Big Data und Gesundheit

Dr. Thilo Weichert
Netzwerk Datenschutzexpertise

Künstliche Intelligenz, Big Data und digitale Gesellschaft –
Herausforderungen für die politische Bildung

Samstag 03.03.2018

Gustav-Stresemann-Institut, Europäische Tagungs- und Bildungsstätte Bonn

Inhalt

- Medizindaten und Grundrechtsschutz
- Rechtsgrundlagen
- Digitale Medizin
- Datenherkunft und Zwecke
- Schutzziele
- Schutzmechanismen
- Europäische Datenschutz-Grundverordnung (DSGVO)
- Schlussfolgerungen

Medizindaten und Grundrechtsschutz

- Grundrecht auf Datenschutz (Art. 2 I, 1 I GG, Art. 8 GRCh)
- Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 2 I, 1 I GG)
- Schutz von Leben und Gesundheit (Art. 2 II GG, Art. 2, 3 GRCh)

> Medizinische und informationelle Selbstbestimmung (Information und Wahlfreiheit)

- Sozialstaatsprinzip (staatliche Fürsorge) (Art. 20 I GG, Art. 27 ff. GRCh)
- Schutz von Berufsfreiheit, Eigentum, Forschung …

Vertraulichkeit und Recht

- Eid des Hippokrates (ärztliche Schweigepflicht, Patientengeheimnis): Anvertrauen von Informationen über (körperliche, seelische, familiäre, soziale, ökonomische) Not ist Grundlage für wirksame Hilfe > § 203 StGB, ärztliche Berufsordnungen
- Schutz der Gesundheitsdaten wegen besonderer Sensibilität > Datenschutzrecht, Sozialgesetzbücher
- Schutz in Spezialgesetzen: ASiG, KrankenhausGe, KrebsregisterGe, GendiagnostikG, InfektionsschutzG, TransplantationsG …

> Informationelle und medizinische Selbstbestimmung

Neuer Rechtsrahmen: Datenschutz-Grundverordnung (DSGVO)

Gültig ab 25.05.2018 – Umsetzung durch BDSG-neu (BGBl. I 2017 S. 2097)

- Art. 4 Nr. 13-15: Definition von genetische, biometrischen und Gesundheits-Daten
- Art. 9 Abs. 1: Verbot Verarbeitung besonderer Kategorien pers.bez. Daten

Schutz lebenswichtiger Interessen

Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, … med. Diagnostik, Versorgung und Behandlung im Gesundheits- und Sozialbereich

Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit

- Art. 9 Abs. 2: Ausnahmen: Einwilligung
- Art. 22: Big Data, autom. Entscheidung, Profiling, Art. 28 Auftragsverarbeitung (Cloud Computing)
- Art. 89: Archiv, wissenschaftliche Forschung, Statistik

Digitale Medizin

- Mobile Computing
- Social Communities
- Cloud Computing – Outsourcing
- Analytics – **Big Data** > virtuelles „Wissen“ und „Entscheiden“
- Sensorik (Wirksysteme), Cyborgs, Robotik
- Genetik (Genanalyse, Genome Editing)

> Volume, Variety, Velocity > Value

> Personalisierte Medizin > automatisierte „Heil(ung)sversprechungen“

Verantwortliche Medizindatenverarbeiter

- Ärzte, Apotheken, Krankenhäuser, Heil- und Pflegedienste (medizinische Leistungserbringer)
- Informationstechnische Dienstleister (AIS, KIS , ApothekenrechenRZ)
- Netzwerke (Ärztenetzwerke, Telematik-Infrastruktur, KV-Safenet, Internet)
- Abrechnungsstellen (Kassen, priv. Versicherung, PVS, Hausarztverbände, Dienstleister)
- Kontrollstellen (KVen, MDK, Aufsicht, Kammern)
- Forschung (Netzwerke, Register)
- Wellness- und Lifestyle-Bereich (Social Media, Quantified Self)

u. Statistik, Pharmaindustrie, Werbung, Versicherungen, Arbeitgeber…

Zwecke

- Behandlung und Betreuung
- Pflege und Nothilfe (z. B. Ambient Assisted Living)
- Gesundheitsmanagement
- Wirtschaftlichkeitskontrolle, Qualitätssicherung
- Genetische und medizinische Forschung
- „Selbstoptimierung“ des Betroffenen
- „Zweit-Zwecke“ für Versicherungen, Arbeitgeber, Werbung, Pharmaindustrie, Polizei, Behörden

Risiken

Für Betroffene

- Beeinträchtigung der Vertraulichkeit
- Beeinträchtigung der Wahlfreiheit
- Medizinische Diskriminierung
- Gesundheitsmanipulation
- Körperliche und seelische Schäden
- Kommerzielle Ausbeutung

Für (Gesundheits-) Einrichtung

- Ansehensverlust, Akzeptanzverlust
- Finanzieller Schaden, Schadenersatz

Materieller Schutzziele

- Privatsphäre
- Vertraulichkeit und Integrität informationstechnischer Systeme, Telekommunikationsgeheimnis
- Allgemeines Persönlichkeitsrecht (freie individuelle Entfaltung)
- Hilfeschutz (besondere Vertraulichkeit)

> Keine Offenbarung möglicherweise beschämender oder schadender (sozialer, körperlicher, seelischer, familiärer, ökonomischer) Notlagen

Technisch-organisatorische Schutzziele

- Vertraulichkeit (z. B. Verschlüsselung)
- Integrität, Authentizität (z. B. digitale Signatur)
- Verfügbarkeit (z. B. Backup, Stromversorgung)
- Intervenierbarkeit (Löschen, Sperren, Berichtigen)
- Transparenz, Revisionsfähigkeit (Protokolle, Dokumentation)
- Nichtverkettbarkeit (z. B. Mandantentrennung, Rollenkonzept)

Rechtliche Schutzmechanismen

Einwilligung (informed consent): explizit, freiwillig, bestimmt und rückholbar

Gesetzliche Regelungen

- Materiell: Zweckfestlegungen, Daten- und Prozesstransparenz, Verfahrenssicherungen
- Technisch-organisatorisch: Verschlüsselung, Pseudonymisierung, Mandantentrennung
- Anonymisierung/Aggregierung

Einwilligung bei medizinischem Big Data

Rechtlich wirksam nur wenn Erklärung

Bewusst
Informiert
Freiwillig (ohne Abhängigkeit)
Widerrufbar

Realität:

Zu komplex für bewusste Entscheidung
Keine Information, keine Wahlmöglichkeit
Abhängigkeit von den Behandelnden
Vollendete Tatsachen, langfristige Speicherung

Transparenz

Adressaten: Betroffene (auch Recht auf Nichtwissen), Heilberufsausübende (Arzt, Krankenhaus …), (staatliche) Aufsicht, Hierarchie, demokratisch legitimierte und rechtliche Genehmigungs- und Kontrollinstanzen (z. B. DS-Aufsicht, Ethik-Kommissionen), (wissenschaftliche) Fachöffentlichkeit, Öffentlichkeit

Realität: Geheimhaltung bei Gesundheitseinrichtungen, Forschungsstellen, Pharmaunternehmen …

Bspl.: pseudonymisierte Rezeptdaten von Apothekenrechenzentren für Medizindatenvermarkter (z. B. IMS Health/IQVIA), „Betriebs- und Geschäftsgeheimnis“

Anonymisierung/Pseudonymisierung

- Löschen od. Ersetzen der Identifikatoren durch Pseudonyme (bzgl. Patient, Arzt, Abrechner, Dienstleister)
- Aggregierung von Datensätzen u./o. von Merkmalsdaten

Instrumente

- Krankheitsregister (z. B. Krebs) mit Treuhänder
- Datentransparenz unter staatlicher Aufsicht und Kontrolle (z. B. §§ 303a ff. SGB V)
- Mehrschichtige Pseudonymisierungsverfahren (z. B. Biobanken, Problem: potenziell unbeschränktes Zusatzwissen, z. B. aus dem Internet)

Neue DSGVO-Instrumente

Verhaltensregeln > Art. 40, 41

- EU oder national
- Genehmigung und Registrierung
- Überwachung durch akkreditierte Experten

Zertifizierung > Art. 42, 43

- Förderung durch EU
- Freiwillig und transparent (Kriterien, Notifikation, Registrierung)
- Dauer max. 3 Jahre, Entzug durch Aufsicht od. Zertifizierungsstelle
- Akkreditierung der Zertifizierungsstelle
- EU-Kommission legt Standards fest

DSGVO: Autom. Entscheidung/Profiling

(1) Betroffenenrecht, „nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“

(2) Ausnahmen: Abschluss u. Erfüllung v. Vertrag, Rechtsvorschrift, explizite Einwilligung

(3) Angemessene Schutzmaßnahmen sind nötig (incl. Eingreifen einer Person u. Darlegung d. eigenen Standpunkts, Entscheidungsanfechtg.)

(4) Verbot bzgl. sensitiver Daten, wenn keine angemessenen Maßnahmen gemäß Art. 9 Abs. 2

Exemplarisch: Regelungsvorschlag Forschung

Probleme:

- Föderaler und regelungsspezifischer Flickenteppich
- Ungenügende Schutzvorkehrungen: Pseudonymisierung, Filetrennung, Zweckbindung
- Ungeeignete Schutzvorkehrungen: Meldung bei DS-Aufsicht, Genehmigung durch Ressort

Lösung:

- Forschungsgeheimnis (mit Zeugnisverweigerung u. Beschlagnahmeschutz)
- Zentrales unabhängiges Bund-Länder-Forschungsgremium auf Staatsvertragsbasis mit gestufter Pflicht und Befugnis zu Überwachung, Genehmigung, Standardisierung
- Aufbau einer informationellen Forschungs-Infrastruktur (Pseudonymisierungsgremien, Transparenzregister)

Schlussfolgerungen

Für die Betroffenen

- (Medizinische) Daten sind nicht immer (heilsame) Informationen
- Computer können nicht behandeln, sondern nur unterstützen
- Vertraulichkeit ist nicht obsolet

Gesamtgesellschaftlich

- Stärkung des IT- und Gesundheitsstandorts
- Verbesserung der Gesundheit
- Stärkung der individuellen Selbstbestimmung
- Gesundheitsservice als staatliches Angebot (Private-Public-Partnership)

> Big Data im Gesundheitsbereich? Ja, aber bitte unter strenger Kontrolle!

Big Data und Gesundheit

Thilo Weichert
Waisenhofstr. 41, 24103 Kiel
0431 9719742
weichert@netzwerk-datenschutzexpertise.de
www.netzwerk-datenschutzexpertise.de