Christoph Bauer
Frank Eickmeier
Michael Eckard

E-Health: Datenschutz und Datensicherheit

Herausforderungen und Lösungen im IoT-Zeitalter

Springer Gabler

E-Health: Datenschutz und Datensicherheit

Christoph Bauer · Frank Eickmeier
Michael Eckard

E-Health: Datenschutz und Datensicherheit

Herausforderungen und Lösungen im IoT-Zeitalter

Unter redaktioneller Mitarbeit von Kerstin Kafke, Daniela Klette und Astrid Schwaner

Springer Gabler

Christoph Bauer
HSBA – Hamburg School of Business und
ePrivacy GmbH
Hamburg, Deutschland

Michael Eckard
ePrivacy GmbH
Hamburg, Deutschland

Frank Eickmeier
UNVERZAGT VON HAVE und
ePrivacy GmbH
Hamburg, Deutschland

ISBN 978-3-658-15090-7 ISBN 978-3-658-15091-4 (eBook)
https://doi.org/10.1007/978-3-658-15091-4

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Gabler ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Die Digitalisierung des Gesundheitswesens hat vor kurzem in Deutschland begonnen und schreitet mit großen Schritten voran. Startups ebenso wie Großkonzerne entwickeln Technologien und Anwendungen, um die Gesundheitsversorgung einer alternden Gesellschaft auch in den kommenden Jahrzehnten zu gewährleisten. Fitnesstracker und andere Analysetools bieten gesundheitsbewussten Patienten die Möglichkeit, ihren Körper rund um die Uhr zu überwachen – und datenverarbeitenden Firmen und Herstellern neue Einnahmequellen.

Bei dieser rasanten Entwicklung werden die Themen Datenschutz und Datensicherheit häufig als Hindernis gesehen, was sie nicht sein müssen. Jedenfalls sind der Datenschutz und die Datensicherheit von enormer Bedeutung: Gesundheitsdaten sind hochsensibel und können in den falschen Händen großen Schaden anrichten. Gerade jetzt, wo viele Produkte und Geschäftsmodelle sich noch in der Entstehung befinden, ist der richtige Moment, um praktikable und sichere Strategien für den verantwortungsvollen Umgang mit sensitiven Gesundheitsdaten zu entwickeln.

Datenschutz ist ein Grundrecht, eine Herausforderung – und ein Wettbewerbsvorteil. Deshalb haben wir uns entschieden, ein Fachbuch als Handreichung für Hersteller, Entwickler, medizinisches Fachpersonal und interessierte Patienten herauszugeben, das sich genau dieser Herausforderung stellt. Wir möchten mit dem vorliegenden Buch praxisnahe Lösungsmöglichkeiten aufzeigen, um eine verantwortungsvolle Datenschutzpraxis schon beim Design der Produkte zu fördern. Dabei beziehen wir schwerpunktmäßig gerade auch das neue Datenschutzrecht (Datenschutz-Grundverordnung) mit ein, das ab Mai 2018 direkte Gültigkeit in allen EU-Ländern hat. Auf weitere landesspezifische Regelungen wird i. d. R. kein Bezug genommen, da diese den Rahmen dieses Buches sprengen würden.

Teil I des Buchs führt in die Entwicklung datenverarbeitender Produkte in der E-Health-Branche ein: Welche Produkte und Technologien gibt es im digitalen Gesundheitsbereich? Welche Daten werden mit welchen Methoden erhoben und zu welchen Zwecken (Kap. 1)? Wie entwickelte sich der E-Health-Markt in den vergangenen Jahren (Kap. 2)?

Teil II stellt die aktuellen Herausforderungen rund um Datenschutz und Datensicherheit bei E-Health zusammen und nennt Lösungsansätze: Welche Grundprinzipien des Datenschutzes müssen Anbieter von E-Health-Produkten einhalten (Kap. 3)? Welche rechtlichen Rahmenbedingungen beeinflussen die digitale Gesundheitsbranche in Deutschland (Kap. 4)? Welche wichtigen rechtlichen Anforderungen existieren zusätzlich international (Kap. 5)? Welche technischen Anforderungen müssen Anbieter erfüllen, um Datensicherheit zu gewährleisten (Kap. 6)?

In Teil III bieten die Ergebnisse empirischer Studien Einblicke in den aktuellen Stand von Datenschutz und Datensicherheit bei E-Health-Produkten (Kap. 7 und 8). Das Abschlusskapitel fasst gebündelt und praxisnah die konkreten technischen bzw. rechtlichen Anforderungen für die Bereiche Datenschutz und Datensicherheit zusammen (Kap. 9).

Wir hoffen, Ihnen damit eine erste Orientierung im unübersichtlichen Feld der technischen und juristischen Anforderungen an Datenschutz und Datensicherheit im Bereich E-Health zu geben. Unser großer Dank gilt Kerstin Kafke, Daniela Klette, Britt Petersen und Astrid Schwaner für die inhaltliche Mitwirkung, für viele weitere Hinweise und die umfassende Redaktion des Buches.

Hamburg
im Mai 2017

Prof. Dr. Christoph Bauer
Dr. Frank Eickmeier
Michael Eckard

Inhaltsverzeichnis

Teil I

Das Internet der Dinge

Der vernetzte Alltag und Daten

1

Christoph Bauer

Der Wecker reißt Sie jäh aus dem Schlaf, denn Ihr smartes Armband zeigt an, dass Sie nach einer unruhigen Schlafperiode gegen 03.00 Uhr nun um 06.17 Uhr das Ende einer Tiefschlafphase erreicht haben und es die beste Zeit ist, aufzustehen. Hoch motiviert gehen Sie joggen, das smarte Armband misst Ihren Puls, Ihre Laufgeschwindigkeit und die zurückgelegte Strecke: Heute sind Sie trotz des nächtlichen Aufwachens ziemlich fit. Die eingebauten Sensoren haben außerdem Ihrem Schweiß entnommen, dass Sie heute besonders viel Vitamin C brauchen. Daher schneiden Sie sich nach der Laufrunde die empfohlenen Obststücke klein, als Ihnen Ihr Smartphone eine Push-Meldung sendet, dass Sie vor dem Frühstück ihr blutdrucksenkendes Medikament einnehmen müssen. Sie tun das, klicken auf „erledigt" und Ihr Hausarzt erhält sogleich die Nachricht, dass Sie das Medikament wie vorgeschrieben genommen haben und dass Ihre Packung in sieben Tagen leer sein wird. Seine Praxis sendet daher automatisch ein neues elektronisches Rezept an die Apotheke Ihres Vertrauens und diese wird Sie morgen Vormittag mit einer Push-Meldung daran erinnern, es in der Mittagspause abzuholen.

Die Digitalisierung hat neben anderen Lebensbereichen auch den Bereich der Gesundheit erfasst. Menschen haben immer ihren Körper und seine Gesundheit beobachtet und erforscht. Nun ist das durch den technischen Fortschritt – die Entwicklung von bezahlbaren Kleinstcomputern, die Smartphonedichte in Industriestaaten und das wachsende Angebot von Gesundheits-Apps – in bisher undenkbar großem Maßstab möglich. Derzeit sind über 100.000 Fitness- und Gesundheits-Apps auf dem Markt.[1] Der Trend, auf seine Gesundheit und Fitness zu achten, verbindet sich heute mit den technischen Möglichkeiten, umfangreiche Körperdaten selbst zu erfassen (Self-Tracking).[2] Dennoch befinden Experten, dass sich die Gesundheitsbranche „noch am Anfang der digitalen

[1]Albrecht et al. (2016, S. 69). Siehe auch Lupton (2016, S. 6).

[2]Campillo-Lundbeck (2016).

C. Bauer et al., *E-Health: Datenschutz und Datensicherheit,*
https://doi.org/10.1007/978-3-658-15091-4_1

Transformation“[3] befindet: Bis die Digitalisierung sich im gesamten Gesundheitssystem Deutschlands durchgesetzt hat, wird wohl noch einige Zeit vergehen. Das individuelle Self-Tracking könnte sich allerdings bald ausbreiten: „Die Verbreitung der Selbstvermessung wird in den kommenden Jahren weiter zunehmen und sich zum Massenphänomen entwickeln, welches fest in die Systeme der Gesundheitswirtschaft integriert ist.“[4] Studien belegen das wachsende Interesse an einer elektronischen Speicherung der eigenen Patientendaten gerade bei Patienten, die mindestens einmal pro Monat zum Arzt gehen.[5]

Die Digitalisierung des Gesundheitssystems bietet Chancen, den demografischen Wandel aufzufangen: Unter anderem ermöglicht sie massive Kosteneinsparungen durch vereinfachte digitale Kommunikationswege zwischen Arztpraxen, Versicherern, Krankenhäusern und Patienten sowie durch mehr Eigenverantwortung mündiger Patienten, die ihre Patientenakte künftig digital selbst verwalten.[6] Die Nutzer profitieren davon, dass neue Kommunikationsmedien und -technologien ihren Alltag erleichtern. Der damit einhergehenden „Erosion der Privatsphäre“[7] bringen sie allerdings wenig Aufmerksamkeit entgegen. Vor allem im Bereich des Datenschutzes stellt die Digitalisierung unsere Gesundheitsbranche vor neue Herausforderungen: Von den aktuell angebotenen Apps sind nur die wenigsten anerkannte Medizinprodukte nach dem Medizinproduktegesetz (MPG).[8] Dabei deckt die Zertifizierung als Medizinprodukt die Bereiche Datenschutz und Datensicherheit kaum ab. Die Qualitäts- und Sicherheitsunterschiede sind enorm. Gesundheit, Lifestyle und Fitness vermischen sich auf einem riesigen wachsenden Markt, dessen zahlreiche Anbieter niemand mehr alle kennen kann. Wer welche Daten verarbeitet und an wen weiterleitet, ist oft nicht transparent.

Alle E-Health-Anwendungen basieren jedoch auf den Daten ihrer Nutzer. Diese Daten sind zum Teil höchst sensibel, denn sie verraten viel über den Gesundheitszustand des Nutzers und sollten weder in falsche Hände geraten, noch sollten Medikationen manipuliert werden können. Sowohl Patienten als auch medizinisches Fachpersonal verfügen noch über zu wenig Bewusstsein für Datenschutzrisiken bei Medizin-Apps.[9] Aufgrund der sich schnell weiterentwickelnden Technologien und sich wandelnden Sicherheitsanforderungen ist es für die Anbieter schwierig, dem Datenschutz gerecht zu werden. Bessere Orientierungsmöglichkeiten sowie verlässliche Qualitäts- und Datenschutzstandards sind nötig. Dieses Buch ist als Fachbuch für E-Health-Akteure gedacht, vom Technologieanbieter über medizinisches Fachpersonal bis zum gut informierten Nutzer.

[3] BVDW (2016, S. 13).

[4] Andelfinger und Hänisch (2016, S. 51). Siehe auch DIVSI (2016, S. 7).

[5] Stiftung Münch (2015).

[6] Andelfinger und Hänisch (2016, S. 26).

[7] Heckmann (2012, S. 277).

[8] BfArM (2015).

[9] CHARISMHA (2016, S. 316).

1.1 Definition von E-Health, mHealth, Wearables und IoT

Da die Begriffe aus dem Bereich E-Health noch sehr jung sind und sich stetig weiterentwickeln, liegen noch kaum einheitliche Definitionen vor.[10] Bedingung für eine produktive Diskussion über den Umgang mit sensitiven Gesundheitsdaten im Spannungsfeld von Datenschutz und Informationsfreiheit ist jedoch eine klare Definition der Begriffe.[11] Im Folgenden werden die wichtigsten Termini als Grundlage für die weiteren Kapitel definiert.

Beim Oberbegriff **E-Health**[12] folgt dieses Fachbuch der Definition und Schreibweise des Bundesministeriums für Gesundheit: „Unter E-Health fasst man Anwendungen zusammen, die für die Behandlung und Betreuung von Patientinnen und Patienten die Möglichkeiten nutzen, die moderne Informations- und Kommunikationstechnologien (IKT) bieten."[13] Dazu zählen Online-Angebote, z. B. interaktives Gesundheitscoaching, Telemedizin und auch der Bereich Mobile Health, kurz **mHealth.** Diese ebenso junge wie wachstumsstarke Unterkategorie von E-Health kann man als „eine durch Mobilgeräte elektronisch unterstützte Gesundheits-Versorgung"[14] definieren. Hier hat sich die Schreibweise aus der Informatik mit kleinem m bisher durchgesetzt. mHealth umfasst sowohl die mobile Hard- als auch die Software. Vom Oberbegriff E-Health, der beispielsweise auch Krankenhausinformationssysteme umfasst, grenzt sich mHealth durch die Tragbarkeit der verwendeten Geräte ab.

Die Hardware im Bereich mHealth sind neben Smartphones und anderen Kleinstgeräten häufig **Wearables,** am Körper getragene Kleinstcomputer.[15] Gesundheit und Fitness sind laut der International Working Group on Data Protection in Telecommunications zwei Haupteinsatzgebiete von Wearables. Beispiele für Wearables sind etwa Fitnesstracker oder tragbare Messgeräte zur Überwachung des Blutzuckerspiegels und anderer Gesundheitswerte. Die Wirkweise ist bereits manchmal vollautomatisch, beispielsweise beim Diabetiker-Pflaster, das anhand der gemessenen Werte vollautomatisch Insulin abgibt. Wearables liefern künftig voraussichtlich noch bessere Messergebnisse als Smartphones, da sie direkt am Körper getragen werden und zunehmend darauf ausgelegt sind, immer getragen zu werden, beispielsweise smarte Armbanduhren oder Armbänder. Wearables sind entweder mit anderen Geräten, z. B. einem Smartphone oder Computer, über Bluetooth oder andere Sender vernetzt, oder sie übermitteln die Daten direkt über das Internet auf den Server des Anbieters.[16] Bisher ist die Verbreitung von Wearables

[10] PWC Strategy& (2016, S. 25 und 33).

[11] Vgl. Bittner (2016).

[12] Vgl. CHARISMHA, 51. siehe DIVSI (2016, S. 82).

[13] BMG (2015). Ähnlich WHO (2016).

[14] CHARISMHA (2016, S. 14). Vergleiche auch ENISA (2015, S. 8).

[15] IWGDPT (2015, S. 1).

[16] DIVSI (2016, S. 94).

in Deutschland noch ziemlich gering. Sie könnten aber in den kommenden Jahren zum Durchbruch des Internet of Things führen.[17]

Das **Internet of Things** (Englisch für „Internet der Dinge", kurz IoT) bezeichnet „die Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgaben für den Besitzer erledigen können"[18]. Dazu zählen im Gesundheitsbereich Wearables oder die elektronische Krankenversicherungskarte.

Die Software für mHealth-Produkte sind die sogenannten **Medizin-Apps**[19] **oder Medical Apps.** Darunter verstehen wir Anwendungen (engl. „Application", kurz „App"), die Heilberufsgruppen im Berufsalltag assistieren sollen oder die den Patienten bei der Bewältigung einer Krankheit unterstützen. Das kann beispielsweise durch die Speicherung oder Auswertung von Patientendaten, Erinnerungen an die Einnahme von Medikamenten oder Behandlungshinweise geschehen. Im engeren Sinne sind Medizin-Apps nur solche Apps, die unter die strengen Regularien für Medizinprodukte hinsichtlich Sicherheit, Verkehrsfähigkeit und Überwachung (z. B. Medizinproduktegesetz) fallen. Im weiteren Sinne des Gesundheitsbegriffs zählen hierzu auch Fitness- und Wellness-Apps. Für die Zuordnung eines mHealth-Produktes zu den Lifestyle-Produkten oder den echten Medizinprodukten ist der Hersteller selbst verantwortlich.[20] Für den Blick auf Datenschutz und Datensicherheit ist diese Zuordnung nicht so bedeutend, da es hier darum geht, welche (sensiblen) personenbezogenen Daten verwendet und wie sie gesichert werden.

Ein weiterer Anwendungsbereich von E-Health ist die **Telemedizin.** Darunter verstehen wir „den Einsatz von Telekommunikations- und Informationstechnologien im Gesundheitswesen zur Überwindung einer räumlichen Trennung zwischen Patient und behandelndem (Zahn-)Arzt sowie zwischen mehreren Ärzten […]"[21].

Mithilfe von Smartphones und Wearables kann der Nutzer seine Gesundheitswerte selbst erfassen, beim sogenannten **Self-Tracking**[22]. Der Nutzer schafft sich so ein **Quantified Self,** indem er den eigenen Körper komplett vermisst und erfasst. Werden (Gesundheits-)Daten in großer Menge zusammengeführt, kann man von **Big Data** sprechen als der „Verarbeitung von großen, komplexen und sich schnell ändernden Datenmengen […,] um bisher verborgene Zusammenhänge sichtbar und nutzbar zu machen"[23]. In der **Gesundheitswirtschaft** wird Big Data z. B. zu Forschungszwecken, zur Verbesserung der Versorgung oder zur effizienteren Planung von Ressourcen in

[17]PWC (2015, S. 4 ff.).

[18]Springer Gabler Verlag (2016).

[19]Vgl. BfArM (2015).

[20]Vgl. BfArM (2015).

[21]BZÄK und KZBV (2015, S. 16).

[22]Andelfinger und Hänisch (2016, S. 54).

[23]DIVSI (2016, S. 6).

einem Krankenhaus verwendet. Beim Gesundheitsmarkt ist zu guter Letzt zwischen dem **ersten (staatlich finanzierten) und zweiten (privat finanzierten) Gesundheitsmarkt** zu unterscheiden.[24]

1.2 Sammlung und Nutzung von Daten

Um Gesundheits- oder Fitness-Anwendungen zu nutzen, muss der Nutzer gezwungenermaßen Daten über seine Person eingeben oder der Datenerhebung zustimmen. Ob die Verarbeitung der Daten dem Datenschutz unterliegt, hängt von der Qualität der Daten ab. Für den Bereich Datenschutz relevant sind grundsätzlich alle **personenbezogenen Daten.** Diese umfassen Informationen über den Nutzer wie Name, Adresse, Kontaktinformationen, aber auch Gerätekennungen, Standortdaten, Login-Daten und alle anderen Informationen über eine identifizierte oder identifizierbare natürliche Person. Auch Filmaufnahmen und Fotos vom Nutzer oder von Dritten stellen schützenswerte Daten dar.

Als **Gesundheitsdaten** werden alle personenbezogenen Daten betrachtet, die Aufschluss über die physische oder psychische Gesundheit einer Person geben. Dazu gehören auch Daten über ärztliche Behandlungen oder Vorsorgemaßnahmen sowie Einzeldaten, die in Kombination mit anderen personenbezogenen Daten Rückschlüsse über den Gesundheitszustand oder gesundheitliche Risiken des Nutzers zulassen. Auch reine **Lifestyledaten,** die den Lebensstil oder Verhaltensmuster einer Person beschreiben, können als Gesundheitsdaten betrachtet werden, wenn sie Rückschlüsse auf den Gesundheitszustand des Nutzers zulassen. Innerhalb der Gesundheitsdaten lassen sich des Weiteren besonders sensitive Datengruppen unterscheiden, etwa biometrische Daten und genetische Daten, die explizit als besondere personenbezogene Daten in Datenschutzgesetzen genannt sind und damit unter erhöhtem Schutz stehen. Allerdings stehen Gesundheitsdaten generell unter erhöhtem Schutz durch die entsprechende Erwähnung in den Datenschutzgesetzen.[25]

Mögliche Instanzen, die Gesundheitsdaten erheben und verarbeiten, sind private und öffentliche Gesundheitsdienstleister, Beteiligte der Abrechnungsverfahren, unterschiedliche Kontroll- und Qualitätssicherungsinstitutionen (z. B. Krebsregister), IT-Dienstleister, Forschungseinrichtungen, Geräte und Anwendungen der Wellness- und Lifestylewirtschaft wie Fitnesstracker, Plattformen, soziale Netzwerke und Selbsthilfeforen im Internet sowie Statistiken und soziodemografische Datenerhebungen.[26]

[24] BMG (2016a).

[25] Vgl. DSGVO. Art. 9.

[26] Weichert (2014, S. 833 f.).

1.2.1 Anwendungsbeispiele für Tracking-Methoden bei E-Health

Die Hauptquelle für die Sammlung von personenbezogenen Daten in großen Mengen (Big Data) ist das **Tracking,** bei dem durchgehend von Geräten wie Smartphones oder Wearables bestimmte Daten erfasst und teilweise in Echtzeit an Server oder Anbieter übertragen werden.[27] Tracking kann man definieren als „die kontinuierliche Aufzeichnung bestimmter Einzelinformationen in ihrem zeitlichen Verlauf […], die sich in der Gesamtbetrachtung zu einem Erkenntnis erweiternden Datensatz zusammensetzen"[28].

Die personenbezogenen Daten können über verschiedene Tracking-Methoden gesammelt werden, die sich stetig weiterentwickeln und sich auch je nach Desktop- oder mobiler Nutzung unterscheiden. Das bekannteste Hilfsmittel bei Besuch von Webseiten sind die **Browser-Cookies,** „einfache Textdateien […], die auf dem Endgerät eines Nutzers (z.B. Computer, Tablet, Smartphone) abgelegt werden und die Wiedererkennung des Nutzers ermöglichen"[29]. Neben Cookies gibt es Web-Browser-basierte Alternativen, beispielsweise das Fingerprinting, Common IDs, eTag, Local Storage, Flash-Cookies und Authentification Cache, sowie Alternativen für mobile App-Browser, etwa die Advertiser IDs von iOS und Android.[30] So muss sich beispielsweise der Nutzer eines Gesundheitsforums im Internet nicht jedes mal erneut identifizieren, wenn er zwischen den Unterseiten des Forums wechselt.

Die **Tracking-Methoden bei IoT, Wearables und Apps** sind sehr zahlreich, daher sollen hier nur zwei Beispiele genannt werden: **Beacons** verwenden eine auf einer energiesparenden Bluetooth-Technologie basierende Funktechnologie, die mit einer Reichweite von bis zu 50 m Signale von kleinen Sendern an Smartphones in der Umgebung sendet. Sender und Empfänger werden Beacons genannt.[31] Beacons machen die genaue Ortung von Nutzern und Gegenständen auch innerhalb geschlossener Räume möglich.[32] Im Gesundheitsbereich können sie die häusliche Nachsorge nach Krankenhausaufenthalten oder Kuren oder die häusliche Pflege erleichtern, indem sie Nachrichten beispielsweise dann auf die Smartwatch des Patienten senden, wenn der Patient in die Nähe eines Gegenstandes kommt, den er benutzen soll, beispielsweise in der Küche an Flüssigkeits- oder Nahrungsaufnahme erinnert oder in der Nähe der Waage an die Gewichtskontrolle. Health-Beacons können auch einen Alarm auslösen, wenn der Patient das Haus verlässt, ohne seinen Gehstock, Schlüssel oder sein Handy mitzunehmen.[33] Sie verfolgen also jede Bewegung des Nutzers und zeichnen somit ein detailliertes Bewegungsprofil.

---

[27] DIVSI (2016, S. 10 und 24 f.).

[28] DIVSI (2016, S. 25).

[29] BVDW (2015, S. 5).

[30] BVDW (2015, S. 1).

[31] Onlinemarketing.de (2016).

[32] Sperling (2014).

[33] De Lio (2016).

Die Tracking-Technologie der **Near Field Communication** (NFC) ermöglicht über einen Chip die Verifizierung von Personen. Im Gesundheitsbereich ist ihr Einsatz beispielsweise zum Öffnen einer Tür im Krankenhaus oder beim Kauf von verschreibungspflichtigen Medikamenten denkbar. Des Weiteren können **GPS-Sender** den Aufenthaltsort und Bewegungsprofile von Nutzern eines Smartphones oder eines smarten Armbands erfassen. Diverse **medizinspezifische Sensoren** messen Gesundheitswerte wie den Puls, die Zusammensetzung des Schweißes oder ähnliches.[34]

1.2.2 Nutzerprofilerstellung

Auf diese Weise erhobene, scheinbar unzusammenhängende und im Einzelnen nicht sensitive Daten können, wenn sie zusammengeführt werden, genaue Rückschlüsse auf die betroffene Person, ihr Verhalten, ihre Gewohnheiten sowie ihren Gesundheitszustand zulassen. Sie machen somit die Bildung detaillierter Profile realer Personen möglich.[35] Man spricht bei der Zusammenführung und Auswertung von Daten zu Big Data von **Aggregierung.** Oft sammeln Dritte Daten aus verschiedenen Quellen und werten sie mithilfe von **Algorithmen** aus. „Die ordnenden und verknüpfenden Algorithmen, die hier zum Einsatz kommen, erreichen schon heute eine ungeahnte Tiefe und Komplexität."[36]

Zum Erkenntnisgewinn und wissenschaftlichen Fortschritt tritt hierbei ein Datenschutzproblem: Der Nutzer bekommt die Profilerstellung aufgrund fehlender, intransparenter oder schlicht nicht gelesener Datenschutzerklärungen oft gar nicht mit. Experten sprechen daher von „einer neuen Generation von Herausforderungen für den Datenschutz"[37] durch die Aggregierung von Daten. Gesteigert wird das Datenschutzproblem durch die zunehmende Ortsbezogenheit und die Permanenz der Datenverarbeitung bei mobiler Internetnutzung: Wearables, Smartphones etc. „generieren komplette Datenspuren, die über bisherige Grenzen der verschiedenen Lebensbereiche hinweg verknüpft werden können"[38].

[34] Siehe zu weiteren Anwendungsbeispielen Kap. 2.

[35] IWGDPT (2015, S. 5–6).

[36] Seemann (2012, S. 246).

[37] IWGDPT (2015, S. 5–6).

[38] Lewinski (2012, S. 31 f.). Siehe auch Lüke (2012, S. 161).