Big Data und KI im Gesundheitssystem: Warum wir einen kollektiven Datenschutz brauchen

Rainer Mühlhoff, muehlhoff@tu-berlin.de, http://RainerMuehlhoff.de, @RainerMuehlhoff

Ursprüngliches Autorenmanuskript, März 2020.

Erschienen in veränderter Fassung als „Die Illusion der Anonymität: Big Data im Gesundheitssystem“, Blätter für deutsche und internationale Politik, 08/2020.

Die Medizin verspricht sich besonders viel von der Digitalisierung. Durch die umfassende elektronische Verarbeitung von Fall- und Patientendaten soll das Gesundheitssystem effizienter und die Versorgung verbessert werden. Die medizinische Forschung wertet große Datensätze (Big Data) mittels „Data Mining“ und künstlicher Intelligenz aus, um seltene Krankheiten zu erkennen und neue Diagnose- und Therapiemöglichkeiten zu erschließen. Großen Datenunternehmen der Google-Holding Alphabet wird schon seit Jahren nachgesagt, die westliche Schulmedizin in der Zukunft grundlegend zu revolutionieren.

Während in diesen Debatten oft das Innovationspotenzial im Vordergrund steht, werden Datenschutzbedenken relativiert oder – im internationalen Kontext – als spezifische Befindlichkeit „der deutschen Bevölkerung“ abgetan.[1] Dabei ist Datenschutz in der Gesundheitsversorgung besonders wichtig, wie ich im folgenden argumentieren werde. Mehr noch: Wir brauchen sogar ein neues, erweitertes Verständnis von Privatsphäre, welches auch die Verwendung anonymisierter und pseudonymisierter Daten streng reguliert, die als „Big Data“ an zahlreichen Stellen im Gesundheitssystem aggregiert und ausgewertet werden. Denn auch anonymisierte Daten können dazu verwendet werden, sensible Informationen über unsere Gesundheit – z.B. ob wir Alkoholabhängig sind, zu Depressionen neigen oder Diabetes haben – *abzuschätzen*, auch solche, die wir selbst nicht preisgeben möchten.

Datenlecks und klassischer Datenschutz

Gesundheitsdaten sind besonders schützenswürdig: Viele Befunde und Diagnosen, etwa über Erbkrankheiten, Diabetes oder eine HIV-Infektion, ändern sich ein Leben lang nicht mehr. Gelangen solche Informationen in die falschen Hände, können sie über Jahrzehnte zum Nachteil der Betroffenen verwendet werden. Entsprechend wertvoll sind Patientendaten auf dem (Schwarz-)Markt der Datenbroker und Analytics-Services. Allein in den letzten Wochen sind über die Tagespresse mehrere Datenlecks im Gesundheitssystem bekannt geworden, die potenziell von solchen Akteuren ausgenutzt worden sein könnten: Millionen Krankenakten und Befunddaten deutscher Arztpraxen waren aufgrund schlecht

1 PriceWaterhouseCoopers GmbH. 2018. „Das deutsche Gesundheitswesen auf dem Prüfstand“.

geschützter Server im Internet zugänglich.[2] Einsatzdaten des Deutsche Rote Kreuzes in Brandenburg lagen gänzlich ungesichert auf einem Internetserver und konnten dort sogar manipuliert werden.[3] 2018 wurde bekannt, dass durch einen Hackerangriff auf eine norwegische Gesundheitsbehörde Patientendaten von mehr als der Hälfte der norwegischen Bevölkerung entwendet wurden.[4]

Diese – lediglich exemplarische – Auswahl von Fällen zeigt, was jede Informatiker_in gut kennt. Elektronische Datenspeicherung ist stets mit inhärenten Risiken verbunden, die eine ständige und kostspielige Wartung der Systeme erfordern. Technologien (z.B. Verschlüsselungsverfahren) sind irgendwann veraltet und müssen durch neue, sicherere ersetzt werden; Programmierfehler (Bugs) werden oft zufällig entdeckt und dann öffentlich gemacht, sie müssen dann schnell und flächendeckend behoben werden; und schließlich führt Fehlkonfiguration von sicherheitsrelevanten Softwarekomponenten nicht selten dazu, dass Daten gänzlich schutzlos zugänglich sind. Werden solche Schwachstellen ausgenutzt und Daten entwendet, geben Betreiber_innen meist bekannt, dass sie die Lücken umgehend schließen. Für die Betroffenen ist dann jedoch meist schon ein irreversibler Schaden entstanden, der bei Gesundheitsdaten, die lange „aktuell“ bleiben, umso größer ausfällt.

Die Entwendung sensibler Daten durch Sicherheitslücken ist ein systematisches Risiko der digitalen Datenaufbewahrung. Grundsätzlich ist der mögliche Schaden umso größer, je mehr Datensätze an ein und demselben Ort gespeichert werden. Bei starker Datenaggregation können auf einen Schlag die Daten vieler Tausend oder Millionen Patient_innen entwendet werden. Dieser Punkt betrifft auch die „elektronische Patientenakte“ (ePA), die als Erweiterung der „elektronischen Gesundheitskarte“ (eGK) bis 2021 in Deutschland eingeführt werden soll. Während die eGK nur die Stammdaten, ggfs. Notfalldaten und einen Medikationsplan der Patient_in auf der Karte selbst – also dezentral – speichert, werden die Daten der ePA auf einem zentralen Server abgelegt.[5] Die ePA bricht also mit dem Prinzip der dezentralen Speicherung und physischen Überlassung des Speichermediums an die Dateneigentümer_innen und ermöglicht potenziell die gesammelte Entwendung vieler Datensätze durch einen einzigen Einbruch auf dem Server.

Big Data: Warum Anonymisierung oft nicht hilft

Während die Einführung der elektronischen Gesundheitskarte auf ärztlichen und öffentlichen Widerstand stieß, konnte im Dezember 2019 eine andere gravierende Maßnahme relativ sang- und klanglos vom Deutschen Bundestag beschlossen werden: Bundesgesundheitsminister Jens Spahn hat mit dem „Digitale-Versorgung-Gesetz“ einen Rahmen für die

2 https://www.tagesschau.de/investigativ/ndr/hannover-patientendaten-101.html ; https://www.tagesschau.de/investigativ/br-recherche/patientendaten-101.html

3 https://www.tagesschau.de/investigativ/br-recherche/datenleck-drk-101.html

4 https://www.br.de/nachrichten/netzwelt/norwegen-hacker-stehlen-daten-von-3-millionen-patienten

5 Gematik: „Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur“, 18.11.2019, S. 28. https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gematik_Whitepaper_Datenschutz_und_Informationssicherheit.pdf

Zusammenführung und zentrale Speicherung der Behandlungsdaten aller gesetzlich Versicherten in Deutschland geschaffen, um diese Daten der Forschung zugänglich zu machen.[6] Datenschutzbedenken wurde mit dem Hinweis begegnet, dass die Daten pseudonymisiert an die Sammelstelle – den Spitzenverband Bund der Krankenkassen – weitergeleitet werden. Das heißt, Name, Geburtsdatum, Versichertennummer etc. werden durch eine Chiffre ersetzt, die es erlaubt, Datenpunkte, die zur selben Person gehören, einander zuzuordnen, jedoch ohne die Identität der Betroffenen offenzulegen.

Pseudonymisierung ist ein verbreitetes Verfahren zur Aufbereitung aggregierter Datensätze, die etwa statistisch ausgewertet oder zum Training einer künstlichen Intelligenz (maschinelles Lernen) verwendet werden sollen. Um in den Daten von Millionen Patient_innen neue Krankheitszusammenhänge zu entdecken, ist es schlechterdings egal, wie die Patient_innen heißen. Zugleich ist der Hinweis, dass die sensiblen Behandlungsdaten nur pseudonymisiert erfasst werden, eine geläufige Strategie, um Datenschutzeinwände auszuhebeln – sie trifft unser *individualistisches* Denken über Datenschutz nämlich in seinem blinden Fleck: Datenschutz wird im westlichen Diskurs mit dem Recht jedes Einzelnen verbunden, die Speicherung und Verwendung seiner personenbezogenen Daten zu kontrollieren (informationelle Selbstbestimmung). Sobald ein Datensatz keine identifizierenden Informationen mehr enthält, weil er z.B. anonymisiert wurde, sehen die meisten Menschen in seiner Verwendung keine Gefahr mehr für sich selbst und das Recht auf informationelle Selbstbestimmung gilt als gewahrt.

Es ist wohl die entscheidende Herausforderung des Datenschutzes im Zeitalter von Big Data, künstlicher Intelligenz und prädiktiver Analytik, sich von der liberalistischen Konzeption eines Rechts auf informationelle Selbstbestimmung zu lösen – und zwar indem dieses Schutzrecht noch verschärft, nicht etwa gelockert wird. Denn pseudonymisierte Datensätze erlauben in vielen Fällen Rückschlüsse auf Einzelpersonen, und zwar nicht nur auf die in dem Datensatz enthaltenen Personen selbst, sondern auch auf Unbeteiligte. Man kann zwei Verfahrensweisen unterscheiden, die das ermöglichen: Die erste funktioniert über „Re-Identifikation“ von Einzelpersonen in anonymen Datensätzen; die zweite betrifft die statistische Abschätzung sensibler Informationen anhand von prädiktiven Analysen.

Re-Identifizierung: Anonymität ist relativ

Das Risiko, in einem anonymisierten Datensatz vieler Patientendaten re-identifiziert zu werden, ist eigentlich ein alter Schuh. In der Informatik wird das unter dem Stichwort „Datenbanksicherheit“ thematisiert. Den Anstoß hierfür hat ein Fall aus den USA der 1990er Jahre gegeben, der auch als Warnung in Bezug auf das „Digitale-Versorgung-Gesetz“ in Erinnerung gerufen werden sollte: Der US-Bundesstaat Massachusetts hat in den 1990er Jahren die medizinischen Behandlungsdaten von ca. 135.000 staatlichen Bediensteten und ihren Familienmitgliedern pseudonymisiert zu einer Datenbank zusammen-

6 *Bundesgesetzblatt Teil I*, Nr. 49 vom 18.12.2019: S. 2562.

gestellt und für Forschungszwecke zugänglich gemacht. Latanya Sweeney, damals Informatikstudentin am MIT, hat in diesem Datensatz durch geschickte Kombination mit öffentlich zugänglichen Daten aus dem Wähler_innen-Register von Massachusetts exemplarisch die Krankenakte des damaligen Gouverneurs von Massachusetts, William Weld, rekonstruiert.[7]

Diese spektakuläre Aktion hat die wissenschaftliche und regulatorische Debatte des Datenschutzes in den USA stark beeinflusst. Sweeneys Re-Identifizierungsattacke gilt heute als Elementarbeispiel für einen Angriffstyp, der mittels Ausnutzung von Hilfsinformationen aus anderen zugänglichen Quellen verfährt. Seit ihrer Veröffentlichung werden in Fachkreisen jedes Jahr neue, und immer kompliziertere Re-Identifizierungsangriffe auf Datensätze aller Art veröffentlicht.[8] In der mathematischen Theorie der Datenbanksicherheit ist überdies formalisiert worden, dass „Anonymität" kein eindeutig bestimmtes, sondern ein stark vom Kontext abhängiges Kriterium ist und in einer umgekehrten Relation zur sogenannten „utility" – dem statistischen Nutzwert – eines Datensatzes steht. Nur ein Datensatz, in dem alle Einträge gleich aussehen, gewährleistet volle Anonymität, ist aber für statistische Auswertungen kaum nützlich; sobald sich einzelne Datenpunkte von anderen abheben, steigt das prinzipiell untilgbare Risiko der Re-Identifizierbarkeit.[9]

Prädiktive Analysen: Auch erratene Informationen verletzen die Privatsphäre

Re-Identifikation Einzelner in anonymen Daten ist heute allerdings gar nicht mehr das größte Risiko im Zusammenhang mit anonymisierten Daten. Eine zweite Form des Missbrauchs solcher Daten ist aktuell viel virulenter, obschon sie in Politik und Öffentlichkeit noch kaum beachtet wird. Anhand großer (potenziell anonymisierter) Datensätze kann man sogenannte prädiktive Analysen (*predictive analyses*) erstellen, die sensible Daten über Menschen anhand verfügbarer Daten aus anderen Quellen *abschätzen*. Es handelt sich dabei um Korrelationsanalysen, die mittels maschineller Lernverfahren die statistischen Zusammenhängen zwischen sensiblen Informationen (z.B. Krankheiten, psychologischen Behandlungen oder erblichen Vorbelastungen) und behaviorellen Daten analysieren. Behaviorelle Daten fallen in der Praxis meist bei der Nutzung digitaler Dienste an, wie z.B. über Fitness-Tracker oder Wearables, oder bei der Nutzung von Social Media Diensten.

So haben Mediziner_innen von der University of Pennsylvania gezeigt, dass anhand der automatischen Auswertung von Postings auf Facebook vorhersagbar ist, ob ein User an

7 Ohm, Paul. 2010. „Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization". *UCLA Law Review* 77; Sweeney, Latanya. 1997. „Weaving Technology and Policy Together to Maintain Confidentiality". *The Journal of Law, Medicine & Ethics* 25 (2–3): 98–110.

8 Vgl. Ohm 2010. a.a.O. und besonders spektakulär: Die Re-Identifikation von Netflix-Usern in einer pseudonymisiert publizierten Datenbank aus Film-Bewertungen, Narayanan, Arvind, und Vitaly Shmatikov. 2008. „Robust de-anonymization of large sparse datasets: a decade later". *Proc. of the 2008 IEEE Symp. on Security and Privacy*.

9 Dwork, Cynthia. 2011. „A Firm Foundation for Private Data Analysis". *Communications of the ACM* 54 (1): 86.

Krankheiten wie Depression, Psychosen, Diabetes oder Bluthochdruck leidet.[10] Facebook selbst hat bekannt gegeben, mittels künstlicher Intelligenz suizidale User anhand ihrer Postings zu erkennen und in akuten Fällen automatisiert die Behörden zu informieren.[11] Ein Medienbericht von 2012 hat aufgearbeitet, dass prädiktive Analysen durch Auswertung von Kreditkartentransaktionen Schwangerschaften erkennen können.[12] Das Ziel solcher prädiktiver Analysen besteht nicht darin, die *Identität* einer Person in den anonymisierten Daten aufzudecken. Sie werden vielmehr dazu verwendet, für beliebige anonyme „User", über die leicht zugängliche behaviorelle Daten (etwa durch die Verwendung eines digitalen Dienstes) bekannt sind, sensible Informationen vorherzusagen, auch wenn die Betroffenen diese Informationen selbst nicht preisgeben möchten. Es wurde vielfach thematisiert, dass diese Technologie schon heute zu Missbrauch, Diskriminierung und sozialer Ungleichheit führt, etwa wenn der Zugang zu Jobs, Krediten, KFZ-Versicherungen oder sozialstaatlichen Leistungen von automatisierten Entscheidungen auf Grundlage prädiktiver Analysen abhängig gemacht wird.[13]

Um den möglichen Missbrauch dieser Technologie, besonders im Gesundheitssektor, zu bekämpfen, benötigen wir ein erweitertes Verständnis von Privatsphäre, das sich auch auf *abgeschätzte*, nicht nur auf explizit *erhobene* Informationen erstreckt: Die *prädiktive Privatheit* einer Person ist verletzt, wenn sensible Informationen über diese Person gegen ihren Willen statistisch abgeschätzt und in Entscheidungen einbezogen werden, die wesentliche Auswirkungen auf Chancen oder Wohlergehen dieser Person haben. Zugleich benötigen wir ein breites Bewusstsein dafür, dass prädiktive Analysen nur möglich sind, wenn und weil viele Bürger_innen sowie politische Entscheidungsträger_innen keine Einwände dagegen erheben, ihre Daten (ggfs. anonymisiert) zur Verfügung zu stellen. Nur anhand der Daten vieler „normaler" Nutzer_innen, die meinen „nichts zu verbergen zu haben", lassen sich die prädiktiven Algorithmen trainieren, die *andere* Individuen als Abweichler_innen erkennen können. Im Zeitalter von Big Data und KI ist Datenschutz somit keine Privatsache mehr: Daten, die man selbst freiwillig weitergibt, können dazu verwendet werden, sensible Informationen über *andere* Menschen abzuschätzen. Auch die weltweit fortschrittliche europäische Datenschutzgrundverordnung ist gegen dieses Phänomen wirkungslos[14], denn sie bleibt weitestgehend dem liberalistischen Paradigma informationeller Selbstbestimmung verhaftet. Gegen die Risiken prädiktiver Analytik hilft dagegen nur ein kollektivistisches Verständnis von Datenschutz, nach dem wir alle ein Interesse daran haben, dass auch die anderen sorgsam mit ihren Daten umgehen.

---

10 Merchant, Raina M. et al. 2019. „Evaluating the Predictability of Medical Conditions from Social Media Posts". *PLOS ONE* 14 (6).

11 https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12

12 Duhigg, Charles. 2012. „How Companies Learn Your Secrets". *The New York Times*, 16. Februar 2012. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

13 Eubanks, Virginia. 2017. *Automating inequality: how high-tech tools profile, police, and punish the poor*. First Edition. New York: St. Martin's Press; O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

14 Wachter, Sandra. 2019. „Data Protection in the Age of Big Data". *Nature Electronics* 2 (1): 6–7.