



Der Wert unserer Daten

Wissenswertes für Kunden und Manager von Telekommunikationsunternehmen, Finanzdienstleistern, Smartphone-Herstellern, Facebook und Biobanken

Daten sind das Gold des 21. Jahrhunderts – so zumindest hört und liest man es sehr oft in ökonomischen Beiträgen zur Digitalisierung wirtschaftlicher Prozesse [1]. Je mehr Daten generiert werden und je wichtiger wir sie nehmen, erhalten auch politische Entscheidungen zum Verhältnis von Nutzung bzw. Auswertung und damit auch von Monetarisierung unserer Daten einerseits und deren Privatheit und Schutz andererseits eine immer größere Bedeutung. Um hier richtig zu entscheiden, bräuchte man eigentlich Kosten-Nutzen-Analysen, die es jedoch ganz einfach nicht gibt.

Was es auf jeden Fall gibt, ist jedoch – wahrscheinlich hierzulande weltweit am deutlichsten – ein großes Unbehagen im Hinblick auf den Zugang von Unternehmen und staatlichen Institutionen zu personenbezogenen bzw. persönlichen Daten. Weil Datenschutz und Datensicherheit weltweit immer wichtiger werden, führte die Europäische Union (EU) am 25. Mai 2018 (Beginn der EU-weiten Gültigkeit) eine umfassende Reihe von Datenschutzbestimmungen ein: die Datenschutz-Grundverordnung (DSGVO oder DS-GVO; französisch Règlement général sur la protection des données RGPD, englisch General Data Protection Regulation GDPR). Während die USA noch nicht so weit sind, gibt es in Kalifornien seit dem 1.1.2020 ein Gesetz, den California Consumer and Privacy Act (CCPA), das regelt, wie Unternehmen auf der ganzen Welt mit den personenbezogenen Daten von in Kalifornien ansässigen Personen umgehen dürfen und das der EU DSGVO sehr ähnlich ist.

In vielen Ländern der Welt ist die Situation noch nicht geklärt. Hinzu kommt, dass es erstens nur sehr wenige Daten dazu gibt, wie viel der Datenschutz den Menschen wirklich wert ist, dass diese zweitens oft nur qualitativer Natur und auf Meinungen zum Datenschutz im Allgemeinen be-

schränkt sind, und dass drittens quantitative Daten hierzu völlig fehlen. Es ist deshalb von großem Interesse, dass im Januar und März 2020 2 Studien erschienen sind, in denen jeweils gemessen wurde, wie viel verschiedene Typen von Daten den Menschen aus verschiedenen Ländern ganz konkret wert sind.

Jeffrey Prince vom Department of Business Economics and Public Policy an der Indiana University und Scott Wallsten vom Technology Policy Institute in Washington, DC, publizierten im Januar 2020 eine Studie, im Rahmen derer gemessen wurde, wie viel US\$¹ verschiedene Typen von Daten (über Finanzen, Biometrie, Standort, Netzwerke, Kommunikation und Web-Nutzung), die von verschiedenen Institutionen gesammelt werden, den Menschen aus verschiedenen Ländern (USA, Mexiko, Brasilien, Kolumbien, Argentinien und Deutschland) jeweils ganz konkret wert sind.

Man kann diese Frage auf 2 Arten stellen:

- „Wie viel würden Sie verlangen, um Ihre Daten preiszugeben?“ und
- „Wie viel würden Sie bezahlen, damit Ihre Daten nicht preisgegeben werden?“

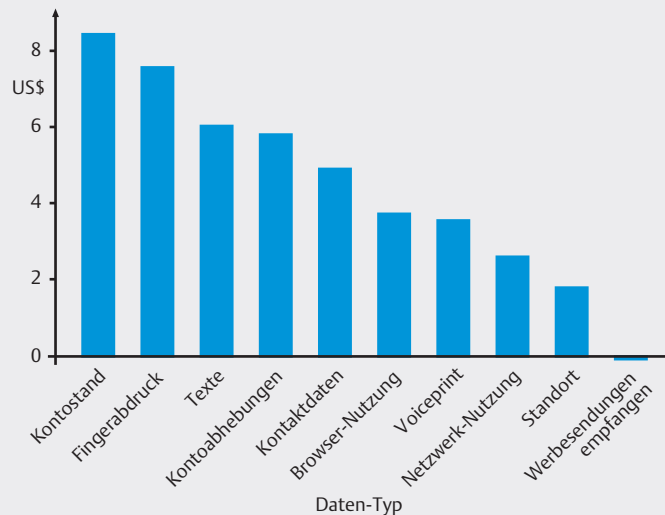
Man spricht im ersten Fall von „willingness to accept (WTA)“ und im zweiten Fall von „willingness to pay“ (WTP). Da es erstens bereits mehr Studien zum ersten Verfahren (WTA) gibt und dieses Bezahlmodell auch tatsächlich eher praktische Anwendung in

der realen Wirtschaft findet², stellte man die Fragen im WTA-Modus. Wie man weiß, sind die Bewertungen in diesem Modus eher höher als im WTP-Modus, sodass die erhobenen Werte die tatsächlichen Werte der Menschen eher über- als unterschätzten.

Die Autoren gingen auf recht komplexe Weise vor: Sie entwickelten 4 Fragebögen, die sich auf 4 Plattformen beziehen, auf denen persönliche Informationen über den jeweiligen Teilnehmer vorliegen: Den Mobilfunkanbieter, das Finanzinstitut (Bank), das Smartphone und das Facebook-Konto des Befragten. Konkret wurde gefragt, für wieviel Geld monatlich die Teilnehmer bereit wären, ihre persönlichen Daten zu Finanzen, Biometrie, Standort, Netzwerke, Kommunikation und Web-Nutzung zur Verfügung zu stellen. Die Umfrage war internetbasiert und wurde bei 15 600 Menschen durchgeführt. Die Teilnehmer konnten dabei unter verschiedenen Angeboten der Plattformen auswählen, bei denen sie für die Überlassung unterschiedlicher Typen von Daten, unterschiedlich große monatliche Zahlungen erhielten. Zudem wurde bei der Hälfte aller Befragungen (randomisierte Zuordnung) vorher auf die Vorteile der Nutzung solcher Daten durch Dritte hingewiesen, insbesondere im Hinblick auf die Möglichkeiten von zielgenauer Werbung. Die Ergebnisse waren durchaus bemerkenswert: Im Durchschnitt aller Länder und Plattformen legten die Menschen den größten Wert auf die Geheimhaltung von Finanzdaten, biometrischen (Fingerabdruck-) Informationen und von ihnen produzierten Texten (► **Abb. 1**).

1 Die Studie wurde jeweils in der Landeswährung durchgeführt. Zur Auswertung der Daten wurden die Währungen der anderen Länder in US\$ umgerechnet, dessen Wert im Hinblick auf die Kaufkraft für Oktober 2019 vom International Monetary Fund festgelegt wurde.

2 „The choice to measure WTA rather than WTP is largely driven by the fact that several proposals (and existing marketplaces, such as DataCoup) involve firms paying consumers for their data rather than consumers paying firms to keep their data private“, schreiben die Autoren hierzu [6].



► **Abb. 1** Durchschnittlicher von den Teilnehmern (aus allen Ländern, über alle 4 Plattformen hinweg und über die Bedingung „Vorherige Information zum Benefit von Data sharing – ja/nein“ gemittelter) geforderter monatlicher Betrag für die Erlaubnis, auf bestimmte Typen von Daten des Nutzers zuzugreifen und Dritten zur Verfügung zu stellen (nach Daten aus [6]).

Um einer Plattform den Austausch dieser Informationen mit Dritten zu ermöglichen, müsste die Plattform den Nutzern monatlich 8,44 US\$ für Daten zum Bankguthaben, 7,56 US\$ für den Fingerabdruck, 6,05 US\$ für das Lesen der persönlichen Texte und 5,80 US\$ für den Austausch von Informationen über Bargeldabhebungen zahlen. Nur monatlich 1,82 US\$ wollten die Nutzer dagegen für die Weitergabe ihres Standortes und im Mittel gar nichts für die Zusendung von Werbung per Kurznachrichte bezahlt haben.

Zwischen den untersuchten 6 Ländern gab es signifikante Unterschiede (► **Abb. 2**). Im Allgemeinen ließen sich die Menschen in Deutschland ihren Verzicht auf den Datenschutz teurer bezahlen als die Menschen in den USA und in Lateinamerika. Deutsche Befragte wollten für Daten zu Bankguthaben monatlich 15,43 US\$ und für Daten zu Barabhebungen monatlich 13,42 US\$.

Dieses Ergebnis ist weitgehend auf die starke Abneigung der Deutschen zurückzuführen, ihre finanziellen Daten anderen preiszugeben. Bei ihrem Fingerabdruck hingegen sind die Deutschen nicht so pingelig: Wie aus ► **Abb. 1** hervorgeht, wird der Fingerabdruck im Durchschnitt aller Länder von allen untersuchten Datentypen am zweithöchsten bewertet – nicht aber von den Deutschen. Oder nochmal anders:

Während den Deutschen Daten über ihren Fingerabdruck nur halb soviel wert sind wie Daten über ihr Bankkonto, ist es bei den Kolumbianern umgekehrt. Interessant ist zudem das Ergebnis, dass es den Menschen relativ wenig wert ist, zielgerichtete Werbung nicht zu bekommen; in Lateinamerika (Argentinien, Kolumbien und Mexiko) würden die Menschen sogar etwa 2,50 US\$ pro Monat bezahlen, um Werbung zu bekommen. Dieses Ergebnis war übrigens – wie alle anderen auch – unabhängig davon, ob Vorinformationen zu den positiven Auswirkungen von Datenüberlassung und damit von zielgerichteter Werbung gegeben worden waren oder nicht. Der Schutz von Daten zum eigenen Standort war den Menschen in jedem Land ebenfalls nur wenig wert (im Mittel weniger als 2 US\$/Monat; ► **Abb. 1**). Relativ viel wert war den Menschen überall dagegen, was sie an privaten Texten schreiben (etwa 6 US\$/Monat) und mit welchen Menschen sie Kontakte haben (etwa 5 US\$/Monat).

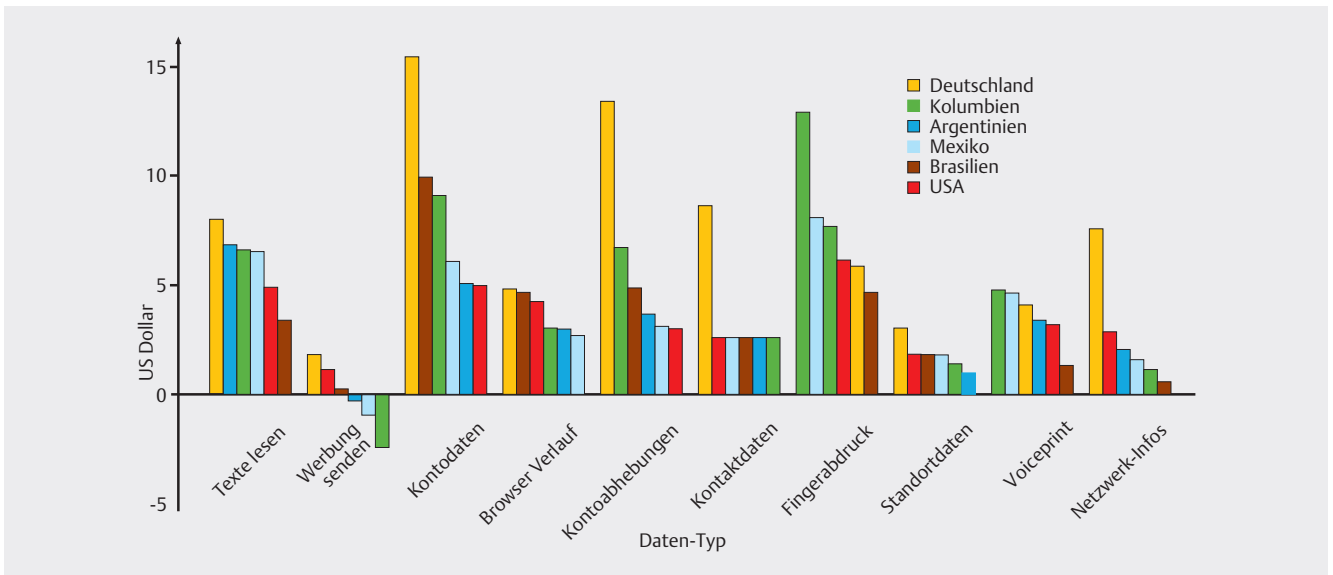
Weiter wurde untersucht, ob sich die 4 Plattformen darin unterscheiden, wieviel sie für die Nutzung der eigenen persönlichen Daten zahlen müssten. Im Prinzip sollte es hier von Plattform zu Plattform keine wesentlichen Unterschiede geben, denn es geht ja darum, dass jede Plattform für das Gleiche bezahlt, nämlich dafür, die persönlichen Daten mit Dritten zu teilen – und

das könnten jeweils genau dieselben sein. Es sei angemerkt, dass der Parameter WTA („willingness to accept“) in seiner monetären Ausprägung in diesem Zusammenhang als Index für Vertrauen operationalisiert wurde. In der Realität vertrauen die Menschen den verschiedenen Plattformen in unterschiedlichem Maße. (Vielleicht glauben die Nutzer auch, dass die Praktiken der Datenfreigabe bei den Plattformen unterschiedlich sind.) Weil in den Umfragen nicht für jede Plattform nach den gleichen Arten von Informationen gefragt wurde (das ergibt keinen Sinn), sind Vergleiche zwischen den Plattformen (im Hinblick auf die gleichen Fragen) nur begrenzt möglich (► **Abb. 3**).

Zwar sind die Menschen länderübergreifend eher bereit, Kontaktinformationen mit Facebook zu teilen als mit ihrem Mobilfunkanbieter. Der Betrag, den Facebook den Nutzern für das Recht, Kontaktdaten zu teilen, zahlen müsste, unterscheidet sich zwischen einzelnen Ländern jedoch erheblich: In Deutschland ist er mit Abstand am höchsten.³ Zudem ist interessant: Von allen 4 Plattformen wird dem Mobilfunkanbieter das wenigste Vertrauen entgegengebracht. Mit Ausnahme von Deutschland hat es Facebook aber offenbar geschafft, ein größeres Vertrauen zu erzielen, wobei möglicherweise aber auch anzunehmen ist, dass den Menschen oft gar nicht klar ist, was Facebook alles mit ihren Daten anstellen kann (und ja tatsächlich auch anstellt [9]).

Im Hinblick auf demografische Variablen gibt es aus dieser Studie wenig Neues zu berichten: Ältere vertrauen weniger (d. h.

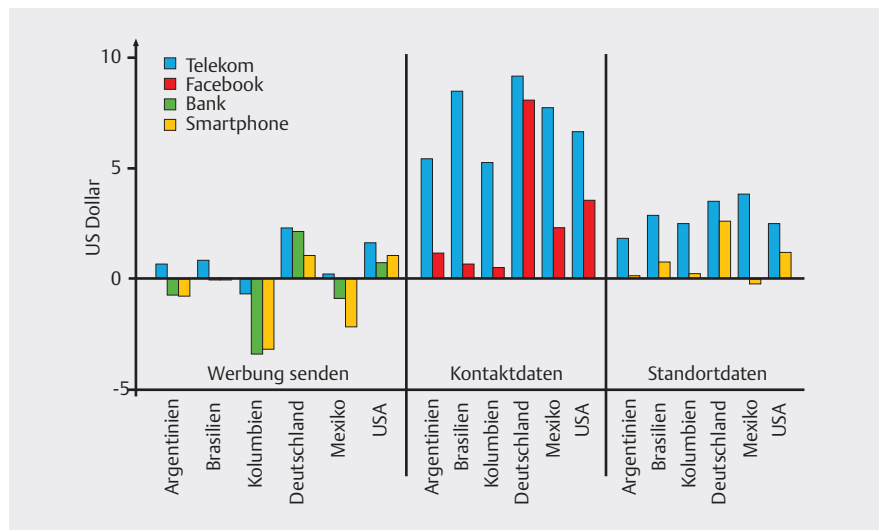
3 Hierzu die Autoren im Original: „Germans seemed particularly Facebook-averse, requiring the platform to pay them around \$8/month for the right to read their texts or share information about their contacts or network. By contrast, people in the U.S. required about \$5/month to allow access to their texts, \$3.50 to share information about their contacts, and \$3/month to share information about their networks. For Latin American countries, the numbers for texts are generally between those for the U.S. and Germany“ [6]. Die Lateinamerikaner sind also nicht in jeder Hinsicht die „besseren Amerikaner“ (d. h. noch weiter von uns entfernt als diese), beispielsweise im Hinblick darauf, was sie sich gegenseitig schreiben.



► **Abb. 2** Durchschnittswerte für das, was man in den 6 untersuchten Ländern für den Verzicht auf Datenschutz monatlich verlangt in Abhängigkeit von der Art der Daten (Daten-Typ). Die Abbildung bestätigt die Vermutung, dass die Deutschen dazu neigen, ihre Privatsphäre mehr zu schätzen als andere (nach Daten aus [6]).

fordern mehr Geld für die Weitergabe ihrer Daten) als jüngere, Frauen vertrauen weniger als Männer; das Einkommen hatte übrigens keinen Einfluss auf das Vertrauen bzw. die finanziellen Forderungen. Ob Informationen vor der Befragung zu den Vorteilen der Weitergabe von Daten gegeben wurden oder nicht, hatte interessanterweise keinen Einfluss auf die Forderungen bzw. das Vertrauen. Dies zeigt nach Meinung der Autoren an, dass die Bewertungen (bzw. Forderungen) der Menschen bezüglich ihrer Privatsphäre relativ stabil und wenig beeinflussbar seien.

Abschließend sei zu dieser Studie noch bemerkt, dass es hier nicht um eine Kosten-Nutzen-Analyse des Datenschutzes handelte, sondern nur um eine der Kosten. Nehmen wir ein Beispiel, das auch die Autoren verwenden, um dies zu illustrieren: „Nehmen wir an, dass die Geheimhaltung von Standortdaten bedeutet, dass ihr Smartphone im Straßenverkehr keine oder weniger genaue Fahrhinweise gibt. Die Nettovorteile, die sich aus der Forderung nach der Geheimhaltung von Standortdaten auf Smartphones ergeben würden, lägen daher bei 1,20 Dollar (► **Abb. 3**, erster Balken von rechts) abzüglich der Tatsache, wie sehr die Menschen qualitativ hochwertige Wegbeschreibungen auf ihrem Telefon schätzen. Dasselbe Argument gilt für alle Arten von Daten“ [6]. Da die Teilnehmer



► **Abb. 3** Menschen in allen 6 Ländern vertrauen ihrem Mobilfunkanbieter (blaue Säulen) weniger als Facebook (rote Säulen), denn der müsste mehr als Facebook bezahlen, um Kontaktinformationen zu erhalten (Mitte). Nur in Deutschland misstraut man Facebook nahezu ebenso stark wie dem Mobilfunkanbieter. Auch der Smartphone-Firma (orange Säulen) misstrauen die Deutschen mehr als die Menschen in den anderen Ländern, wenn es um Daten zum Standort geht (rechts). Man sieht auch hier im Vergleich zum Mobilfunkanbieter (blaue Säulen), dass diesem weniger vertraut wird (d. h. es wird mehr Geld verlangt). Auch beim Vergleich der geforderten Kosten für das Zulassen von Werbung (links) von Bank, Smartphone-Firma und Mobilfunkanbieter schneidet dieser am ungünstigsten ab. Negative Werte zeigen hier an, welcher Plattform die Menschen in den Ländern für Werbung bezahlen würden (nach Daten aus [6]).

nur danach gefragt wurden, was ihnen die Aufgabe von Privatsphäre wert ist, und nicht danach, wieviel sie dafür bezahlen würden, weil sie einen Nutzen davon haben, ist auch keine Differenzbildung zur Abwägung von Kosten und Nutzen möglich.

Eine zweite Studie zum Datenschutz stammt aus den USA und dreht sich um den Schutz privater individueller, genetischer Informationen in Biobanken. Dies wurde in den USA vor Jahren schon immer wichtiger, weil dort bereits Millionen von Men-

schen ihr ganz privates Genom aus Interesse an ihrer Abstammung durch private Anbieter dieses „Services“ haben untersuchen lassen. In einem Einwanderungsland, in dem die Herkunft und diesbezügliche Traditionen grundsätzlich mehr beachtet und vor allem gepflegt werden als in den (sich weiterentwickelnden) Herkunftsländern ist dies kein Wunder. Auch gibt es eine zunehmende Zahl von Firmen, die aufgrund von genetischen Informationen bestimmte Dienstleistungen, wie z. B. personalisierte Medizin, anbieten.

Biobanken spielen gerade in der Genforschung eine große Rolle, da die Auswertung und Analyse einer großen Zahl von Datensätzen die notwendige Voraussetzung dafür ist, diese Daten dann auch auf der Ebene des Einzelnen beispielsweise für eine personalisierte medizinische Behandlung fruchtbar zu machen. Solche Biobank-Forschung bringt jedoch neue ethische, soziale und politische Herausforderungen, die über den Datenschutz im Rahmen der bisherigen biomedizinischen Grundlagenforschung hinausgehen. Man sprach diesbezüglich auch schon von einer „neuen Bankenkrise“ [8] – und meinte damit nicht Geldinstitute, sondern Forschungsbiobanken. Frühere Umfragen gaben jedoch Entwarnung, denn solche Daten wurden zunächst meist von akademischen Institutionen erhoben. Dabei lag (mindestens implizit) die Betonung grundsätzlich darauf, dass die teilnehmenden Personen ihre genetischen Daten freiwillig zur weiteren Nutzung zur Verfügung stellten [4]. So gab es in einer der größten Umfragen zur Einstellung gegenüber einem Biobank-Forschungsprojekt bei 13 000 Teilnehmern keine Hinweise darauf, dass die Zustimmung zur Teilnahme von der Strenge der Datenschutzbestimmungen abhing [7]. Als Vorteil der Studie nannten 84% (und damit die meisten) der Befragten: „Ich hätte das Gefühl, dass ich künftigen Generationen helfen würde“ [7]. Allerdings, nach ihren Sorgen befragt, gaben mit noch 51% die meisten Teilnehmer an, sich über ihre Privatheit zu sorgen. Die von nur 36% der Befragten am wenigsten bejahte Sorge war: „Ich würde mir Sorgen machen, dass jemand mit meinen Gesundheitsinformationen Geld verdienen könnte.“

In einer systematischen Übersicht von 53 Studien mit insgesamt 47 974 Teilneh-

mern zu Fragen der Privatsphäre im Zusammenhang mit menschlichen genetischen Daten waren die Befragten mehr besorgt über die Nutzung durch Arbeitgeber, Versicherer und die Regierung als durch Forscher und kommerzielle Einrichtungen [3]. Es zeigte sich zudem, dass viele Teilnehmer die Privatsphäre, Vertraulichkeit, Kontrolle und Sicherheit miteinander zu vermischen schienen.

Weil die genetische Forschung gerade sehr rasch fortschreitet, könnte es auch in den Köpfen der Leute schnelle Änderungen geben, die wiederum die Forschung beeinträchtigen könnten. So könnte das wachsende Bewusstsein für den kommerziellen Wert genetischer Daten die Leute misstrauisch machen, wie beispielsweise die Kooperation der Firmen GlaxoSmithKline (Pharma-Branche) und 23andme (Genom-Analyse). Berichte über Hacker-Angriffe im Gesundheitswesen machen die Lage nicht besser und schüren weiteres Misstrauen. Weil aber Gen-Datenbanken auf die Mitwirkung der Bevölkerung angewiesen sind, muss man fragen dürfen, wie diese jüngsten Entwicklungen die Erwartungen der Öffentlichkeit beeinflussen könnten.

Vor diesem Hintergrund wurde der kürzlich publizierte Genomic Data Governance Survey (GDGS) im Befragungszeitraum vom 27. November bis 20. Dezember 2018 durchgeführt, in dessen Rahmen 2020 Teilnehmer nach ihrer Bereitschaft gefragt wurden, ihre Daten zur Verfügung zu stellen. Die andere Frage zielte auf die Bezahlung ab, die sie als Gegenleistung erwarten würden. Hierzu wurde den Befragten zunächst mittels einer 3-minütigen Präsentation öffentlich zugängliche Informationen dazu gegeben, wie genetische Datenbanken verwendet werden, was mit diesen Daten geschieht und welche Vorteile sowie Risiken für Personen daraus folgen können, die ihre Daten zur Verfügung stellen (► **Abb. 4**).

Dann wurden die Teilnehmer per Zufall in 5 Gruppen eingeteilt, wobei die Einteilung entlang 5 Organisationsformen erfolgte, die als vermeintlicher Absender der Fragen fungierten (jeweils charakterisiert mit einem kurzen Satz, der im Folgenden im Original wiedergegeben wird [2]):

- „Genetic Data Inc. is a U. S. for-profit technology corporation;
- GreatCare Hospital is a U. S. non-profit hospital system;
- Genomics & Health Research Lab is located at Middle State University;
- BioPharmaCo is a global for-profit drug company;
- The National Institutes of Health (NIH) is a U. S. federal research agency.“

Die Autoren weisen im Hinblick auf diese Namen und Beschreibungen darauf hin, dass sie bewusst den Begriff „Krankenhaus“ (hospital) und nicht „Academic Medical Center“ verwendeten, weil frühere ähnliche Umfragen die Biobank in den Kontext von akademischen, medizinischen Zentren oder einer Universitätsklinik eingebunden hatten. Danach gingen die Autoren wie folgt vor: „Um die grundsätzliche Bereitschaft zur Bereitstellung von Daten zu ihrem Genom zu messen, wurden die Befragten dann über eine Gelegenheit von der Organisation, der sie zufällig zugewiesen wurden, informiert. Der hierzu verwendete Vignettentext war bis auf die Namen und Beschreibungen der Organisationen identisch. Der Vignettentext einer z. B. gewinnorientierten Institution lautete beispielsweise wie folgt: ‚Stellen Sie sich vor, dass Sie heute die Gelegenheit haben, Ihre DNA-Daten der Firma Genetic Data Inc. für ein biomedizinisches Forschungsprogramm zur Verfügung zu stellen. Sie erhalten Ihre DNA-Daten, wenn Sie der Firma eine kleine Speichelprobe zur Verfügung stellen. Genetic Data Inc. ist ein US-amerikanisches gewinnorientiertes Technologieunternehmen. Wie bereit wären Sie, Ihre genetischen Daten der Firma Genetic Data Inc. zur Verfügung zu stellen, im Lichte dessen was Sie gerade über Biobanken und die Firma erfahren haben. Wählen Sie bitte eine der folgenden 4 Optionen.‘

Die 4 Antwortmöglichkeiten waren (in jeweils zufälliger Reihenfolge):

- ‚Zur Spende für wohltätige Zwecke bereit‘ (im Folgenden als ‚Spender‘ bezeichnet);
- ‚Zur Spende gegen einen bestimmte Geldbetrag bereit‘ (als ‚Verkäufer‘ bezeichnet);
- ‚Unwillig zur Spende, zumindest im Moment‘;

Recent and Future Trends with DNA Data

- Today your unique DNA sequence can be rapidly generated and digitally stored, just from saliva, for about \$100
- When data from many people are combined together, the resulting DNA database can be used for many different purposes. For example:
 - medical research (e.g. finding new pharmaceutical drugs)
 - health care (e.g. testing for risk of breast cancer)
 - family ancestry research
 - citizen identity verification
 - crime-scene investigation
 - and more

DNA data also reveal a lot about you

- These databases can be used to predict physical and mental risks for each individual. For example:
 - Risks of depression, dementia, and having children with birth defects
- Your risks can also be discovered from your relative's data
 - Even if your own data is missing
- The databases can also be used to prove (or disprove) paternity
- And to catch criminals. For example:
 - The cold-case "Golden State Killer" was recently caught using a commercial database that happened to include DNA from his relative

What is the financial value of DNA data?

- As these databases prove useful, their financial value is being realized
 - Bigger is better: Some have millions of people's DNA in them
 - Many combine DNA with medical records & personal information
- Companies and hospitals are starting to sell and rent access to DNA databases
- These transactions suggest companies may be willing to pay \$130 per sample for database access (Reuters 2018)

Providing your DNA data

- Currently, some organizations will pay you to obtain your DNA data
- Others offer to obtain it in exchange for a personalized report on your health risks and ancestry information
- Still others ask you to donate it for free, as a charitable act that contributes to medical research
- Regardless of how they obtain it, most organizations agree to attempt to protect the data and your privacy
- You also must sign a legal document acknowledging that you understand there are still privacy risks; your data could still be stolen or misused

► **Abb. 4** Informationen für die Teilnehmer vor Beginn der Befragung. Mit den Zahlenangaben wurde den Teilnehmern eine ungefähre Vorstellung ihrer Antworten bewusst gegeben (nach Daten aus [2]).

- ‚Generell unwillig zur Spende‘ (beide Optionen werden im Folgenden mit ‚nicht willens‘ bezeichnet) [2].

Den „Verkäufern“ [...] wurden dann die Folgefrage gestellt, wieviel Geld sie als Bezahlung von Genetic Data Inc. (bzw. der jeweils benannten Institution) erwarteten. Sie hatten dann die Möglichkeit, den Betrag in US\$ einzugeben. Um zu erfassen, wie viel den Befragten Informationen über ihr persönliches Genom wert war, wurden alle zudem wie folgt gefragt: „Stellen Sie sich vor, Sie hätten die Möglichkeit, einen Bericht mit Informationen über Ihre Abstammung und über Ihr persönliches Risiko für 20 verschiedene, genetisch bedingte Krankheiten zu

erhalten. Dafür benötigt die Institution eine Speichelprobe mit Ihrer DNA. In diesem Fall werden Ihre DNA-Daten jedoch nicht gespeichert oder für einen anderen Zweck verwendet. Wieviel wären Sie bereit, für diesen Bericht zu zahlen?“ [2]. Danach konnten die Teilnehmer erneut einen Betrag in US\$ eingeben.

Um den Einfluss der Regelungen zur Datenweitergabe und Datensicherheit auf die Bereitschaft der Teilnehmer, ihre Daten zur Verfügung zu stellen, zu untersuchen, wurden die Teilnehmer anschließend noch gebeten, 12 in randomisierter Reihenfolge vorgestellte Richtlinien zu beurteilen (► **Abb. 5**). Nach jeder Richtlinie wurden

die Befragten gebeten, eine von 5 Antwortmöglichkeiten auszuwählen:

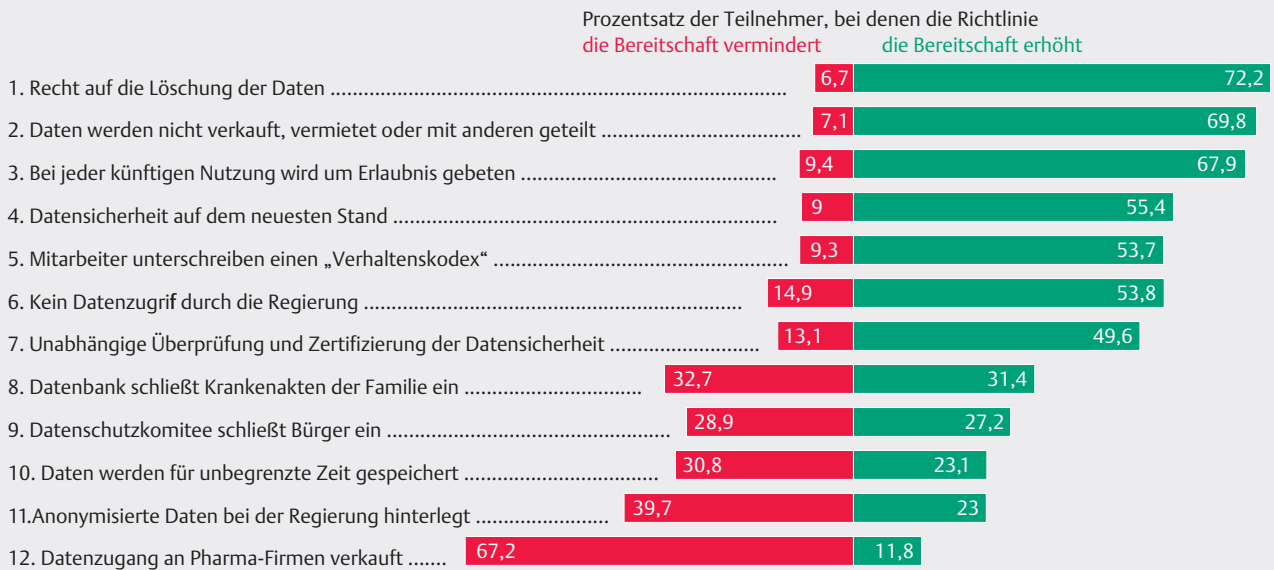
- „reduziert die Bereitschaft stark“;
- reduziert die Bereitschaft etwas“;
- kein Effekt“;
- erhöht die Bereitschaft etwas“;
- erhöht die Bereitschaft stark“ [2].

Das vielleicht wichtigste Ergebnis der Studie besteht darin, dass im Vergleich zu früheren ähnlichen Befragungen (bei denen für gewöhnlich mehr als 50 % zur Spende bereit waren) die Bereitschaft zur Spende der Informationen deutlich geringer war: Nur 11,7 % aller Teilnehmer (n = 234) waren „Spender“. Demgegenüber waren 37,8 % (n = 764) keinesfalls bereit zur Überlassung ihrer Daten, und die Mehrheit (50,6 %; n = 1022) wollte die Daten nur gegen Bezahlung hergeben („Verkäufer“). Der verlangte Preis lag im Mittel bei 130 US\$ (entsprach also dem in der Vorabinformation genannten „üblichen Preis“). Gefragt danach, wieviel sie für einen Bericht über ihr privates Genom bezahlen würden, antworteten Spender im Mittel mit 75 US\$ und „Verkäufer“ mit 95 US\$.

Im Hinblick auf die 5 unterschiedlichen Institutionen gab es keine großen Unterschiede: Bei „Krankenhaus“ gab es mit 14,5 % vergleichsweise mehr „Spender“, bei Universität (14,0 %) und „Regierung“ (12 %) absteigend weniger. Noch weniger „Spender“ gab es bei „Technologie-“ (10,9 %) und Pharma-Firmen (6,2 %). Über den Einfluss der Richtlinien zur Benutzung der Biodatenbank auf die Bereitschaft, seine Daten zu spenden, informiert ► **Abb. 5**, in der die Richtlinien gelistet sind, in Abhängigkeit davon, wie sehr sie die Bereitschaft zur Spende steigern konnten.

Wenn die eigenen Daten auf Antrag gelöscht werden oder nicht verkauft, vermietet oder mit anderen geteilt werden, erhöht das die Bereitschaft zur Spende am ehesten. Der Verkauf an eine pharmazeutische Firma reduziert diese am meisten. „Spender“ und „Verkäufer“ unterschieden sich vor allem bei den Richtlinien 8, 10 und 11, die bei den „Spendern“ die Bereitschaft noch stärker senkten.

Im Hinblick auf die 5 Typen von Institutionen waren die 12 Richtlinien (bis auf Richtlinie 7) von kaum unterschiedlicher Wir-



► **Abb. 5** Einfluss der Regelungen zur Datenweitergabe und Datensicherheit auf die Bereitschaft der Teilnehmer, ihre Daten zur Verfügung zu stellen. (Die Werte addieren sich nicht zu 100 %, weil der Anteil derjenigen, die gegenüber der Regelung neutral waren, nicht angegeben ist (nach Daten aus [2]).

kung. Die Einschätzung der Risiken und Vorteile der eigenen genetischen Daten ist also weitgehend unabhängig davon, von wem sie verwaltet werden. Die deutliche Präferenz für Einschränkungen über die gemeinsame Nutzung der Daten oder deren Wiederverwendung (ohne ausdrückliche Genehmigung des Einzelnen) ist ein Problem für die öffentlichen, aber insbesondere auch für die privaten Biobanken.

Insgesamt zeigt die Studie, dass die Leute heute weniger bereit sind, ihre Daten freiwillig zu spenden und – offenbar auch in den USA – auf Datenschutz einen zunehmenden Wert legen. Die vielfach eingeforderte höhere Kontrolle über die eigenen Daten macht das Leben der mit Biobanken arbeitenden Menschen nicht leichter. Unberücksichtigt blieben von den Autoren (dem Design der Studie geschuldet) die lokalen oder gar persönlichen Beziehungen zwischen den Managern und den Kunden der Biobanken. Wenn also das örtliche Krankenhaus zur Datenspende auffordert, könnte es um die Spendenbereitschaft anders (d. h. deutlich besser) bestellt sein.

Im Lichte der ersten, diskutierten Studie, ist die zweite Studie definitiv begrenzt, da man wirklich gerne wüsste, wie es um die Sorgen der Deutschen um Informationen über ihre Gene bestellt ist. Aber wir

sind im Hinblick auf die kommerzielle Anwendung den USA um Jahre hinterher (ich kenne persönlich hierzulande niemanden, der sein Genom hat sequenzieren lassen, jedoch durchaus einige Amerikaner, die das spaßeshalber – „kostet ja nur 100 Dollar“ – schon gemacht haben). Daher fehlen uns auch vielfache persönliche Erfahrungen mit solchen Daten. Und deswegen sind wir entweder ahnungslos oder ängstlich oder beides, denn was man nicht kennt, macht Angst.

Fassen wir zusammen: Man weiß letztlich nur wenig darüber, wie wichtig den Menschen tatsächlich der Schutz der Privatsphäre im Hinblick auf personenbezogene Daten ist. Die Antwort aus der ersten dargestellten länderübergreifenden Studie auf diese Frage ist klar: Uns Deutschen ist der Datenschutz deutlich mehr wert als anderen Nationen. Weiterhin kam heraus, dass der Datenschutz je nach Datentyp (Bankkonto, Texte, Fingerabdruck, Standort etc.), Land (Argentinien, Brasilien, Deutschland, Kolumbien Mexiko und die USA) und Institution (z. B. Telecom, Sparkasse, Facebook oder Apple) zwischen gar nichts und etwa 15 US\$ monatlich Wert ist. Eine zweite, nur in den USA durchgeführte Studie ergab, dass man nur wenig bereit ist, Daten zum eigenen Genom freiwillig zu spenden, sondern im Schnitt dafür 130 US\$ haben möch-

te. Wenn auch die erste Studie keinen Effekt des vorherigen Briefings auf die danach erfragten Bewertungen ergab, so muss man für die zweite Studie durchaus zu bedenken geben, was man wohl erwarten, wenn man Versuchspersonen vorher sagt, dass das eigene Genom 130 US\$ wert ist, und sie dann fragt, für wie viel Geld sie diese Information verkaufen würden? – 130 US\$ (wer hätte das gedacht?). Interessant ist, dass man in der zweiten Studie (also in den USA) gegenüber privaten und öffentlichen Institutionen kaum verschieden eingestellt war, und dass die Ergebnisse (im Vergleich zu den Ergebnissen früherer ähnlicher Studien) klar zeigen, dass man auch dort den Datenschutz für wichtiger zu nehmen beginnt.

Insgesamt empfand nicht nur ich als Rezipient der Studien, dass die Menschen erstaunlich wenig Geld für Datenschutz einzutauschen bereit sind, haben doch 2 Berichte im New Scientist diesbezüglich etwa den gleichen Tenor [5, 10].

Tritt man 2 Schritte zurück und nimmt nicht nur eine empirisch-naturwissenschaftliche, sondern zugleich auch eine geisteswissenschaftliche Perspektive ein, so stellt sich in Anbetracht beider Studien die Frage nach deren Relevanz für die Praxis. Das sehen die Autoren der ersten Studie sehr prag-

matisch, schreiben sie doch in der Einleitung: „Wenn wir zum Beispiel feststellen sollten, dass die Europäer bestimmte Elemente ihrer Privatsphäre mehr schätzen als die USA, dann könnte eine strenge Datenschutzregelung wie die, die durch europäische Datenschutzgrundverordnung geschaffen wurde, in Europa, aber nicht in Amerika, Nettovorteile bringen“⁴ [6].

Man muss ihnen entgegenhalten, dass es bei Verordnungen oder Gesetzen nie nur um das geht, was Menschen tun, sondern auch um das, was sie tun sollen. Man hat keine Studie gemacht, ob man in Kalifornien über den Datenschutz anders denkt als in den übrigen US-Bundesstaaten, bevor man den dortigen strengen Datenschutz (CCPA; ähnlich streng wie die DSGVO in der EU) eingeführt hat. Man hat sich vielmehr überlegt, was für die Menschen und sogar die Wirtschaft gut ist, denn es sind kalifornische Firmen, die ihre digitalen Produkte weltweit verkaufen und damit zu den reichsten Firmen der Welt geworden sind. Das soll aus deren Sicht so bleiben, weswegen man sich besser dem weltgrößten Binnenmarkt – der EU – anpasst. Und auch die EU hat gar keine Studie gemacht, bevor sie die DSGVO eingeführt hat. – Warum? – Weil es bei Recht und Gesetz nicht allein um physikalische Realität geht, sondern auch um deren Bewertung durch viele, in Gemeinschaft lebende Menschen. Schon immer haben sich Menschen in Gemeinschaft Normen unterworfen, die jeden einzelnen in seiner Freiheit beschneiden, aber dem Großen und Ganzen der Gemeinschaft dienlich sind. Dieses betrifft weitaus mehr als sich in US\$ ausdrücken lässt. Grundwerte wie Kommunikationsgemeinschaft, Freiheit, Privatheit, Solidarität, Vertrauen, Gerechtigkeit

4 “If, for example, we were to discover that Europeans value certain elements of their privacy more than the U.S., then a strict privacy regime like that created by GDPR might yield net benefits in Europe but not America.”

sowie Schutz des Lebens und der Lebensgrundlagen sollten nicht täglich nach ökonomischen Prinzipien ausgehandelt werden dürfen, weil es eben genau diese Prinzipien Werte sind, die solches Aushandeln überhaupt erst möglich machen.

Diese Position ist – das muss hier gesagt sein dürfen – nicht Empirie-feindlich. Im Gegenteil: Sie schützt auch die Freiheit der empirischen Forschung, die uns immer wieder Überraschendes über uns selbst vor Augen hält, einen Spiegel, der uns unser wahres Gesicht zuweilen deutlicher zeigt als die unser – zuweilen rosa verzeichnendes – geistiges Auge allein vermag.

Interessenkonflikt

Es liegt kein Interessenkonflikt vor.

Korrespondenzadresse

Prof. Dr. Dr. Manfred Spitzer
Universität Ulm
Abteilung für Psychiatrie
Leimgrubenweg 12–14
89075 Ulm

Literatur

- [1] Bhageshpur K. Data Is The New Oil – And That’s A Good Thing. Forbes Technology Council, 15. November 2019. www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/#536ea5d37304, abgerufen am 9.4.2020
- [2] Briscoe F, Ajunwa I, Gaddis A et al. Evolving public views on the value of one’s DNA and expectations for genomic database governance: Results from a national survey. PLoS ONE 2020; 15 (3): e0229044. doi. journal.pone.0229044
- [3] Clayton EW, Halverson CM, Sathe NA et al. A systematic literature review of individ-

uals’ perspectives on privacy and genetic information in the United States. PLoS ONE 2018; 13 (10): e0204417

- [4] Kaufman D, Murphy J, Scott J et al. Subjects matter: a survey of public opinions about a large genetic cohort study. Genet Medicine 2008; 10: 831–839
- [5] Murugesu J. Half of people in the US would sell their genetic data for \$95. New Scientist 2020; 3274; 21.3.2020. www.newscientist.com/article/2237162-half-of-people-in-the-us-would-sell-their-genetic-data-for-95/ 3; abgerufen am 8.4.2020
- [6] Prince J, Wallsten S. How Much is Privacy Worth Around the World and Across Platforms? Technology Policy Institute (TPI), 409 12th Street SW, Suite 700, Washington, DC 20024; January 2020. techpolicyinstitute.org/wp-content/uploads/2020/02/Prince_Wallsten_How-Much-is-Privacy-Worth-Around-the-World-and-Across-Platforms.pdf; abgerufen am 8.4.2020
- [7] Sanderson SC, Brothers KB, Mercaldo ND et al. Public Attitudes toward Consent and Data Sharing in Biobank Research: A Large Multi-site Experimental Survey in the US. The American Journal of Human Genetics 2017; 100: 414–427
- [8] Scott CT, Caulfield T, Borgelt E et al. Personal medicine – the new banking crisis. Nature Biotechnology 2012; 30: 141–147
- [9] Spitzer M. www (WeltWeite Werbung) und die Folgen. Radikalisierung, Spionage, Vertrauens- und Wahrheitsverlust. Nervenheilkunde 2018; 37: 303–311
- [10] Stokel-Walker C. People will sell access to their fingerprints for just \$7.56 a month. New Scientist 2020; 3269; 15.2.2020. www.newscientist.com/article/2232793-people-will-sell-access-to-their-fingerprints-for-just-7-56-a-month/ 3; Abgerufen am 8.4.2020

Bibliografie

DOI <https://doi.org/10.1055/a-1094-9959>
Nervenheilkunde 2020; 39: 417–423
© Georg Thieme Verlag KG Stuttgart · New York
ISSN 0722-1541