Peter Schaar

Schutz der Privatsphäre im Gesundheitswesen Zu den rechtlichen Grenzen der Überwachung in der Medizin1

Zusammenfassung

IT-Systeme erzeugen große Mengen personenbezogener Gesundheitsdaten, die gegen Missbrauch, Überwachung und illegale Offenbarung geschützt werden müssen. Das Menschenrecht auf Gewährleistung der Privatsphäre erfährt im Zeitalter von Big Data einen Bedeutungszuwachs – auch im Kontext medizinischer Behandlung und Forschung. Die Vertraulichkeit persönlicher Daten muss auch im Umfeld sich schnell ändernder Technologien sichergestellt werden. Datenschutz muss in medizinische IT-Systeme eingebaut werden (Privacy by Design). Patienten müssen effektive Instrumente erhalten, um ihre Ansprüche auf Privatsphäre und Datenschutz durchzusetzen.

Abstract/Summary

IT systems generate huge amounts of sensitive medical data which have to be protected against abuse, surveillance and illegal disclosure. In the age of Big Data the human right to privacy is of growing importance even in the context of medical treatments and research. Confidentiality of personal data has to be safeguarded even in fast changing technological environment. Data protection has to be integrated in medical IT systems (privacy by design). Patients need to be provided with effective means to exercise their rights to privacy and data protection.

Schlüsselwörter

Arztgeheimnis; Big Data; Datenschutz; genetische Daten; Gesundheitsdaten; Privatsphäre.

Keywords

Medical secret; Big Data; data privacy; genetic data; health data; privacy.

DOI 10.14623/zfme.2016.1.31-39

Zwischen dem in Art. 25 der Allgemeinen Erklärung der Menschenrechte verankerten Recht auf Gesundheit und dem Menschenrecht auf Privatsphäre besteht ein enger Zusammenhang. Art. 12 lautet: »Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.«[2]

In der Informationsgesellschaft beschränkt sich der Schutz der Privatsphäre nicht mehr auf die Unverletzlichkeit der Wohnung oder des Schriftverkehrs. Mindestens genauso wichtig ist der Schutz von persönlichen Informationen, die elektronisch generiert, gespeichert und weiterverarbeitet werden. Je sensibler die entsprechenden Daten sind, desto bedeutsamer ist ihr Schutz. Niemand bestreitet ernsthaft, dass Daten über den individuellen Gesundheitszustand zu den persönlichen Informationen gehören, die besonderen Schutzes bedürfen. So stellt die EG-Datenschutzrichtlinie von 1995 Daten über die Gesundheit als »besondere Kategorie personenbezogener Daten«[3] unter besonderen Schutz und stellt strengere Anforderungen an deren Erhebung, Verarbeitung und Nutzung als bei weniger sensiblen Daten.

Bis heute entstehen die bei weitem meisten Gesundheitsdaten im Zusammenhang mit ärztlichen Behandlungen in Arztpraxen und Kliniken. Die Beziehung zwischen Arzt und Patienten ist ihrer Natur nach einseitig. Der Patient, der medizinische Hilfe benötigt, muss dem Arzt gegenüber eine Vielzahl höchst persönlicher Details offenbaren. Vielfach umfassen sie detaillierte Kenntnisse der individuellen Lebensumstände des Patienten: Informationen über seine Wohn- und Arbeitssituation, die familiären Beziehungen, Ess- und Trinkgewohnheiten, Gemütszustand, sportliche Aktivitäten.[4] Bisweilen wird im Rahmen einer Familienanamnese nach Krankheiten naher Verwandter gefragt oder es werden Daten über den Gesundheitszustand des Lebenspartners oder von Freunden erhoben. Auf diese Weise erfährt der Arzt nicht nur intime Details seines Patienten, sondern darüber hinaus auch höchst sensible Angaben über Dritte, die selbst in keiner direkten Beziehung zum Arzt stehen und deshalb auch keine Chance hatten, selbst über die Preisgabe dieser sie betreffenden Informationen zu entscheiden.

Angesichts des tiefen Einblicks, den der Arzt in die persönlichen Verhältnisse des Patienten erhält, ist das Arztgeheimnis eine der ältesten Regeln zum Schutz der Vertraulichkeit überhaupt, weitaus älter als die Menschenrechte oder gar die Gesetzgebung zum Datenschutz. Ohne Gewährleistung der Vertraulichkeit gäbe es kein Vertrauensverhältnis zwischen Arzt und Patienten und eine angemessene Behandlung von Krankheiten wäre in vielen Fällen nicht möglich.

Bereits der hippokratische Eid, dessen Ursprung im alten Griechenland liegt, beinhaltet das Prinzip des Arztgeheimnisses: »Was ich bei der Behandlung oder auch außerhalb meiner Praxis im Umgange mit Menschen sehe und höre, das man nicht weiterreden darf, werde ich verschweigen und als Geheimnis bewahren.«[5]

Geheim zu halten sind demnach nicht nur die eigentlichen Gesundheitsdaten, sondern alles, was der Arzt bei der Ausübung seines Berufs erfährt. Schon die Tatsache, dass eine Person in Behandlung ist, wird durch das Arztgeheimnis geschützt.

Viele der vom Arzt erhobenen Informationen, darauf basierende Diagnosen und Angaben über therapeutische Maßnahmen und Medikamente werden in den Patientenunterlagen erfasst. Ohne Patientenakte würde der Arzt viele Details vergessen und müsste sie bei längerfristigen oder wiederholten Behandlungen immer wieder neu erheben.

In der Vergangenheit erfolgten die ärztlichen Aufzeichnungen in Papierform. Schon deshalb beschränkten sie sich auf die wesentlichen Fakten und Schlussfolgerungen. Darüber hinaus notieren Ärzte bisweilen einige persönliche Eindrücke über den Zustand und das Verhalten des Patienten, um auf diesen bei zukünftigen Kontakten besser eingehen zu können.

Die dramatischen Veränderungen der Welt der Informationsverarbeitung, die vor einigen Dekaden begonnen haben, sind an Arztpraxen und Krankenhäusern nicht vorbeigegangen. Nicht nur aus diesem Grund sind die Rahmenbedingungen medizinischer Tätigkeiten in schnellem Wandel begriffen: Änderungen der sozialen, rechtlichen und wirtschaftlichen Rahmenbedingungen fordern Anpassungen der Gesundheitsversorgung. Auch wenn der Hausarzt in vielen Weltregionen immer noch der wichtigste Ansprechpartner der Patienten ist, werden schwerwiegende gesundheitliche Probleme in einem zunehmend differenzierten Gesundheitswesen heute arbeitsteilig behandelt. Fachärzte, spezialisierte Kliniken und Rehabilitationszentren, örtliche und regionale Gesundheitsverbünde und Laboratorien arbeiten zusammen und sind vielfältig miteinander vernetzt. Schließlich sind für die Leistungsabrechnung und die Qualitätskontrolle valide Informationen über die jeweiligen therapeutischen Maßnahmen und ggf. über ihren Erfolg – oder auch Misserfolg – erforderlich. Die im Gesundheitswesen verwendeten Daten stammen dabei nicht mehr allein von dem Patienten selbst. Medizinische Informationen werden vielmehr durch technische Geräte erzeugt und sie werden digital gespeichert und mittels Hard- und Software ausgewertet.

Die medizinische und molekularbiologische Forschung hat das Umfeld und die Methoden ärztlicher Kunst drastisch verändert. Dies gilt insbesondere für die Erforschung des menschlichen Genoms, wobei sich die Kosten für die einzelne genetische Analyse in den letzten Jahren – insbesondere durch Einsatz von Big Data-Technologien – drastisch reduziert haben.[6] Genetische Daten liefern Aussagen zum gegenwärtigen Gesundheitszustand, zu Krankheitsdispositionen und anderen Risiken, die sich weit in der Zukunft realisieren könnten. Schließlich können genetische Daten zur Entwicklung personalisierter Therapien bei Krebs und anderen schweren Krankheiten beitragen, indem sie Aussagen über die Wahrscheinlichkeiten liefern, mit denen bestimmte Medikamente oder Behandlungsmethoden bei dem jeweiligen Patienten ansprechen. Vor diesem Hintergrund sind nicht nur die genetischen Daten selbst besonders schützenswert.[7] Auch der Schutzbedarf biologischen Materials, das etwa in Biobanken vorgehalten wird, nimmt zu, denn schon aus kleinsten Partikeln lassen sich umfassende genetische Informationen gewinnen.

Genetische Informationen sind auch für Akteure außerhalb des Gesundheitswesens interessant: Wenn etwa der Arbeitgeber die genetischen Dispositionen eines Bewerbers oder Beschäftigten kennt, hat das Auswirkungen auf die Entscheidungen über die Einstellung neuer Mitarbeiter oder bei der Auswahl von Entlassungskandidaten. Kranken- und Lebensversicherungen könnten genetische Daten bei der Entscheidung über die Aufnahme eines neuen Versicherungsnehmers oder bei der Festlegung der Versicherungsprämien verwenden. Auf diese Weise könnten Menschen mit besonderen Krankheitsdispositionen aus dem Arbeitsleben ausgegrenzt werden und zugleich ihres Versicherungsschutzes verlustig gehen. Anders als in Deutschland gibt es für diese Zweitverwertung genetischer Daten in vielen Weltregionen keine rechtlichen Begrenzungen.

In jedem modernen Krankenhaus werden schon jetzt medizinische Datensätze gespeichert, die – bezogen auf jeden einzelnen Patienten – viele Megabytes umfassen und die – bezogen auf die Einrichtung – insgesamt leicht die Größenordnung von Terrabytes erreichen können. Andererseits haben im Regelfall viele Mitarbeiter der jeweiligen Institutionen Zugriff auf die Daten, vielfach ohne die erforderliche Differenzierung der Zugriffsrechte und ohne eine angemessene technische Absicherung. Nicht nur das medizinische Personal der jeweiligen Institutionen hat Zugriff auf die Daten, sondern auch Mitarbeiter technischer Dienstleister, welche die IT betreuen.[8] Zunehmend gelangen medizinische Daten auch zu Sozialversicherungsträgern oder sie werden an pharmazeutische Unternehmen und Forschungseinrichtungen übermittelt, bisweilen ohne Kenntnis der Betroffenen.[9]

Medizinische Daten bilden nur ein – wenn auch besonders sensibles – Segment der massenhaft bei der Digitalisierung von Geschäftsprozessen und Dienstleistungen anfallenden personenbezogenen Daten. In einem Umfeld der allgegenwärtigen Datenverarbeitung (ubiquitous computing) und des »Internets der Dinge« werden medizinische Daten und aus sonstigen Quellen stammende Informationen miteinander verknüpft.

Nicht nur medizinische Geräte, die ein besonderes Zulassungsverfahren durchlaufen und bestimmten Qualitätskriterien entsprechen müssen, generieren Gesundheitsdaten. Auch Smartphones und Fitnesstracker erzeugen Informationen über den Gesundheitszustand und sie zeichnen das persönliche Verhalten auf – Schrittzahl, sportliche Aktivitäten, Herzfrequenz, Blutdruck, Schlaf- und Ernährungsgewohnheiten. Diese Daten werden regelmäßig in der Cloud gespeichert, also auf Servern im Internet. Dies geschieht weitgehend ohne jegliche Kontrollmöglichkeiten des Betroffenen, auf den sie sich beziehen.

Viele im digitalen Alltag anfallende Daten können mit medizinischen Informationen verknüpft werden: Was wir kaufen, wie wir uns im realen Leben und im Internet bewegen und wer unsere echten oder virtuellen Freunde sind. Persönliche Verhaltens- und Interessenprofile können Aussagen über den individuellen Gesundheitszustand ermöglichen. Eines der am häufigsten in den Medien diskutierten Beispiele ist der Fall einer jungen Frau, deren Schwangerschaft von einer Supermarktkette auf Grund ihres geänderten Einkaufsverhaltens – gesündere Nahrungsmittel, Hautcremes usw. – aufgedeckt wurde. Die Eltern der Frau, von gezielt auf Schwangere abzielender Werbung an die Tochter aufgeschreckt, erfuhren so von der Schwangerschaft, über die die Tochter noch nichts gesagt hatte.[10]

Dieses Beispiel belegt, dass selbst Daten, die auf den ersten Blick als nicht sonderlich sensibel erscheinen und deshalb nicht besonders geschützt sind und die als Basis für Auswertungen dienen, ihrerseits höchst sensible Ergebnisse liefern können, auch im Hinblick auf den individuellen Gesundheitszustand. Auch deshalb muss der Umgang mit medizinischen Daten im Kontext der informationstechnischen Entwicklung auch außerhalb des Gesundheitssektors gesehen werden.

Im Jahr 1890 haben die US-Juristen Samuel Warren und Louis D. Brandeis in den USA ihren berühmten Aufsatz zum »Right to Privacy« veröffentlicht.[11] Sie begründeten darin ein Recht, allein gelassen zu werden (»right to be le(f)t alone«), abgeleitet aus den in der US-Verfassung verankerten Grundrechten, insbesondere dem Schutz vor staatlicher Willkür und dem Schutz des Privateigentums. Im ausgehenden 19. Jahrhundert, war »Privacy« eine angemessene Antwort auf die zeitgenössischen Gefährdungen, die von

dem Einsatz der seinerzeitigen Techniken ausgingen, speziell von der Fotografie, weil professionelle Fotografen gezielt das Privatleben von mehr oder weniger prominenten Mitbürgern ablichteten und ihre Fotos an Zeitungen verkauften.

Das derzeitige Datenschutzrecht wurde in den letzten Dekaden des 20. Jahrhunderts entwickelt. Das weltweit erste Datenschutzgesetz, dasjenige des Landes Hessen, wurde 1970 verabschiedet, die EG-Datenschutzverordnung stammt aus dem Jahr 1995.[12] Seither hat sich die Welt der Datenverarbeitung dramatisch fortentwickelt. Vor 50 Jahren wurden die meisten Daten noch manuell verarbeitet und Computer hatten – verglichen mit heute – geradezu lächerliche Verarbeitungskapazitäten. Die Informationstechnik stand ganz überwiegend hinter Mauern in abgeschotteten Rechenzentren – fernab von Büros und anderen Arbeitsplätzen oder gar dem häuslichen Wohnzimmer. Grenzüberschreitende Datenübermittlungen fanden zwar statt, waren jedoch die Ausnahme. Gentests waren zwar Gegenstand von Science Fiction, von ihrer Realisierung war die Wissenschaft noch weit entfernt.

Wenn heute über Informationsverarbeitung diskutiert wird, gehört »Big Data« zu den am häufigsten verwendeten Begriffen. Big Data beschreibt den Umgang mit extrem gewachsenen Datenvolumina, die aus unterschiedlichsten Quellen stammen, und die in großer Geschwindigkeit, quasi in Echtzeit, ausgewertet werden.[13] In Big Data werden große Hoffnungen gesetzt, auch im Hinblick auf die Medizin. Bisweilen hört man die Aussage, dass sich neue Erkenntnisse allein aus statistischen Zusammenhängen gewinnen ließen, und zwar auch ohne die zu Grunde liegenden Prozesse zu verstehen – der Fokus liegt auf Korrelation statt auf Kausalität. Auch wer – wie der Autor – die Vorstellung von der Entbehrlichkeit analytischen Denkens angesichts der riesigen Datenmengen nicht teilt, kann sich der Erkenntnis nicht verschließen, dass Big Data unser Leben dramatisch verändert und dass die Bedeutung entsprechender Ansätze angesichts der ungebremsten technologischen Entwicklung weiter zunimmt – auch in der Medizin.

Der Übergang von analoger zu digitaler Informationsverarbeitung ist inzwischen soweit fortgeschritten, dass die analoge Speicherung rein quantitativ kaum noch ins Gewicht fällt. Kaum eine Arztpraxis und kein Krankenhaus kommen heute ohne Computerunterstützung aus. Immer leistungsfähigere IT-Systeme erzeugen immer mehr Daten. Begrenzter Speicherplatz ist angesichts neuer Speicherungstechniken und des dramatischen Preisverfalls bei den Speichermedien heute kein Thema mehr. Neue Konzepte erlauben etwa den Betrieb von »In-Memory-Datenbanken«, welche riesige Datenmengen verglichen mit älteren Datenbanktechniken in einer vielfach höheren Geschwindigkeit verarbeiten.[14]

Alle modernen Netzwerke fördern die De-Lokalisierung der Informationsverarbeitung. Daten reisen im Internet in Sekundenbruchteilen um die Welt und werden auf global verteilten Servern gespeichert, wobei der Ort der Verarbeitung und Speicherung weder vom Betroffenen noch von der für die Datenverarbeitung verantwortlichen Stelle letztlich zu kontrollieren ist. Durch nationales Recht definierte Vorgaben für den Umgang mit personenbezogenen Daten stoßen deshalb auf faktische Grenzen. Aber auch in seiner Substanz ist das Datenschutzrecht unter Druck geraten.[15] Hergebrachte Grundsätze des Datenschutzes werden durch die schnelle informationstechnische Entwicklung in Frage gestellt, insbesondere die Prinzipien der Erforderlichkeit und der Zweckbindung. In der durch Big Data geprägten Welt geht es nicht um Begrenzung der Datenerhe-

bung oder um Datenminimierung. Vielmehr funktionieren entsprechende Modelle umso besser, je mehr Daten gesammelt und ausgewertet werden.

Die wachsenden Datenmengen sind in den letzten Jahren zur wichtigsten Finanzierungsquelle von Internetdiensten geworden. Daten, die von den Nutzern freiwillig geliefert worden sind, etwa bei ihren Aktivitäten in sozialen Netzwerken, werden mit Informationen anderen Ursprungs zusammengeführt und sind im wahrsten Wortsinne Geld wert. So entstehen bei der Internetnutzung, beim Telefonieren oder beim Autofahren digitale Datenspuren (»Metadaten«), die ggf. zusammen mit den von den Betroffenen freigegebenen Inhalten (Statusmeldungen bei Facebook oder Twitter-Kommentare, »Freundes«listen und Fotos) sehr aussagekräftige persönliche Profile liefern, die sowohl bei Unternehmen als auch bei staatlichen Stellen auf reges Interesse stoßen. Dabei haben Gesundheitsdaten ein besonders großes wirtschaftliches Potenzial,[16] insbesondere wenn es um die Identifikation von Patienten mit schweren Krankheiten geht, bei denen sehr teure Medikamente und hochpreisige Behandlungsmethoden in Frage kommen. Andererseits darf nicht übersehen werden, dass Big Data neue Möglichkeiten mit sich bringt, etwa zum frühzeitigen Erkennen bestimmter Gesundheitsrisiken oder bei der Verordnung wirksamer Medikamente.

Angesichts der weiterhin ungebremsten informationstechnologischen Entwicklung sind überzeugende datenschutzrechtliche Lösungen dringend erforderlich, die aber nicht verhindern, dass die Gesellschaft und jeder Einzelne an den Vorteilen einer immer effektiveren Datenverarbeitung partizipieren. Ziel eines zeitgemäßen Datenschutzes kann nicht sein, die informationstechnische Entwicklung zurückzudrehen. Ein Zurück in das analoge Zeitalter wird es nicht geben.

Im Mittelpunkt derartiger Lösungen muss stehen, dass nicht alles mit Informationen gemacht werden darf, was technisch möglich ist. Umgekehrt müssen wir uns eingestehen, dass bestimmte Regeln zum Umgang mit Daten, die in einer durch »small Data« geprägten Welt formuliert worden sind, in einem Umfeld allgegenwärtiger Registrierung und von Big Data nicht mehr effektiv funktionieren. Im Mittelpunkt des derzeitigen Datenschutzrechts steht das einzelne Datum, das für einen bestimmten Zweck erhoben und verarbeitet wird und das nur ausnahmsweise – bei Vorliegen einer gesetzlichen Erlaubnis oder mit Einwilligung des Betroffenen – für andere Zwecke verarbeitet werden darf (Zweckbindung). Die traditionelle datenschutzrechtliche Kernfrage lautet: Welche personenbezogenen Daten werden für die Erfüllung eines legitimen Zwecks benötigt? Die zentralen Kriterien sind die Relevanz und Erforderlichkeit bezogen auf einen bestimmten, vorab bekannten Zweck. Mit anderen Worten: Das derzeitige Datenschutzrecht betrachtet die Informationsverarbeitung aus der Mikro-Perspektive. Dagegen sehen Unternehmen und staatliche Stellen auf die Datenverarbeitung zunehmend aus einer Makro-Perspektive: Wie können die aus verschiedenen Quellen stammenden Daten genutzt werden, um Zusammenhänge aufzudecken oder Probleme frühzeitig zu erkennen? Die (personalisierten) Massendaten werden nicht zu Unrecht als das »neue Öl« der Informationsgesellschaft verstanden.[17]

Die Datenschutz-Community ist deshalb zunehmend mit der Frage konfrontiert, wie das Datenschutzrecht, dessen zentrale Ziele – informationelle Selbstbestimmung, Vertraulichkeit des privaten Bereichs, Schutz vor Missbrauch persönlicher Daten – nach wie vor gültig sind, in dem neuen informationstechnischen Umfeld durchgesetzt werden können. Überzeugende Lösungen müssen die Mikro-Perspektive stärker als bisher mit

systemischem Denken verknüpfen. Technologische Fragestellungen können allein durch Konzepte, die auf Verbot, Erlaubnis und individueller Einwilligung beruhen, nicht befriedigend beantwortet werden. Technischen Konzepten wie der Anonymisierung und der Verwendung pseudonymer statt direkt mit einer Person verknüpfter Daten kommt dabei zentrale Bedeutung zu. Entsprechende Instrumente gehören in den Werkzeugkasten des modernen Datenschutzes ebenso wie Verpflichtungen für die Datenverarbeiter, sich vorab mit den Auswirkungen und Risiken von Verfahren auseinanderzusetzen und datenschutzrechtliche Anforderungen frühzeitig in IT-Systeme zu integrieren (Privacy by Design).[18]

Letztlich kann es nicht darum gehen, die Grund- und Menschenrechte unter der Flagge des technischen Fortschritts einzuschränken oder gar zu ignorieren. Vielmehr müssen rechtliche und technische Verfahren entwickelt und eingesetzt werden, die dem Einzelnen und der Gesellschaft wieder mehr Kontrolle über die Daten geben. Nur wenn den Menschen ihr Recht auf informationelle Selbstbestimmung – nach der Feststellung des deutschen Bundesverfassungsgerichts[19] ein Grundrecht! – garantiert wird, können sie ihre Persönlichkeit frei entfalten und ihre anderen Grundrechte wahrnehmen.

Gerade bei sensiblen Informationen wie den Gesundheitsdaten bleibt die Zweckbestimmung ein zentrales Anliegen, auch unter den sich rapide verändernden technischen Bedingungen. Sofern diese Daten für andere Zwecke, insbesondere für Forschung verwendet werden sollen, bedarf dies weiterhin der individuellen Einwilligung des Betroffenen. Andererseits müssen die Daten gerade bei Zweckänderungen anonymisiert[20] werden, um so das Risiko negativer Folgen für den Einzelnen zu begrenzen. In den meisten Fällen benötigen Forscher für wissenschaftliche Studien weder den Namen noch sonstige eine Person direkt identifizierende Merkmale.

Zudem müssen die Grenzen zwischen akzeptabler und unzulässiger Datenverwendung schärfer gezogen und auch durchgesetzt werden. Dies betrifft zudem den Umgang mit anonymen Daten – jedenfalls dann, wenn diese Daten letztlich doch auf einzelne Personen oder Gruppen bezogen werden, wie dies etwa beim »Scoring« geschieht. Die Scores, also individuelle Kopfnoten, die allein aus dem Vergleich einer Person mit einer statistischen Vergleichsgruppe resultieren, bergen erhebliche Gefahren der Diskriminierung in sich.[21] Diese Gefahr besteht auch bei der personalisierten Medizin, jedenfalls dann, wenn einzelnen Patienten bestimmte Therapien vorenthalten werden, nur weil sie bei anderen Personen mit ähnlichem Gentyp weniger wirksam waren.

Schließlich darf nicht vergessen werden, dass es einen Kernbereich privater Lebensgestaltung gibt, der weder der privatwirtschaftlichen noch der staatlichen Überwachung zugänglich ist, wie das Bundesverfassungsgericht in einer Reihe von Entscheidungen unmissverständlich klargestellt hat.[22] Niemand darf diese rote Linie überschreiten. Individuelle Gesundheitsdaten dürfen nur mit Wissen des Betroffenen und bei Vorliegen einer expliziten, auf die jeweilige Verwendung bezogenen Einwilligung verarbeitet werden.

Um auf den Ausgangspunkt zurückzukommen: Das Recht auf Privatsphäre hat in Zeiten immer effektiverer Registrierung und Überwachung größere Bedeutung denn je. Das gilt gerade für das Gesundheitswesen, in dem stärker als in nahezu anderen Bereichen eine Vielzahl sensibelster persönlicher Daten verarbeitet werden.

ANMERKUNGEN

1 Der vorliegende Beitrag basiert auf einem englischen Vortrag des Autors im Rahmen der internationalen Tagung »The Right to Health – an Empty Promise?« (Berlin, 14.–16.09.2015) des EFI-Projekts »Human Rights in Healthcare« (FAU).

2 Vereinte Nationen, *Resolution der Generalversammlung vom 10. Dezember 1948*.

3 Art. 8 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 23.11.1995, EG-Amtsblatt Nr. L 281 1995, 31.

4 Privacy Protection Study Commission, *Personal Privacy in an Information Society*, Washington 1977, 282.

5 Vgl. K. Deichgräber (1983), *Der hippokratische Eid*, Stuttgart 41983 und H. Diller, *Hippokrates. Ausgewählte Schriften*, Stuttgart 1994; vgl. auch D. Peel, *The future of Health Privacy*, in: M. Rotenberg/J. Scott/J: Horwith (Eds.), Privacy in the Modern Age, New York 2015, hier: 175.

6 Vgl. Executive Office of the President, *Big data: Seizing opportunities, preserving values,* Washington 2014, hier: 15.

7 J. A. Magnuson/P. W. O'Carroll, *Introduction to Public Health Informatics*, in: J. A. Magnuson, J. A./P. C. Fu, (Eds.), Public Health Informatics and Information Systems, London 2014, hier: 15.

8 Vgl. Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, 22. Tätigkeitsbericht (2008/9), 60.

9 Vgl. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 24. Tätigkeitsbericht (2011/2012), 144 ff.

10 Vgl. V. Mayer-Schönberger/K. Cukier, *Big Data – Die Revolution, die unser Leben verändern wird,* München 2013, München, hier: 76.

11 S. Warren/L. Brandeis, *The right to privacy,* in: Harvard Law Review 4 (1890) 193–220, hier: 195.

12 Richtlinie 95/46/EG, vgl. Fn 3.

13 Vgl. T. Weichert, *Big Data – Eine Herausforderung für den Datenschutz*, in: H. Geiselberger, T. Moorstedt (Hrsg.), Big Data – Das neue Versprechen der Allwissenheit, Berlin 2013, 131–148, hier: 133.

14 Vgl. etwa M. Steinbrecher/J.-H. Boese, Real-time data mining with in-memory database technology, in: C. Moewes/A. Nürnberger (Eds.) Computational intelligence in intelligent data analysis, Berlin/Heidelberg 2014, 275–284, hier: 275 ff.

15 Vgl. O. Tene/J. Polonetsky, *Privacy in the Age of Big Data*, in: Stanford Law Review Online 2012, 64; vgl. auch P. Schaar, *Datenschutz in Zeiten von Big Data*, in: HMD – Praxis der Wirtschaftsinformatik 2014, 840 und Weichert (Anm. 13).

16 Vgl. Peel (Anm. 5) 175.

17 Erstmals vermutlich verwendet von Humby, 1986, http://ana.blogs.com/maestros/2006/11/data_is_the_new.html (Abruf am 24.11.2015).

18 32nd International Conference of Data Protection and Privacy Commissioners, Privacy by Design Resolution, Jerusalem, 2010; https://www.ipc.on.ca/site_documents/pbd-resolution.pdf (Abruf am 24.11.2015).

19 Bundesverfassungsgericht, Urteil vom 15. Dezember 1983 (»Volkszählungsurteil«), 1 BvR 209/83, BVerfGE 65, 1 ff.

20 Definition in § 3 Abs. 6 Bundesdatenschutzgesetz.

21 Vgl. P. Schaar, *Scoring – datenbasierte Bonitätseinschätzung zum Vorteil von Verbrauchern und Wirtschaft? Rede auf der Konferenz Herausforderungen und Chancen in einer digitalisierten Welt am 15. März 2007*, vgl. http://www.bfdi.bund.de/DE/Infothek/Reden_Interviews/2007/Konferenz_1503.html?cms_templateQueryString=scoring&cms_sortOrder=score+desc (Abruf am 24.11.2015).

22 Vgl. insb. Bundesverfassungsgericht, Urteil vom 3. März 2004 (»Großer Lauschangriff«), 1 BvR 2378/98, BVerfGE 109, 279 ff.

LITERATURHINWEISE

Aust, H. P., *Spionage im Zeitalter von Big Data. Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht,* in: Archiv des Völkerrechts 52 (2014) 375–406.

BITKOM-Arbeitskreis Big Data, *Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte*, Leitfaden, BITKOM, September 2012, www.bitkom.org/de/publikationen/ 38337_73446.aspx (Abruf am 12.09.2015).

Eckart, W. U., *Geschichte der Medizin. Fakten, Konzepte, Haltungen,*[6]Berlin/Heidelberg 2009.

November, J. A., *Biomedical computing. Digitizing life in the United States*, Baltimore 2012.

Pietsch, W., *Big Data in der Medizin: Sprechstunde beim Superrechner,* in: Spiegel Online, Juli 2013, www.spiegel.de/wissenschaft/medizin/big-datawundermittel-auch-fuer-diemedizin-a-911333.html (Abruf am 12.09.2015).

Schaar, P., *Verbraucherpolitik in der digitalen Welt – Der gläserne Kunde? Stellungnahme, Bundesbeauftragter für den Datenschutz,* April 2005, http://www. bfdi.bund.de/SharedDocs/Publikationen/VerbraucherpolitikInDerDigitalenWelt-DerGlaeserneKunde.html (Abruf am 12.09.2015).

Schaar, P., *Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft,* München 2007.

Trojanow, I./Zeh, J., *Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte*, München 4 2014.