Datensouveränität

Datensouveränität ist als Teilbereich von Digitaler Souveränität ein unscharfer Diskursbegriff und wird verwendet, um verschiedene Aspekte der individuellen oder gesellschaftlichen Befähigung zum selbstbestimmten Umgang mit Big Data zum Ausdruck zu bringen. Grundannahme ist dabei, dass aktuelle rechtliche Regelungen, politische Agenden und individuelle Kompetenzen nicht ausreichend an die neuen Bedingungen der Massendatenverarbeitung angepasst sind. Der Datensouveränitätsbegriff wird von verschiedenen Akteuren unterschiedlich geprägt. Da er anders als „informationelle Selbstbestimmung“ stärker die Ermöglichung von Datenerhebung und Datenverarbeitung betont, wird er von manchen Datenschützern auch als „Lobbybegriff“ bezeichnet. Die in dem Zusammenhang mit Datensouveränität diskutierten Probleme gehen jedoch deutlich über die Verfügbarmachung von Daten hinaus. Der Diskurs ist uneinheitlich und verzweigt, außerdem ergeben sich zahlreiche Überschneidungen mit anderen Themen wie rechtlicher Rahmen und Datensicherheit.

ZENTRALE THEMENBEREICHE

Recht und Datenschutz

Rechtliche Fragen bilden den kontroversesten Aspekt der Debatten um Datensouveränität. Hier beschreibt Datensouveränität häufig den Ansatz, Daten aufgrund der wertvollen Erkenntnisse, die sich aus ihnen gewinnen lassen, weniger als individuelles Eigentum, sondern als kollektives Gut zu betrachten. Daraus würde auch folgen, die Widersprüche zwischen den Grundsätzen des aktuellen Datenschutzes (Datensparsamkeit, Einwilligungserfordernis und Zweckbindung) und den Anforderungen von Massendatenanalysen (Datenreichtum, automatischer Musterkennung ohne vorentworfenes Ziel und Rekontextualisierung) zugunsten letzterer aufzulösen. Nutzer von Digitaltechnologien sollten aber auch unter Big-Data-freundlichen Bedingungen in der Lage sein, informiert und selbstbestimmt zu entscheiden, was mit ihren Daten geschieht. Dazu müsste nicht nur Transparenz in den Prozessen etabliert, sondern auch Einschränkungs- und Wahlmöglichkeiten im Verlauf des Datenanalyseprozesses ermöglicht werden. Datenschützer befürchten jedoch den Verlust der im Datenschutzrecht verankerten informationellen Selbstbestimmung.

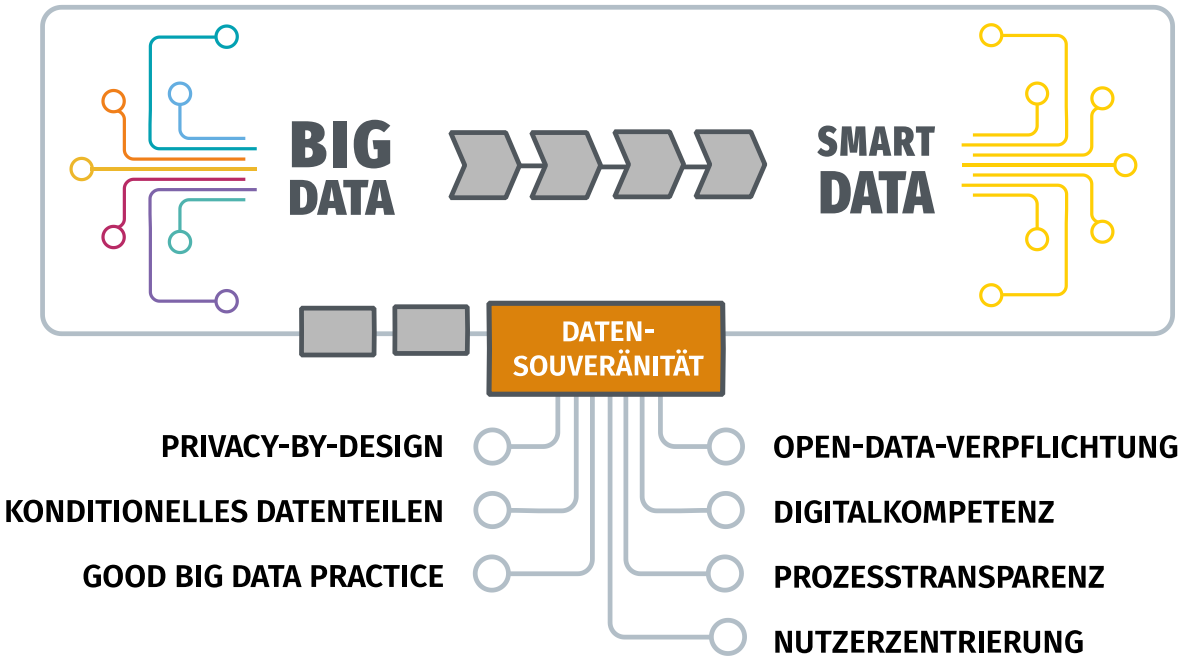
Politische Strategie

Im politischen Diskurs wird der Begriff der Datensouveränität verwendet, um den angestrebten Zustand der Unabhängigkeit von ausländischen Datenverarbeitungsunternehmen zu bezeichnen. Eng damit verbunden ist das Ziel, bei der Entwicklung von Künstlicher Intelligenz und der Stärkung der Datenwirtschaft eine internationale Führungsposition zu erlangen. Dazu strebt die Bundesregierung die Förderung von Forschung und Innovation, beispielsweise im Rahmen einer nationalen KI-Strategie, aber auch um den Ausbau der digitalen Infrastruktur als deren Grundbedingung zu setzen, an. Deutsche Datenverarbeitungsunternehmen und Forschungseinrichtungen hoffen auf den Abbau regulatorischer Hürden für die Sammlung und Auswertung von Daten und benötigen technisch wie auch rechtlich sichere Repositorien, Austausch- und Verarbeitungsplattformen für qualitativ hochwertige Datensets.

Digitalkompetenz

Zu überblicken, welche Daten während der Interaktion mit Digitaltechnologien übermittelt werden und wie die Prozesse zur Verwertung dieser Daten eigentlich funktionieren, ist nur wenigen Spezialisten möglich. Es gibt nicht genug spezialisierter Fachkräfte, um den Ambitionen einer deutschen Datenwirtschaft mit Spitzenniveau gerecht zu werden. Zusätzlich müssen auch auf der Anwendungsebene die Nutzer Datenverarbeitungsmechanismen verstehen, um informiert entscheiden zu können, welcher Datennutzung sie zustimmen. Digitale Technologien überfordern Teile der Bevölkerung oder bleiben ihnen aufgrund zu hoher Komplexität und eingeschränkter Bedienbarkeit gänzlich unzugänglich. Um Datensouveränität im Sinne von Kenntnissen und praktischer Befähigung – als Digitalkompetenz – zu erreichen, muss der Vorsprung bei der Big-Data-Entwicklung aufgeholt werden: dies nicht nur in den Bereichen Bildung, Inklusion und Usability sondern auch im Sinne einer gesellschaftlichen Reflexion.

Wir stellen die aktuellen Herausforderungen und Trends des Themenschwerpunkts sowie die wichtigsten Institutionen und Initiativen vor. Unsere Zusammenstellung weiterführender Informationen soll einen tieferen Einstieg in das Thema erleichtern.



© Smart Data Forum

Herausforderungen

- **Anpassung des rechtlichen Rahmens**: Die gesetzlichen Vorgaben zu Datenerhebung und -verarbeitung müssen so angepasst werden, dass sie die Interessen von Datengebern auch unter Bedingungen von Big Data wahren, aber gleichzeitig nicht innovationshemmend wirken. Die Durchsetzung von Ansprüchen aus dem europäischen Datenschutzrecht im Ausland ist ein weiteres zentrales Problem, denn viele der von Europäern generierten Daten werden in den USA oder China verarbeitet. Auch an der rechtlichen Durchsetzbarkeit des Konzeptes von Dateneigentum bestehen Zweifel.

- **Monopolstellung großer Plattformen**: Für viele Nutzer bestehen bei der Auswahl von datengetriebenen Alltagstechnologien kaum Alternativen, da wenige Unternehmen den Markt beherrschen. Die Markthoheit dieser Unternehmen verschafft ihnen eine umfassende Datenbasis zur Entwicklung neuer Angebote, die es anderen Projekten nahezu unmöglich macht, mit ihnen zu konkurrieren.
- **Datenteilen**: Die Bereitschaft von Unternehmen, untereinander Daten zu teilen ist gering. Das ist ein Hemmnis für die Entwicklung neuer Geschäftsmodelle, insbesondere auch für die Einführung von Industrie-4.0-Lösungen und somit hinderlich für die internationale Wettbewerbsfähigkeit der deutschen Wirtschaft. Um die Datenbasis für die Wirtschaft und auch die Forschung zu stärken, wäre es nötig auch für Bürger Anreize zum freiwilligen Datenteilen zu schaffen.
- **Transparenz der Prozesse**: Die Transparenz der Prozesse in der Datenwertschöpfungskette ist für Nutzer und Entwickler wichtig, um angemessen mit ihnen umgehen zu können. Open-Source und Open-Data als bestimmende Prinzipien von Wissenschaft und Datenwirtschaft könnten die Möglichkeiten zur Kontrolle und Mitwirkung gleichermaßen verbessern.
- **Digitalkompetenz:** Die Bürger müssen befähigt werden, neue Digitaltechnologien mündig und in ihrem Interesse zu verwenden sowie Risiken einschätzen und vermeiden zu können. Dazu sind Änderungen im Bildungssystem, gezielte Angebote zur Sensibilisierung für Datenschutzfragen, aber auch die Stärkung von Inklusion durch und in IT-Lösungen nötig.
- **Fachkräftemangel:** Derzeit besteht ein Missverhältnis zwischen der Zahl an IT-Fachkräften in Deutschland und dem Wachstum von Forschungs- und Geschäftsaktivitäten in diesem Bereich. Dies hemmt die weitere Entwicklung.

Trends und Gestaltungsvorschläge

- **Daten- und Wissensinfrastruktur**: Anschub für eine europäische Datensouveränität kann eine nachhaltig und öffentlich betriebene Dateninfrastruktur sein. Diese sollte im Gegensatz zu den Angeboten große Plattformen im Ausland weniger auf der Auswertung und Vermarktung von Konsumdaten basieren, sondern vielmehr breitere, gesellschafts- und wirtschaftsrelevante Domänen in den Fokus stellen. Sie sollte außerdem den Zugang zu großen, qualitativ hochwertigen Datenmengen und deren Analyse und Visualisierung für Unternehmen, Universitäten, Forschungseinrichtungen, Schulen und Bürger ermöglichen und demokratisieren.
- **Nationale KI-Strategie**: Die Bundesregierung hat bereits ihre KI-Strategie veröffentlicht, welche die Entwicklung hin zu einer Spitzenposition deutscher KI-Entwicklung im internationalen Vergleich fördern soll. Zu den geplanten Maßnahmen gehören der Ausbau der digitalen Infrastruktur, die IT-Ausrichtung in Bildung und Forschung, IT-Sicherheit und Vernetzung der Forschung auf europäischer Ebene.
- **Verbindliche Good Big Data Practice**: Rechtliche und technische Ansätze können ein komplexes und disziplinübergreifendes Thema wie Big Data nur schwer fassen und werden daher nur langsam implementiert. Ergänzend sollten deswegen für Datennutzer verbindliche technische und ethische Richtlinien im Sinne einer Good Big Data Practice entwickelt und umgesetzt werden. Denkbar wäre zum Beispiel eine Zertifizierung bei einer vorbildlichen Umsetzung des Datenschutzes.

- **Open-Data-Verpflichtung**: Open-Source und Open-Data schaffen aufgrund ihrer Transparenz eine wichtige Voraussetzung für die informationelle Selbstbestimmung und bieten daher Anreize für das Teilen von Daten und unterstützen die wissenschaftliche Entwicklung. Darum ist bei öffentlichkeitsrelevanten Daten zu überlegen, ob die Unternehmen, die diese im großen Stil Daten sammeln, dazu verpflichtet werden, die Informationen und Daten in frei zugänglichen Repositorien abzulegen.
- **Nutzerzentrierung**: Angebote, welche Interessen der Nutzer in den Mittelpunkt stellen und ihnen neben der Sicherheit ihrer Daten auch direkte Anreize bieten, könnten die Bereitschaft zum Datenteilen für nichtkommerzielle Projekte stärken. Solche Anreize könnten beispielsweise Informationen, verbesserte Dienstleistungen oder die Aussicht sein, mit der Überlassung der eigenen Daten positive soziale Effekte zu ermöglichen.
- **Datenspenderausweis**: Ein Beispiel für nutzerzentrierte Angebote ist die Gesundheitscloud, in der Personen ähnlich einem Organspenderausweis einen selbstgewählten Teil ihrer Gesundheitsdaten freiwillig in einer sicheren Cloud Ärzten oder Forschern zur Verfügung stellen. Damit verbessern sie die Datenbasis der behandelnden Ärzte und tragen so zur Entwicklung neuer Behandlungsformen bei.
- **Privacy-by-Design:** Die umfassende Implementierung von Datenschutzstandards wie Ende-zu-Ende-Verschlüsselung, Nutzer-Authentifizierung und Trennung von Identifizierungsmerkmalen und Inhaltsdaten sollten Datenschutzvorgaben technisch schon in der Datenverarbeitungsprozess integrieren und die Vertrauensbasis für Datenverarbeitung stärken.
- **Konditionelles Datenteilen**: Die Daten bleiben im Besitz der Eigentümer und werden nur bei Bedarf und unter bestimmten Konditionen sicher ausgetauscht.
- **Dezentrale Datentreuhandfunktionen durch Blockchain**: Die zentrale Datenverwaltung durch lokale und unabhängige Treuhänder ist bereits häufig implementiert, die dezentrale Datenverwaltung durch Blockchain-Technologien könnte solche Transaktionen noch unabhängiger und effizienter ausführen.

Institutionen und Initiativen (Auswahl)

- International Data Spaces Association – Ein virtueller Datenraum für den sicheren und datenschutzgerechten Datenaustausch zwischen verschiedenen Teilnehmern. Als „Network of Trusted Data“ ist Industrial Data Spaces ein Modell für eine Infrastruktur mit Privacy-by-Design-Ansatz für den souveränen Austausch von Daten. (BMBF)
- Weizenbaum Institut – Die Aufgabe des Weizenbaum-Instituts für die vernetzte Gesellschaft ist es, aktuelle gesellschaftliche Veränderungen, die sich im Zusammenhang mit der Digitalisierung abzeichnen, zu untersuchen und künftige politische und wirtschaftliche Handlungsoptionen zu skizzieren. Im Forschungsbereich „Wissen, Bildung und soziale Ungleichheit“ recherchiert die Gruppe zu digitaler Souveränität und individuellem Umgang mit digitalen Technologien.
- Humboldt Institut für Internet und Gesellschaft (HIIG) – HIIG erforscht die Entwicklung des Internets aus einer gesellschaftlichen Perspektive. Ziel ist es, die damit einhergehende Digitalisierung aller Lebensbereiche besser zu verstehen. Das

Konzept „Datensouveränität“ wird im Forschungsprogramm „Governance datengetriebener Innovation und Cybersicherheit“ untersucht.

- Digital Society Institute (DSI) – Dieses Institut fördert den Dialog zwischen Gesellschaft, Politik und Wirtschaft zu Digitalisierungsthemen auf der Grundlage wissenschaftlicher Erkenntnisse. Darüber hinaus arbeitet es an der Entwicklung disruptiver Cybertechnologien. In Fokusseminaren versucht das Institut Themen wie Datensouveränität zu analysieren.

Weiterführende Informationen und Publikationen

Datensouveränität

- Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung – Deutscher Ethikrat, 2018
- Datensouveränität im Internet der Dinge – Der Trusted Connector im Industrial Data Space – Industrial Data Spaces, 2018
- Datensouveränität in der digitalen Wirtschaft – Fraunhofer ISST, 2017
- „Eigentumsordnung“ für Mobilitätsdaten? – BMVI, 2017
- Die Datensicherheit stärken und Datensouveränität entwickeln – BMWi, 2016

Digitale Souveränität

- Die Stärkung der digitalen Souveränität – iRights.Lab, Deutsches Institut für Vertrauen und Sicherheit im Internet, 2018
- Digitale Souveränität: Bürger | Unternehmen | Staat – IIT, 2017
- Datensouveränität – Kompetenzzentrum Öffentliche IT, 2017
- Kompetenzen für eine digitale Souveränität – FZI, 2017
- Digitale Souveränität – Sachverständigenrat für Verbraucherfragen, 2017