Beck u. a., Mit Robotern gegen den Pflegenotstand, Policy-Brief der Stiftung neue Verantwortung 4/2013, 1, <http://www.ndws.de/wp-content/uploads/2015/02/Beck2013MRG.pdf>

42 Die soziale Ordnung des Grundgesetzes, 1975, S. 85 ff.; vgl. dazu für andere Grundrechtsbereiche I. Augsberg, „Wer glauben will, muss zahlen“? Erwerb und Aufgabe der Kirchenmitgliedschaft im Spannungsfeld von Kirchenrecht und Religionsverfassungsrecht, AöR 138 (2013), 493, 527; K. H. Ladeur, Das islamische Kopftuch in der christlichen Gemeinschaftsschule, JZ 2015, 633, 635.

43 Vgl. auch zu Überlegungen, insbesondere kartellrechtliche Maßnahmen gegen Vermachtung von „Datenbesitz“ in Stellung zu bringen Bull, Fn. 36, S. 116.