



FORUM PRIVATHEIT UND SELBSTBESTIMMTES
LEBEN IN DER DIGITALEN WELT

Policy Paper

DATENSPARSAMKEIT ODER DATENREICHTUM?

**Zur neuen politischen Diskussion
über den datenschutzrechtlichen
Grundsatz der Datensparsamkeit**

IMPRESSUM

Autoren:

Alexander Roßnagel, Michael Friedewald, Christian Geminn, Thilo Hagendorf, Jessica Heesen, Thomas Hess, Michael Kreutzer, German Neubaum, Carsten Ochs, Hervais Simo Fhom

Kontakt:

Michael Friedewald

Telefon +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:

Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt

ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage, August 2017



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz.

Datensparsamkeit oder Datenreichtum?

Datensparsamkeit oder
Datenreichtum?

Ist Datensparsamkeit überholt?

In der politischen Diskussion ist immer häufiger die Einschätzung anzutreffen, Datensparsamkeit sei überholt und gehöre „ins vergangene Jahrhundert“ (Merkel auf dem CDU-Parteitag am 6.12.2016). Vizekanzler Gabriel forderte am 17.11.2016, „dass wir uns endgültig verabschieden müssen von dem klassischen Begriff des Datenschutzes, weil der natürlich nichts anderes ist als ein Minimierungsgebot von Daten. Das ist ungefähr das Gegenteil des Geschäftsmodells von Big Data“. Das Netzwerk Digitalisierung der CDU fordert in seinem Strategiepapier vom 13.6.2017: „Datensparsamkeit kann heute nicht mehr die generelle Verhaltensleitlinie sein. Denn sie reduziert Chancen für neue Produkte, Dienstleistungen und Fortschrittmöglichkeiten“. „Gute Rahmenbedingungen“ für das „Management von riesigen Datenmengen ... – Big Data“ – zu schaffen, „das ist eine Aufgabe, auch für Europa. ... Wer sich nicht daran beteiligt, die Vielzahl an Daten zu nutzen, sei es in der Medizin, sei es in der Zukunft der Mobilität, sei es in Angeboten der Plattform-Wirtschaft, der wird zurückfallen und nicht die Arbeitsplätze der Zukunft haben. Und deshalb müssen wir vorne mit dabei sein.“ (Merkel 6.12.2016). Ähnlich haben sich in jüngster Zeit viele weitere Politikerinnen und Politiker der Großen Koalition geäußert.

**Datensparsamkeit in der
Politik**

Zutreffend ist: Die fortschreitende Digitalisierung aller Lebens-, Wirtschafts- und Verwaltungsbereiche führt dazu, dass immer mehr Daten erhoben, verarbeitet und genutzt werden. Daher liegt der Schluss nahe: Wenn Digitalisierung nicht zu verhindern ist, wenn sie sogar große Entwicklungschancen verspricht, müssen die dafür notwendigen Datenverarbeitungen ermöglicht werden. Also lieber Datenreichtum statt Datenarmut? Aber geht es bei Datensparsamkeit tatsächlich darum, die Verarbeitung von Daten zu verhindern und den gesellschaftlichen Fortschritt zu bremsen? Dieses Policy Paper klärt Missverständnisse und bietet notwendige Differenzierungen für eine sachliche Diskussion über Datensparsamkeit.

Was sind die Gründe für die Forderung nach Aufgabe der Datensparsamkeit?

Heutzutage findet sich eine Vielzahl an Diensten im Internet, die Konsumenten kostenfrei nutzen können. Populäre Beispiele sind die Suchmaschine von Google oder das soziale Netzwerk von Facebook. Doch die Nutzung ist nur auf den ersten Blick kostenfrei. Zwar fällt kein Nutzungsentgelt an. Die Nutzer zahlen allerdings indirekt mit ihren personenbezogenen Daten, mit denen der in Anspruch genommene Internetdienst Geld verdient, etwa indem er personalisierte Werbung auf Basis der personenbezogenen Daten anbietet. Der Internetdienst gewährt Werbenden somit nicht nur Zugang zu allen Nutzern, sondern kann aufgrund der personenbezogenen Daten eine Vorauswahl der Zielgruppe vornehmen, was der Effektivität der Werbemaßnahmen zugutekommt. Bei Facebook ist dieses Vorgehen Kern des Geschäftsmodells. Anbieter anderer Internetdienste, etwa auch Onlineshops, verwenden personenbezogene Daten, um personalisierte Dienste anzubieten. Dies kann Kunden durchaus einen Nutzen stiften, z. B. geringere Suchkosten, und die Qualität des Dienstes erhöhen, z. B. schnellere und bessere Suche.

Zunahme datenbasierte Geschäftsmodelle

Die aktuelle Debatte ist auch vor der Frage zu sehen, welche wettbewerblichen Rahmenbedingungen deutsche Internetdienste haben, wenn es um die Frage geht, welche Daten sie wie nutzen dürfen. So haben US-Unternehmen vielfach nicht nur eine große Marktmacht bei den Internet-Diensten für Konsumenten. Sie profitieren dabei gebe-

Besorgnis aufgrund ungleicher Wettbewerbsbedingungen

nenfalls auch von den im Vergleich weniger restriktiven US-Datenschutzbestimmungen sowie von der immer noch schwierigen Durchsetzbarkeit europäischen und deutschen Rechts ihnen gegenüber. Etliche Politiker befürchten, dass deutsche Unternehmen, die personenbezogene Daten verwenden, aufgrund eines zu restriktiven Datenschutzrechts im (internationalen) Wettbewerb einen Nachteil hätten und somit das Prinzip der Datensparsamkeit letztlich zu Wachstumseinbußen in Deutschland führe.

Was bedeutet Datensparsamkeit?

Die Bezeichnung „Datensparsamkeit“ ist missverständlich. Dieses Prinzip des Datenschutzrechts zielt nicht darauf ab, möglichst wenige Daten zu verarbeiten. Entscheidend ist nicht die Menge der Daten an sich, sondern ausschließlich ihr Personenbezug. Dieser ist aus Gründen der Vorsorge möglichst gering zu halten. Datensparsamkeit steht somit nicht im Widerspruch zur Verarbeitung vieler Daten. Sie greift nur bei Daten, die sich auf einzelne natürliche Personen beziehen.

Das datenschutzrechtliche Prinzip, den Personenbezug der Daten auf das geringstmögliche Maß zu beschränken, hat zwei Erscheinungsformen. Zum einen beschränkt es den Eingriff in die Grundrechte der betroffenen Person auf das Unvermeidbare. Nur wenn auf die konkrete Datenverarbeitung hinsichtlich des Umfangs, der Form und der Zeit nicht verzichtet werden kann, um den von dem Verantwortlichen gewählten Zweck zu erreichen, ist die Datenverarbeitung erforderlich. Als Regel zur Abwehr von übermäßigen Grundrechtseingriffen bezieht sich das Prinzip auf den konkreten Datenverarbeitungsvorgang. Wenn etwa der Browser-Fingerprint des Kundenrechners, die zuvor besuchten Seiten sowie Alter und Geschlecht nicht für die Erfüllung eines E-Commerce-Vertrags erforderlich sind, ist die Erhebung dieser Daten zu unterlassen.

Zum anderen zielt Datensparsamkeit auf Vorsorgemaßnahmen, um Grundrechtsgefährdungen soweit wie möglich zu reduzieren. Je weniger personenbezogene Angaben über eine natürliche Person gesammelt werden, desto geringer ist das Schadenspotential der jeweiligen Datenverarbeitung. Die Notwendigkeit, solche Vorsorgemaßnahmen zu ergreifen, ergibt sich vor allem aus der „Explosion“ der Menge personenbezogener Angaben und aus der Globalisierung der Datenverarbeitung und der damit verbundenen besonderen Erhöhung der Grundrechtsrisiken. Unter bestimmten Umständen wird Datensparsamkeit sogar zum einzig verbleibenden Mittel, um das Grundrecht auf Datenschutz zu gewährleisten und informationelle Selbstbestimmung auszuüben. Personenbezogene Daten, die im Rahmen vernetzter Informationsverarbeitung entstehen und verarbeitet werden, sind für die betroffene Person faktisch nicht mehr kontrollierbar, ihre Berichtigung oder Löschung ist praktisch nicht mehr durchsetzbar – insbesondere, wenn sich die personenbezogenen Angaben nicht mehr in der Europäischen Union befinden. Dieses Risiko nimmt in Umgebungen allgegenwärtiger Datenverarbeitungen (z. B. Internet der Dinge) noch erheblich zu. In all diesen Fällen kommt es entscheidend auf die vorsorgende Vermeidung personenbezogener Angaben an.

Als Ausdruck des Vorsorgeprinzips bezieht sich die Datensparsamkeit auf die Gestaltung von Datenverarbeitungssystemen: Soweit etwa die Zielsetzung des Systems dies ermöglicht, sind sie so zu gestalten, dass sie mit anonymen oder pseudonymen Daten arbeiten. Weiteres Beispiel: Wenn es etwa darum geht, eine Dienstleistung abzurechnen, sollte dies – wenn möglich – auf der Basis einer Flatrate erfolgen, um die Erhebung von Leistungsdaten hinsichtlich Datenumfangs oder Nutzungszeiten zu vermeiden, die notwendig wäre, wenn die Dienstleistung nach Umfang oder Zeiträumen abgerechnet wird.

Entscheidend für das Prinzip der Datensparsamkeit ist, dass es nicht darauf zielt, die Verarbeitung jeder Form von Daten zu vermeiden. Vielmehr ist es von der Zielsetzung des Persönlichkeitsschutzes her dann erfüllt, wenn der Personenbezug von Daten vermieden wird. Es ist daher ausreichend, wenn von den Daten nicht auf eine bestimmte natürliche Person geschlossen werden kann.

Datensparsamkeit regelt und erlaubt freien Datenfluss ...

... und reduziert die dabei anfallenden Grundrechtsgefährdungen ...

... indem der Personenbezug von Daten verringert wird

Das Prinzip der Datensparsamkeit ist dreistufig angelegt. Zunächst enthält es die Vorgabe, auf personenbezogene Daten vollständig zu verzichten, wenn die Funktion der Datenverarbeitung auch anderweitig erbracht werden kann. Kann dieses Ziel mangels alternativer Möglichkeiten nicht erreicht werden, ist der Verantwortliche gehalten, den Verarbeitungsprozess so zu gestalten, dass die Verwendung personenbezogener Daten minimal ist – z. B. durch eingeschränkte und besonders kontrollierte Zugriffsmöglichkeiten. Die dritte Stufe beinhaltet die zeitliche Beschränkung, die personenbezogenen Daten so früh wie möglich zu löschen, zu anonymisieren oder zu pseudonymisieren.

Die Umsetzung dieses Konzepts von Datensparsamkeit leidet daran, dass angesichts der enormen Mengen an gespeicherten personenbezogenen Daten die Instrumente der Anonymisierung und Pseudonymisierung immer schwieriger einzusetzen sind. Von Anonymität und Pseudonymität kann nämlich nur dann gesprochen werden, wenn die Daten „nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können“ (§ 3 Abs. 6 BDSG). Angesichts der immer besseren Auswertungsmöglichkeiten von Big Data-Analysen erhöhen sich die Anforderungen an eine wirksame Vermeidung des Personenbezugs und verschieben sich dynamisch die Grenzen einer nachhaltigen Anonymisierung oder Pseudonymisierung.

Um dieser Herausforderung entgegenzuwirken, sind in den letzten Jahren vielfältige technische Konzepte zur Förderung der Datensparsamkeit vorgeschlagen worden. Beispiele derartiger Konzepte sind Ansätze zur Gewährleistung der Anonymität auf Netzebene wie z. B. Mix-basierte Routing-Protokolle und Mechanismen zur selektiven sowie anonymisierten Weitergabe von sensitiven personenbezogenen Daten.

Entsprechende technische Umsetzungen dieser theoretischen Konzepte existieren – werden allerdings in der Praxis in der Regel als Selbstschutz-Tools eingesetzt und bislang kaum in Angebote von Unternehmen integriert. Dies ist insbesondere der Fall für datenminimierende Authentifizierungsmechanismen, die aufgrund ihrer Eigenschaften in diesem Zusammenhang als besonders vielversprechend erscheinen, jedoch noch zu wenig im großflächigen praktischen Einsatz zu finden sind. Zu den Eigenschaften solcher Systeme – der datenschutzfördernden attributbasierten Berechtigungsnachweise („Privacy-Enhancing Attribute-Based Credentials“) – gehören Möglichkeiten, Eigenschaften zu beweisen („ist volljährig“ oder „ist Mitglied von“), statt vollständige Daten zu offenbaren (wie das Geburtsdatum oder Name und Mitgliedsnummer). Auch lässt sich – anders als in der analogen Offline-Welt – sicherstellen, dass ein solcher digitaler Ausweis beim Verwenden gegenüber verschiedenen Stellen oder zu verschiedenen Zeiten auch verschieden aussieht. Dies bedeutet, dass sich die digitalen Daten nicht miteinander zu einem Nutzungsprofil verknüpfen lassen. Für einige Anwendungsbereiche bietet der neue Personalausweis datensparsame Nutzungsmöglichkeiten, beispielsweise für den Online-Nachweis der Volljährigkeit ohne Bekanntgabe des Geburtsdatums.

Wollen Verantwortliche personenbezogene Daten an Dritte übermitteln, müssen diese vorab anonymisiert oder pseudonymisiert werden. Auch hierfür existieren bereits einige Konzepte, wie etwa Datenanonymisierungsansätze auf der Grundlage von Differential Privacy oder kryptographische Verfahren, die Berechnungen auf verschlüsselten Daten ermöglichen. Trotz ihrer theoretischen Vorzüge werden diese Konzepte allerdings in der Praxis bislang kaum eingesetzt. Hier besteht ein hoher Forschungsbedarf, um solche Konzepte mittel- und langfristig zu (Teil-)Lösungen weiterzuentwickeln und umzusetzen.

Aber auch wenn Anonymisierung oder Pseudonymisierung gelingen und von den verfügbaren Daten nicht auf bestimmte natürliche Personen geschlossen werden kann, können durch Big Data und statistische Verfahren Probleme für die Selbstbestimmung entstehen. Diese bestehen u. a. in der Verwendung diskriminierender Merkmale, in der Einordnung von Personen in statistische Gruppen und in der unterschiedslosen Behandlung aller Gruppenmitglieder. Diese jenseits des Datenschutzrechts bestehenden Prob-

Datensparsamkeit oder Datenreichtum?

Zunehmend schwierigere Vermeidung der Personenbeziehbarkeit

Neue technische Verfahren zum technischen Datenschutz in Theorie und Praxis

Big Data kann trotz technischer Vorkehrungen zu weiteren Problemen führen

leme sollen an dieser Stelle nicht vertieft werden. Sie liefern jedenfalls keinerlei Begründung dafür, etablierte Datenschutzprinzipien, wie das der Datensparsamkeit, für obsolet zu erklären.

An wen richtet sich die Forderung nach Datensparsamkeit?

Datensparsamkeit bedeutet nicht Datenaskese

Datensparsamkeit ist kein Selbstzweck. Daher richtet sich die Forderung nach Datensparsamkeit nicht gegen die betroffene Person. Das Prinzip fordert von ihr keine Datenaskese. Vielmehr will es ihre Selbstbestimmung über die Preisgabe der sie betreffenden Daten stärken. Wenn sie informiert, freiwillig und selbstbestimmt Daten von sich der Öffentlichkeit oder einzelnen Datenverarbeitern preisgibt, übt sie ihre Selbstbestimmung aus – also das, was auch das Prinzip der Datensparsamkeit gewährleisten will.

Datensparsamkeit wirkt vorbeugend

Die Forderung nach Datensparsamkeit richtet sich allein an den Datenverarbeiter als datenschutzrechtlich Verantwortlichen und an den Hersteller von Datenverarbeitungssystemen, diese so zu gestalten, dass sie möglichst wenig personenbezogene Daten benötigen, um ihre Funktion zu erfüllen. Dadurch wird zum einen das mit der Datenverarbeitung verbundene Risiko minimiert und zum anderen die Entscheidungsfreiheit der betroffenen Person gestärkt, in die Verarbeitung ihrer personenbezogenen Daten einzuwilligen und ihre Betroffenenrechte geltend zu machen. Das Prinzip der Datensparsamkeit soll insbesondere einer unbegrenzten Erhebung von Daten mit Personenbezug Einhalt zu gebieten. Es beugt Verletzungen der informationellen Selbstbestimmung und Formen algorithmischer Diskriminierung durch Datenverarbeiter vor.

Ist Datensparsamkeit rechtlich gefordert?

Datensparsamkeit verankert in der Datenschutz-Grundverordnung und

Die Datenschutz-Grundverordnung der Europäischen Union vom 27. April 2016, die am 25. Mai 2018 in allen Mitgliedstaaten unmittelbar gelten wird, enthält in Art. 5 sieben Prinzipien, die der Verarbeitung personenbezogener Daten zugrunde zu legen sind. Nach Art. 5 Abs. 1 lit. c) muss jede Datenverarbeitung das Prinzip der „Datenminimierung“ beachten, nach dem „personenbezogene Daten ... dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ müssen. Nach Art. 20 Abs. 1 der neuen Europäischen Richtlinie (EU) 2016/680 vom 27. April 2016 für den Datenschutz bei Polizei und Justiz, die am 6. Mai 2018 umgesetzt sein muss, gilt das Prinzip auch für die Verarbeitung personenbezogener Daten auch in Polizei und Justiz.

...in der JI-Richtlinie zum Datenschutz in Polizei und Justiz und

Aber nicht nur das Datenschutzrecht der Europäischen Union fordert eine Beschränkung der personenbezogenen Datenverarbeitung auf das notwendige Minimum, sondern auch das Verfassungsrecht der Union und der Bundesrepublik Deutschlands.

...in der EU-Grundrechtecharta

Art. 8 der Grundrechtecharta der Europäischen Union gewährleistet in Abs. 1 jeder Person „das Recht auf Schutz der sie betreffenden personenbezogenen Daten“. Nach Abs. 2 dürfen diese Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“. In dieses Grundrecht dürfen nach Art. 52 Abs. 1 Satz 2 Grundrechtecharta zur Wahrung des Grundsatzes der Verhältnismäßigkeit „Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen“. Die Anforderung der Notwendigkeit nimmt der Europäische Gerichtshof sehr ernst und prüft in mehreren Urteilen, ob die Verarbeitung personenbezogener Daten jeweils „absolut notwendig“ ist.

Aus den Grundrechten auf freie Entfaltung der Persönlichkeit nach Art. 2 Abs. 1 GG und auf Achtung der Menschenwürde nach Art. 1 Abs. 1 GG hat das Bundesverfassungsgericht in ständiger Rechtsprechung bis heute das Grundrecht auf informationelle Selbstbestimmung abgeleitet. Nach seinem Volkszählungsurteil setzt der Schutz der Persönlichkeit „voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten“. Wer (aber) „nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“. Unter den besonderen „Bedingungen der modernen Datenverarbeitung“ gewährleistet das Grundrecht auf informationelle Selbstbestimmung „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. Die informationelle Selbstbestimmung schützt die selbstbestimmte Entwicklung und Entfaltung der Persönlichkeit. Diese kann nur in einer für die betroffene Person kontrollierbaren Selbstdarstellung in unterschiedlichen sozialen Rollen und der Rückspiegelung durch die Kommunikation mit anderen gelingen. Dementsprechend muss die jeweils betroffene Person in der Lage sein, selbst zu entscheiden, welche Daten sie über sich in welcher Rolle und in welcher Kommunikation preisgibt. Diesen Vorrang erst ermöglicht informationelle Selbstbestimmung.

Nach dem Verfassungsrecht der Europäischen Union und der Bundesrepublik Deutschland ist jede fremdbestimmte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten daher ein Grundrechtseingriff. Deshalb wird Persönlichkeits- und Datenschutz am besten dadurch gewährleistet, dass bei der Verarbeitung personenbezogener Daten das Minimierungsprinzip zur Anwendung gelangt.

Kann das Prinzip der Datensparsamkeit abgeschafft werden?

Recht haben Politiker erlassen. Wenn es von der gesellschaftlichen Entwicklung überholt ist, können sie es auch abschaffen oder ändern. Dies geht nach dem Verfassungsrecht der Europäischen Union und der Bundesrepublik Deutschland je nach Regelungsinhalt unterschiedlich schwer und in ganz wenigen Fällen sogar gar nicht.

Um das Prinzip der Datensparsamkeit abzuschaffen, müsste in der Europäischen Union die Grundrechtecharta neu und in veränderter Form beschlossen werden. Dies wäre nur durch einstimmige Neufassung der Grundrechtecharta möglich. Diese könnte aber aus grundlegendsten rechtsstaatlichen Gründen nicht ohne die Berücksichtigung des Prinzips der Verhältnismäßigkeit beschlossen werden. Eingriffe in Grundrechte – auch in die Grundrechte auf Datenschutz nach Art. 8 GRCh und informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG – darf nur erfolgen, wenn sie verhältnismäßig sind. Jeder Eingriff muss einem Allgemeininteresse dienen, für das Erreichen dieses Ziels geeignet und erforderlich und für die betroffene Person angesichts der Bedeutung des verfolgten Ziels und der Tiefe des Eingriffs zumutbar sein. In Anwendung dieses Grundsatzes der Verhältnismäßigkeit hat der Europäische Gerichtshof abgeleitet, dass Eingriffe in das Grundrecht auf Datenschutz auf das „absolut Notwendige“ beschränkt sein müssen. Die Forderung, das Prinzip der Datensparsamkeit zu beseitigen, können die Politiker unionsrechtlich somit nur verwirklichen, wenn sie das Grundrecht auf Datenschutz abschaffen, so dass eine fremdbestimmte Datenverarbeitung kein Eingriff in ein Grundrecht mehr darstellt.

Um in Deutschland das Grundgesetz zu ändern, ist eine Verfassungsänderung mit einer Mehrheit von zwei Dritteln im Bundestag und im Bundesrat notwendig. Allerdings ist das Prinzip der Verhältnismäßigkeit, aus dem das Bundesverfassungsgericht das Gebot der Datensparsamkeit ableitet, als Bestandteil des Grundrechts auf Menschenwürde in

Datensparsamkeit oder Datenreichtum?

... sowie im Verfassungsrecht der Bundesrepublik Deutschland

Abschaffung der Datensparsamkeit sehr schwierig

Das Prinzip der Datensparsamkeit leitet sich aus dem Grundrecht auf Menschenwürde ab ...

Datensparsamkeit oder
Datenreichtum?

**... was ihre Abschaffung im
Rahmen einer Verfassungsän-
derung ausschließt**

Art. 1 Abs. 1 GG und des Rechtsstaatsgebots in Art. 20 Abs. 1 GG anzusehen. Es ist daher Teil des „änderungsfesten Minimums“, das Art. 79 Abs. 3 GG von jeder Verfassungsänderung ausschließt. Eine Aufgabe des Prinzips der Verhältnismäßigkeit ist daher in Deutschland verfassungsrechtlich ausgeschlossen. Aus dem gleichen Grund dürfte die Bundesrepublik Deutschland auch einer Grundrechtecharta nicht zustimmen, in der das Grundrecht auf Datenschutz und der Grundsatz der Verhältnismäßigkeit fehlten. Die Bundesregierung darf nicht gegen die Verfassungsidentität der Bundesrepublik verstoßen, zu der nach dem Urteil zur Vorratsdatenspeicherung des Bundesverfassungsgerichts Datenschutz und Verhältnismäßigkeit gehören.

Was bedeutet Datensparsamkeit für Big Data?

Wie nachteilig ist Datensparsamkeit für die Verarbeitung großer Mengen von Daten? Verhindert sie, sich daran zu beteiligen, „die Vielzahl an Daten zu nutzen, sei es in der Medizin, sei es in der Zukunft der Mobilität, sei es in Angeboten der Plattform-Wirtschaft“? Gefährdet sie tatsächlich „die Arbeitsplätze der Zukunft“ (Merkel 6.12.2016)?

**Datenverarbeitung ohne Per-
sonenbezug möglich**

Keine Beschränkung der Datenverarbeitung ist zu erkennen, soweit Daten verarbeitet werden, die nicht personenbezogen sind. Smart Data, die aus Unternehmen oder Behörden, die aus Maschinen oder Infrastrukturen stammen, die naturwissenschaftliche Phänomene abbilden, die meteorologische oder geographische Zusammenhänge erfassen oder die sonstige – nicht einer bestimmten natürlichen Person zugeordnete – Angaben enthalten, können ohne Probleme mit dem Prinzip der Datensparsamkeit verarbeitet werden. Dies gilt sogar für – ansonsten sehr sensitive – medizinische oder epidemiologische Daten über Krankheitsursachen, -verläufe oder -behandlungen. Dies betrifft auch Beobachtungen des Verkehrsgeschehens und der gesellschaftlichen Mobilität.

**Technische Vermeidung des
Personenbezugs**

Keine Probleme stellen aber auch personenbezogene Daten dar, die vor ihrer weiteren Verarbeitung aggregiert, anonymisiert oder pseudonymisiert worden sind, soweit sie einen effektiven Schutz gegen die Herstellung des Personenbezugs durch Dritte bieten. Sie ermöglichen medizinische Erkenntnisse, detaillierte Einblicke in die Zukunft der Mobilität und in wirtschaftliche Trends sowie die Prognose von Verhalten, Einstellungen und Präferenzen von Betroffenenengruppen.

**Datensparsamkeit schützt vor
nachteiliger Datenverarbei-
tung**

Ein Widerspruch zum Gebot der Datensparsamkeit kann nur dann entstehen, wenn personenbezogene Daten erhoben, gesammelt und bezogen auf eine ganz bestimmte Person ausgewertet werden. Dies ist vor allem der Fall, wenn die Daten für

- das Tracking des Verhaltens von Personen genutzt werden, um auf der Zeitachse etwa die Aufenthaltsorte oder das Kommunikations- oder Surfverhalten einer Person zu ermitteln,
- das Scoring einer individuellen Person ausgewertet werden, um auf der Grundlage vieler Merkmale eine bestimmte Eigenschaft dieser Person zahlenmäßig zu bewerten,
- das Personalizing eingesetzt werden, um bezogen auf eine Person möglichst viele Merkmale zur Beantwortung unterschiedliche Fragestellungen zu dieser Person (z. B. Interesse an bestimmter Werbung, Erbringen eine individuellen Dienstleistung) beantworten zu können, oder für
- das Profiling verwendet werden, um viele Eigenschaften einer Person langfristig und sektorübergreifend zu einem (umfassenden) Persönlichkeitsbild zusammenzuführen und immer wieder für eigene oder fremde Zwecke auszuwerten.

Alle diese Auswertungen erfolgen im Regelfall, um das Verhalten der Person vorherzusagen und beeinflussen zu können. Da die Daten personenbezogen ausgewertet werden, greift diese Datenverarbeitung in die Grundrechte der jeweils betroffenen Person ein.

Diese vielfältigen Grundrechtseingriffe können u. a. nur dann zulässig sein, wenn sie auf das erforderliche Minimum an Daten beschränkt wurden.

Zusammenfassend ist also festzustellen, dass in sehr vielen Fällen der Verarbeitungen großer Mengen an Daten kein Konflikt mit dem Prinzip der Datensparsamkeit entsteht. Soweit Daten ausgewertet werden, die nie personenbezogen waren oder deren Personenbezug effektiv beseitigt worden ist, kann die Verarbeitung großer Datenmengen problemlos zum Fortschritt der Gesellschaft beitragen. Ein Konflikt mit dem Prinzip der Datensparsamkeit kann also im Wesentlichen nur eintreten, wenn die Verantwortlichen bestimmte Geschäftsmodelle oder Zwecke verfolgen, die eine Verhaltensbeobachtung oder -beeinflussung der betroffenen Personen zum Ziel haben.

Chancen von Datensparsamkeit

Als Gegenstrategie zur anlasslosen und massenhaften Datenanhäufung wirkt sich das Prinzip der Datensparsamkeit positiv auf die Einhaltung der Compliance-Pflichten der Verantwortlichen aus. Sie können Datenleaks und Datenmissbräuche durch Datensparsamkeit zwar nicht völlig vermeiden, gleichwohl fallen bei der Einhaltung des Prinzips die Folgen möglicher Angriffe deutlich geringer aus und das Gesamtrisiko sinkt.

Empirische Untersuchungen zeigen, dass die Nutzenden ein höheres Vertrauen in einen Dienst haben, wenn diese lediglich Daten erheben, die erkennbar zur Erbringung des Dienstes benötigt werden. Wenn die Nutzenden den Eindruck haben, dass Dienstleister übermäßig viele Daten erheben, so erhöht dies auch die Wahrscheinlichkeit von Widerstandsmaßnahmen wie der Angabe von falschen Daten. Dagegen kann Datensparsamkeit, die für Nutzende auch als solche erkennbar ist, ihr Verhalten in der Online-Kommunikation in positiver Form beeinflussen: Mit dem Wissen, dass ihre Nachrichten oder Beiträge nicht mit ihrer Person in Verbindung gebracht werden, dürften Nutzende eher bereit sein, z. B. an Online-Diskursen im Rahmen politischer oder gesellschaftlicher Debatten teilzunehmen. Damit wäre eine stärkere Inklusion der Bürgerinnen und Bürger in der Online-Kommunikation möglich.

Datensparsamkeit kann auch das Entstehen datenbasierter, langfristiger Monopole behindern. Unternehmen wie Google, die eine umfassende Datenbasis aufgebaut haben, profitieren davon, dass sie werbetreibenden Dritten sehr exakte Nutzerprofile anbieten und somit sehr zielgruppenspezifische Werbung nutzbar machen können. Dies könnte zu einem selbstverstärkenden Trend führen, durch den bereits erfolgreiche, datensensitive Unternehmen immer erfolgreicher werden und somit ihre Datenbasis stetig steigern können. Im Extremfall kann es dadurch zu Monopolbildungen kommen, was letztlich sowohl zu ökonomischen Schäden auf Seiten der Verbraucher als auch zu Einbußen auf Seiten heimischer Unternehmen führen kann.

Negative Effekte hat die Forderung nach Datensparsamkeit für die Unternehmen, deren Geschäftsmodell darauf basiert, jenseits der Erfüllung ihrer vertraglichen Pflichten personenbezogene Daten zu sammeln und auszuwerten, um das Verhalten von Personen vorherzusagen und beeinflussen zu können. Entscheidend ist, ob für diese Unternehmen unterschiedliche Wettbewerbsbedingungen dadurch bestehen, dass divergierende Datenschutzregelungen gelten. Soweit die Forderungen nach Datensparsamkeit entsprechend dem Marktortprinzip des Art. 3 Abs. 2 Datenschutz-Grundverordnung auch für Unternehmen gelten, die zwar nicht in der Europäischen Union und im Europäischen Wirtschaftsraum angesiedelt sind, aber Daten von betroffenen Personen aus diesem Raum sammeln, führt dies zu gleichen Wettbewerbsbedingungen zwischen europäischen und außereuropäischen Unternehmen. Substantielle Sanktionen von bis zu vier Prozent des Jahresumsatzes sind auch für außereuropäische Unternehmen geeignete Anreize, gesetzeskonform zu handeln.

Datensparsamkeit kann ...

**... unterstützen bei der
Einhaltung von Compliance-
Pflichten**

**... das Vertrauen von Nutze-
rinnen und Nutzern in Produk-
te erhöhen**

**... die Entstehung von Mono-
polen behindern**

**... wettbewerbsfördernd für
europäische Anbieter wirken**

Sind Datensparsamkeit und massenhafte Verarbeitung personenbezogener Daten zu vereinbaren?

Vermeidung des Personenbe- zugs von Daten als zentrales Ziel durch ...

Da Datensparsamkeit nicht die Daten, sondern nur den Personenbezug betrifft, besteht der wichtigste Ansatz, diese Daten ohne Verstoß gegen den Grundsatz der Datensparsamkeit zu verarbeiten darin, dass der Personenbezug beseitigt wird. Dies kann durch geeignete Maßnahmen in unterschiedlichen Stufen des Daten-Lebenszyklus erfolgen.

Soll der Personenbezug bereits bei der Erhebung der Daten beseitigt werden, so müssen entsprechende Schnittstellen, beispielsweise für sog. „Privacy-Enhancing Attribute-Based Credential“, anonyme Netze wie das TOR-Netzwerk und verteilte Datenanonymisierungs- und Datenverschlüsselung-Frameworks auf Nutzerseite realisiert werden.

... technische Maßnahmen

Will der Verantwortliche bereits erhobene Daten für andere Zwecke nutzen oder Dritten (externe Dienstleistern, Forschern, ...) zugänglich machen, kann er beim Umgang mit homogenen Daten aus traditionellen Datenbanksystemen Methoden und Algorithmen zur Datenanonymisierung nutzen. Diese stoßen allerdings in Big-Data-Szenarien wegen der Anforderungen an Performanz und Skalierbarkeit an ihre Grenzen. Alternative Ansätze wie „Secure Multiparty Computation“ und (volle) homomorphe Verschlüsselung, die verteilte Berechnungen auf geheim gehaltenen oder verschlüsselten Daten erlauben, sind heute noch weit von einem praktischen Einsatz entfernt.

... Selbstdatenschutzmaßnah- men

Eine Reaktion des Selbstdatenschutzes könnte auch darin bestehen, genau das Gegenteil von Datensparsamkeit zu praktizieren, nämlich möglichst viele vermeintlich personenbezogene Daten zu generieren. Dieses als „Obfuscation“ bezeichnete Konzept sieht vor, dass der faktische Personenbezug, die Identifizierbarkeit und Überwachbarkeit von Personen dadurch verloren geht, dass Anwendungen wie CacheCloak, TrackMeNot, AdNauseam, Vortex und andere möglichst viel „Datenrauschen“ durch zusätzliche, über das tatsächliche Such- und Surfverhalten hinausgehende, maschinengenerierte Anfragen im Hintergrund erzeugen. Dieses „Datenrauschen“ soll datenverarbeitende Unternehmen und staatliche Stellen daran zu hindern, die richtigen Daten herauszufiltern. Dadurch soll der Anreize sinken, erhobene Daten zu missbrauchen.

...Entwicklung innovativer Geschäftsmodelle

Ein weiterer Ansatz besteht darin, Geschäftsmodelle als Nutzende oder als Gesellschaft nicht zu akzeptieren, die über den von den Nutzenden gewollten Zweck hinausgehen und auf der Auswertung von Personenprofilen (z. B. zu Werbezwecken) beruhen. Dies ist auch angelegt in der Regelung zu datenschutzfreundlichen Voreinstellungen im Art. 25 der Datenschutz-Grundverordnung, in der die Erforderlichkeit für den jeweiligen Zweck in den Vordergrund gestellt wird. Dann müssten die Leistungen, die im Rahmen solcher Geschäftsmodelle erbracht werden, auf andere Weise als durch personenbezogene Werbung finanziert werden. Dies würde dazu führen, dass die Nutzenden für die ihnen zur Verfügung gestellten Dienste Geld zu bezahlen müssten – wie Entgelte für zuverlässige Leistungserbringung auch in vielen anderen Lebensbereichen üblich sind.

Bisher jedoch ist die Zahlungsbereitschaft der Konsumenten dafür, dass Anbieter auf die Verwendung von personenbezogenen Daten verzichten und ihre Dienste gegen Entgelt anbieten, gering. Der Grund liegt sicherlich darin, dass Nutzer einerseits die mit der Datenweitergabe verbundenen Risiken unterschätzen, andererseits den Nutzen ihrer Daten für Dritte nur schwer abschätzen können. Dies führt tendenziell zu einer „Unterschätzung“ des Werts der eigenen Daten. Ausnahmen finden sich bisher nur bei speziellen Diensten: Eine solche Ausnahme ist zu erwarten, wenn es um spezielle Dienste geht, die gezielt bestimmte Sicherheitsmerkmale anbieten und bewerben oder die sich auf bestimmte Berufe mit besonderen Vertrauensanforderungen beziehen.

Neuen Überlegungen, Nutzern sog. „Datentresore“ anzubieten, wo jeder seine Daten speichern und selbst darüber entscheiden kann, wem er diese preisgibt, stoßen auf Bedenken, weil sich hier wieder ein Monopol bilden könnte. Dem müsste durch wettbewerbssichernde Maßnahmen vorgebeugt werden.

Behindert Datensparsamkeit Innovationen?

Solange die Verantwortlichen Zwecke verfolgen, die keine personenbezogenen Daten benötigen, verhindert das Prinzip der Datensparsamkeit Innovationen in keiner Weise. Verfolgen sie jedoch Zwecke, die auf die individuelle Zuordnung der großen Datenmengen ausgerichtet sind, müssen sie berücksichtigen, dass sie dadurch in das Grundrecht auf Datenschutz der betroffenen Personen eingreifen.

Das heißt jedoch nicht, dass dadurch Innovationen unmöglich sind. Soweit die individualisierende Datenverarbeitung dem Willen der betroffenen Person entspricht, etwa, weil sie einen personalisierten Dienst in Anspruch nehmen will, z. B. speziell auf sie zugeschnittene Lernkurse, rechtfertigt dies die Datenverarbeitung. Vergleichbares gilt, wenn der Gesetzgeber anerkannt hat, dass die Datenverarbeitung im überwiegenden öffentlichen oder individuellen Interesse, etwa zum Zweck spezifischer medizinischer Forschung, erfolgt. Dann kann eine Auswertung der für diese innovativen Zwecke erforderlichen Daten erfolgen. In diesen Fällen werden die für die Innovationen gebotene Datenverarbeitung und das Prinzip der Datensparsamkeit aufeinander abgestimmt.

Hier ist nicht der Ort, weiterführende Diskussionen um das als ineffektiv kritisierte Einwilligungsprinzip oder um konturlose Abwägungsregeln zu führen. Allerdings finden sich auch darin keine Argumente für den Abbau rechtlich verankerter Datenschutzprinzipien. Sie führen in der Praxis jedenfalls nicht zu Innovationshemmnissen, sondern ermöglichen diese auch angesichts des Grundsatzes der Datensparsamkeit.

Innovationen können auch in einer Form erfolgen, die die Grundrechte der betroffenen Personen respektieren. In vielen Bereichen kann auch die datensparsame Systemgestaltung innovativ und wirtschaftlich erfolgreich sein. So hat die Durchsetzung datenschutzrechtlicher Anforderungen beim Cloud Computing gezeigt, dass datenschutzfreundliche Innovationen in Europa erfolgreich sein können. Weitere Beispiele sind die Selbstverpflichtungen zahlreicher deutscher Automobilhersteller und Zulieferer als Mitglieder des Verbands der Automobilindustrie 2016, für vernetzte Fahrzeuge wichtige Datenschutzprinzipien – zwei davon mit Bezug zu Datensparsamkeit – einzuhalten. Einen ähnlichen Ansatz verfolgt das Unternehmen Apple, das datensparsamkeitsfördernde Maßnahmen auf der Grundlage von Differential Privacy (DP) für die Erhebung und Analyse von Kundendaten einsetzt. Dies zeigt: Für den Erfolg von datenschutzfreundlichen Innovationen sind vor allem die politischen Rahmenbedingungen entscheidend. Aber zudem ist auch der politische Wille notwendig, geltendes Recht gegenüber allen, also auch außereuropäischen Anbietern, gleichermaßen durchzusetzen.

Die Vorstellungen, die dem Ruf, den Grundsatz der Datensparsamkeit abzuschaffen, zugrunde liegen, könnten zu einem „Race to the Bottom“ führen. Die Umsetzung dieser Forderung würde einen Wettbewerb zwischen Staaten fördern, einander bei ihren Datenschutzstandards zu unterbieten, um mehr Unternehmen anzulocken, die von weniger restriktiven Datenschutzstandards profitieren. Dahinter steht die Hoffnung, dass die gelockerten Datenschutzstandards zu mehr Wachstum und Arbeitsplätzen im eigenen Land beitragen. Damit verbunden wäre jedoch ein erhebliches Risiko für die Rechte und Freiheiten der betroffenen Personen.

Ebenso denkbar wäre auch ein „Race to the Top“, also eine Angleichung der Datenschutzstandards nach oben. Hierzu bieten der Daten- und der Umweltschutz durchaus viele Beispiele. So hat die Datenschutz-Richtlinie bewirkt, dass andere Staaten ihre Datenschutzstandards an die in der Europäischen Union angeglichen haben. In den USA hat die Vorreiterrolle Kaliforniens bei hohen Umweltstandards dazu geführt, dass USA-weit höhere Standards implementiert wurden. Entscheidend war hierfür sicherlich der große wirtschaftliche Einfluss Kaliforniens innerhalb der USA. Aber auch Deutschland könnte seinen Einfluss nutzen und höhere Datenschutzstandards zunächst innerhalb der Europäischen Union durchsetzen und auch auf dem internationalen Parkett, etwa im Rahmen der Vereinten Nationen und des Europarats, stärker für deren globale oder regionale Verbreitung eintreten.

Datensparsamkeit oder
Datenreichtum?

Datenverarbeitung trotz Personenbezug bei Einwilligung oder gesetzlicher Erlaubnis möglich

Cloud Computing und Automobilindustrie demonstrieren die Vereinbarkeit des Prinzips der Datensparsamkeit mit Innovationen

Statt „Race to the Bottom“ ...

„Race to the Top“



GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

PROJEKTPARTNER



Natur **U N I K A S S E L**
Technik
Kultur **V E R S I T Ä T**
Gesellschaft

provet

Projektgruppe verfassungsverträgliche Technikgestaltung

**UNIVERSITÄT
DUISBURG
ESSEN**

Offen im Denken

EBERHARD KARLS
**UNIVERSITÄT
TÜBINGEN**



INTERNATIONALES ZENTRUM
FÜR ETHIK IN
DEN WISSENSCHAFTEN

LMU

LUDWIG-
MAXIMILIANS-
UNIVERSITÄT
MÜNCHEN

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein