Nothing personal? Der Personenbezug von Daten in der DSGVO im Licht von künstlicher Intelligenz und Big Data

Rita Jordan

Zusammenfassung

Mit dem Einsatz selbstlernender Algorithmen steigt auch der Umfang, die Rate und die Geschwindigkeit, mit der Daten erfasst, verarbeitet und ausgewertet werden. Dadurch geraten die Zwecke des Datenschutzrechts (Persönlichkeitsschutz, informationelle und demokratische Selbstbestimmung) und seine Schutzprinzipien (u.a. Zweckbindung, Datenminimierung und Transparenz) in Spannung zu den Gewinninteressen datenbasierter Geschäftsmodelle und dem herrschenden Innovationsdruck. Die technischen Möglichkeiten von Big Data unterwandern die eindeutige Abgrenzbarkeit zwischen personenbezogenen und nicht personenbezogenen Daten, die zentral für das dogmatische Fundament der Europäischen Datenschutzgrundverordnung (DSGVO) ist. Durch immer kleinteiligere Datenschutzerklärungen und die technischen Barrieren einer informierten Einwilligung wird individuellen Nutzer:innen eine aufgeklärte Rechtsausübung erschwert. Einen zentralen Bereich der Digitalisierung, in dem dieses Spannungsfeld sich manifestiert, bieten Smart Cities. Hier verschränkt sich die Innovationskraft algorithmischer Datenverarbeitung für Nachhaltigkeits- und Verkehrsziele mit der physischen Oberfläche urbaner Erfahrungs- und Handlungsräume. Die Ubiquität der erfassten Daten und die damit einhergehenden Risiken für Privatheit legen eine grundlegende Rekonzeptualisierung des Datenschutzrechts sowie eine Demokratisierung der Technologieentwicklung – insbesondere im Bereich KI-basierter Technologien – in städtischen Räumen nahe.

1. Einleitung

Der Beitrag unterstreicht einen kritischen juristischen Blick auf die geltende datenschutzrechtliche Personenbezugsdogmatik anhand eines Beispielszenarios über die Entwicklung intelligent vernetzter Verkehrsinfrastrukturen. Dieses Beispiel leitet hin zu einer politikwissenschaftlich informierten Auseinandersetzung mit dem Bedarf und den Potentialen einer

partizipativen Technologieentwicklung hinsichtlich des Ziels einer demokratischen Einbettung der Digitalisierung in städtische Infrastrukturen.[1] Zunächst wird das geltende, stark auf individuelle Datensubjekte ausgerichtete EU-Datenschutzrecht knapp vorgestellt (2.). Anschließend wird diese Zentrierung auf das Individuum aus rechts- und sozialwissenschaftlichen Perspektiven kritisch beleuchtet (3.). Die Kritik wird daraufhin am Anwendungsbeispiel der intelligent vernetzten Infrastruktur von *Smart Cities* illustriert, um den Bedarf einer demokratischen, über individuenzentrierte Datenschutzmodelle hinausgehenden Technologieentwicklung hervorzuheben (4.). Dadurch verlagert sich der Fokus des Textes vom Thema der regulatorischen Gestaltung effektiven Rechtsschutzes hin zu einem praktisch-politischen Lösungsansatz des Problems auf der Handlungsebene. Zuletzt werden die Erkenntnisse zusammenfasst und ein Ausblick auf zukünftige Herausforderungen gegeben (5.).

2. *Personenbezogene Daten im Sinne der DSGVO*

Der Schutz der DSGVO ist in seiner Grundkonzeption auf das Individuum als Rechtssubjekt bezogen. Dementsprechend sind dem Verordnungstext zufolge alle Informationen geschützt, „die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen." (Art. 4 Nr. 1 DSGVO) Identifizierbar in diesem Sinne ist eine natürliche Person, „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind." (Ebd.).

1 Der disziplinenübergreifende Ansatz dieser Ausführungen lädt dazu ein, den Blick mehr in die Breite der Auseinandersetzungen mit dem Thema des Schutzes personenbezogener Daten zu weiten, als in die Details einer einzelnen Fachdebatte einzusteigen. Ausgangspunkt des Textes ist der Versuch, die sehr kleinteilige juristische Fachdiskussion zur eher strukturellen Perspektive in der soziologischen und politikwissenschaftlichen Literatur in Beziehung zu bringen und gegebenenfalls aufzuzeigen, wo möglicherweise Leerstellen bleiben und Anpassungsbedarfe bestehen. Zugleich ermöglicht das Nachdenken über den Personenbezug von Daten aus diesen beiden Richtungen auch eine kritische Auseinandersetzung mit den Grenzen der jeweiligen Disziplinen.

Im Rückschluss greift das Datenschutzrecht dementsprechend bei einigen Datengruppen nicht ein. Dazu gehören zunächst anonymisierte Daten, „die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann." (Erwägungsgrund 26, S. 5 DSGVO) Auch sachbezogene Daten sind nicht geschützt. Dieser Begriff wird in der Verordnung selbst allerdings nicht definiert, sondern lediglich als Gegenbegriff zu dem der personenbezogenen Daten verstanden. Einen Grenzfall stellen pseudonymisierte Daten dar. Das sind gem. Art. 4 Nr. 5 DSGVO Daten, „die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten." Bei pseudonymisierten Daten ist der Personenbezug unter Einbeziehung aller objektiven Faktoren zu ermitteln. Das meint im Wesentlichen das Verhältnis zwischen dem aktuellen Stand der Technik im jeweiligen Zeitpunkt und dem monetären sowie zeitlichen Aufwand, den eine Entschlüsselung in diesem Lichte erfordert.

Daran zeigt sich, dass die Beziehbarkeit eines Datums auf eine natürliche Person entweder aus der Aussage eines genuin als *persönlich* verstandenem Charakters der abgebildeten Information heraus entstehen kann, oder aber sich aus dem Bezug der Daten zueinander ergibt. Je nach Kontext und den über die Gruppenmitglieder verfügbaren Informationen kann sich die Identifizierbarkeit Einzelner situativ stark unterscheiden.

Die Offenheit des Personenbezugsmerkmals schlägt sich im Wortlaut der DSGVO nieder und ist maßgeblich auf ihren Ansatz der Technologieneutralität zurückzuführen. Dieser dient dem Zweck, eine Umgehung der Schutzvorschriften zu vermeiden, indem der Gesetzestext keine technikspezifischen Regelungen vorsieht, sondern das Schutzgut an sich versucht zu konkretisieren, um auf diesem Weg sowohl analoge als auch digitale Datenverarbeitungen unterschiedlichster Art zu umfassen. Mit dem Wortlaut „Für einen Personenbezug müssen Daten einer […] Person zuzuordnen sein" (Art. 4 Nr. 1 DSGVO) bietet der Gesetzestext allerdings eher eine zirkuläre Aussage als eine tatsächlich konkretisierende Definitionshilfe. Auch der Weg über Gegenbeispiele verspricht keine wirkliche Hilfe, da der Begriff der sachbezogenen Daten lediglich negativ zu dem der personenbezogenen definiert wird. Auch für die Gruppe der anonymisierten Daten wird pauschal ein nicht mehr vorhandener Personenbezug unterstellt. Daran zeigt sich, dass jeweils davon ausgegangen wird, dass die Personenbeziehbarkeit von Daten ein eindeutig festzustellendes Merkmal sei. Auf diese Weise wird eine eindeutige Abgrenzbarkeit suggeriert, die sich in der Anwendung oftmals als zirkelschlüssig herausstellt.

Selbst bei Daten, die ausschließlich Bezüge zu Gegenständen aufweisen oder anonymisiert sind und damit die Kehrseite eines personenbezogenen Datums darstellen, kann im Wege der Kombination mit anderen Datensätzen oder durch die Identifikation einzelner Datenpunkte oftmals doch mit relativ hoher Genauigkeit ein spezifisches Mitglied einer Gruppe ausgesondert werden. Zahlreiche Studien zur Re-Identifizierbarkeit von Datensätzen einer gewissen Größe legen nahe, dass eine vollständige Anonymisierung in hinreichend großen Datensätzen nahezu unmöglich ist (Sweeney 2000; Solove/Schwartz 2011). Statt auf diese verarbeitungsspezifischen Risikolagen genauer einzugehen, fokussiert der Verordnungstext selbst, wie oben dargestellt, auf die Frage, was natürliche Personen identifizierbar macht. Diese interpretatorische Lücke wird in der Praxis durch die Heranziehung verfassungsrechtlicher Grundsätze und Rechtsprechung gefüllt. Doch gerade diese Marker ändern sich häufig je nach Datenlage und Situation, sodass stets ein nicht unwesentliches Risiko der Rechtsverletzung bleibt.

3. Kritik der individualistischen Ausrichtung des Datenrechts

Im Folgenden wird die oben dargestellten Ausrichtung des Datenschutzrechts auf individuelle Personen einer kritischen Prüfung unterzogen. Die Kritik bezieht sich im Wesentlichen darauf, dass eine auf sprachlicher Ebene zunächst offensichtlich scheinende Abgrenzbarkeit personenbezogener zu nicht personenbezogenen Daten nur unzureichende Antworten auf bestimmte kontextabhängige Auslegungsprobleme bietet.

3.1 Herausforderungen von KI und Big Data

Die bereits im Rechtstext angelegten Abgrenzungsprobleme verschärfen sich in Fällen der Datenverarbeitung durch *Machine Learning*- und *Big Data*-Techniken. Die Zunahme sogenannter smarter Umgebungen, d.h. datenintensiver Großsysteme, die auf algorithmischer Datenverarbeitung basieren und so eine Echtzeit-Interaktion mit ihrer Umgebung ermöglichen, werden nicht nur in privaten Kontexten (z.B. im Fall von *Smart Homes*), sondern auch in der Unterhaltungsindustrie sowie dem produzierenden Sektor (z.B. mit *Smart Wearables*) eingesetzt. Der Einsatz am Körper oder einem konkreten Objekt dient meist dem Tracking und damit dem Zweck der Optimierung bestimmter Angebote oder Abläufe. Der Einsatz von KI-

basierten Techniken in der Öffentlichkeit kann sich außerdem regulierend auf das Verhalten von Bürger:innen im öffentlichen Raum auswirken und auch gegen den individuellen Willen eingesetzt werden (z.B. im Fall des *Predictive Policing*). Dieser Beitrag konzentriert sich nicht auf prädiktive Polizeiarbeit im engeren Sinne, richtet sein Augenmerk jedoch auf Problemlagen des Einsatzes intelligenter Technologie in öffentlichen Räumen hinsichtlich des Schutzes von Privatheit und Demokratie.

Zunächst aber sollen die beiden zentralen Begriffe *Big Data* und *Künstliche Intelligenz* für den Zweck dieses Beitrags konkretisiert werden. *Big Data* kann mit einer gängigen Definition als ein Modus der Informationsbearbeitung verstanden werden, die von einer Zunahme der Datenmenge (*Volume*) im Vergleich zu vorangehenden Medien, geprägt ist. Dieses Wachstum bildet sich im gesamten Lebenszyklus digitaler Daten ab, d.h. von der Erhebung über ihre Verarbeitung und Analyse bis hin zu ihrer Visualisierung. Darüber hinaus wird seit geraumer Zeit seitens marktbeherrschender Technologieunternehmen versucht, zusätzlich die Zunahme von Wert (*Value*) und Wahrhaftigkeit (*Veracity*) von Daten in die Definition des Begriffs aufzunehmen (Oracle 2021). Das Merkmal der Wahrhaftigkeit wird allerdings dabei auf die innere Schlüssigkeit eines Datensatzes bezogen und nicht auf eine Übereinstimmung bestimmter Daten mit dem Gegenstand ihrer Abbildung. *Künstliche Intelligenz* hingegen beschreibt auf maschinellem Lernen und neuronalen Netzen basierte Anwendungen, die in datenintensiven Umgebungen eingesetzt werden, um darin Muster und Kategorien zu ermitteln. Ein politisches Verständnis dieser Technologien, soweit eine Generalisierung dessen angesichts ihrer jeweils spezifischen Funktionsweisen überhaupt leistbar bzw. sinnvoll ist, konzeptualisiert datenverarbeitende Systeme in öffentlichen Kontexten als Infrastrukturen (Falco 2021).

Ein hervorzuhebender Effekt des oben beschriebenen (jedenfalls quantitativen) Zuwachses von datengestützten Infrastrukturen im öffentlichen Raum ist unter anderem die dadurch deutlich vereinfachte Möglichkeit der kleinteiligen Erfassung von Bewegungs- und Verhaltensmustern einzelner Personen. Durch die Kopplung dieser Methode mit wirtschaftlichen Anreizen entstehen die für den digitalen Kapitalismus typischen datenbasierten Geschäftsmodelle (Srnicek 2017; Staab 2019). Aus der Digitalisierung der Lebenswelten (Kommunikation, Handel, Verkehr, Dienstleistungen, Gesundheit) ergeben sich immer engmaschigere Aggregate individueller Handlungsweisen, deren Auswertung durchaus Potentiale für die Lösung gesellschaftlicher Probleme (z.B. im Gesundheitswesen) verspricht. Dennoch sind statistische Vorhersagen dieser Art aber auch vorurteilsbelastet und häufig ungenau, was hauptsächlich auf die zugrundeliegenden

Trainingsdatensets zurückzuführen ist. Die immer weiter automatisierte Datenverarbeitung ist nicht nur aufgrund ihrer Masse (3V's) unübersichtlich, sondern auch durch die programmierte Architektur und den Schutz als Geschäftsgeheimnis meist intransparent für Außenstehende. Die Funktionsweise unüberwacht selbstlernender algorithmischer Systeme beschreibt Luciana Parisi folgendermaßen: „Undeterminiertheit ist hier als ein aktives Element zu einem Teil der Berechnung geworden, indem sie ausstellt, wie das logische Denken funktioniert, und wie die Bedeutung von Konzepten geformt werden kann. Hier überschneidet sich die Überprüfung von Hypothesen mit der Generierung hypothetischer Bedeutung, indem Unbestimmtheit jenseits wissensbasierter Automatisierung als ein Weg genutzt wird, um Vorhersagen zu strukturieren." (Parisi 2018, S. 103) Damit wird die strukturelle Intransparenz algorithmischer Datenverarbeitungstechniken als sog. *Black Box* noch durch die innere Opazität ihrer Funktionsweise verstärkt.

3.2. Auslegungs- und Übersetzungsprobleme

In Bezug auf das Datenschutzrecht weist Nadezdha Purtova (2018) in einer umfassenden Studie darauf hin, dass die technischen Entwicklungen in naher Zukunft eine perfekte Identifizierbarkeit ermöglichen werden. Dadurch werde die oben dargestellte, in der DSGVO angelegte Abwägung zwischen Deanonymisierungsaufwand und Schutzinteresse mittelfristig obsolet. Die Autorin geht davon aus, dass durch die Digitalisierung der Lebenswelt ein konzeptuelles Verschwimmen von vier bis dato getrennten Sphären zu erwarten sei, die eine von ihr als *Onlife* (Purtova 2018, S. 41; vgl. auch Hildebrandt 2020, S. 6 ff.) bezeichnete Situation hervorbrächten: Die davon betroffenen, bisher als klar abgrenzbar codierten Sphären sind Realität/Virtualität, Mensch/Maschine/Natur, Informationsknappheit/Informationsüberfluss sowie eine von selbstständigen, statischen Entitäten und binären Beziehungen geprägten Weltsicht hin zu einem Fokus auf Interaktionen, Prozesse und Netzwerke (vgl. Purtova 2018, S. 41).

Purtova zufolge hat diese Transformation der Lebenswelt zweierlei Auswirkungen auf das Recht: Mit der zunehmenden Datafizierung gehe einerseits ein gesteigertes Schutzbedürfnis für Einzelne einher, wodurch die Relevanz eines robusten Datenschutzrechts zunächst unterstrichen wird. Anderseits deutet Vieles darauf hin, dass die derzeitige Ausgestaltung des Datenschutzrechts für ein derart weitgreifendes Schutzbedürfnis nicht gewappnet sei und daher auf absehbare Zeit zu kollabieren drohe („system overload", vgl. Purtova 2018, S. 72 ff.). Einen der zentralen Gründe dafür

sieht Purtova in der weiten Definition der Personenbeziehbarkeit von Daten. Im Zusammenspiel mit den erweiterten technischen Möglichkeiten werde sich das Datenschutzrecht auf lange Sicht funktional von einem *lex specialis* zu einem *lex generalis* des Persönlichkeitsschutzes entwickeln. Die Vollzugskraft der DSGVO, vornehmlich in den darin festgeschriebenen Zuständigkeiten und Prüfkompetenzen manifestiert, sei für Grenzfälle und hochkomplexe Technologien wie bspw. automatisierte Gesichtserkennung nur unzureichend geeignet (Purtova 2018, S. 75).

3.3 Ausweitung der Bezugsgruppe (Group Privacy)

Eine weitere Kritik an der geltenden Zentrierung des Datenschutzrechts auf den Schutz von Einzelsubjekten ergibt sich aus der Annahme, dass in Prozessen algorithmischer Datenverarbeitung meist Bezugsgruppen anhand emergenter Kategorisierungen gebildet werden. Diese fortlaufende Kategorisierung ermöglicht eine Steuerung in Echtzeit, indem sie temporäre Merkmale wahrscheinlichkeitsbasiert gerinnen lässt und auf diese Weise den sozialen Raum entlang der kalkulierten Vorhersagen strukturiert. Die im Rahmen dieses Prozesses entstehenden Bezugsgruppen sind in ihrer Datenförmigkeit zugleich sowohl deskriptiver als auch prädiktiver Natur (Mittelstadt 2016, S. 477). Die fortlaufende Re-Konfiguration wirkt sich wiederum modulierend auf die zugrundeliegenden Datensätze aus. Unter diesen Umständen ist es für Einzelpersonen sehr unrealistisch, effektive Kontrolle über die jeweils über sich selbst im Umlauf befindlichen Daten und Informationen zu erlangen (Mittelstadt 2016, S. 481). Der Umfang der im Einzelfall verarbeiteten Daten und die Komplexität der angewandten Methoden rechtfertigen der Ansicht des Autors nach ein kollektives Recht auf Privatheit für *ad hoc* von Algorithmen gebildete Personengruppen (Mittelstadt 2016, S. 485). Mit diesem Ansatz wird die subjektzentrierte Ausrichtung des Datenschutzrechts um eine wertvolle Perspektive der Gruppenorientierung ergänzt, welche bis dato hauptsächlich im Antidiskriminierungsrecht verankert war und damit anderen rechtlichen Voraussetzungen unterlag.

Mit einer ähnlichen Stoßrichtung heben auch Mann und Matzner (2019) die Vorteile einer Erweiterung des Datenschutzrechts um gruppenbezogenen Privatheitsschutz in Fällen von KI-basierten, strukturell diskriminierend wirkenden Anwendungen hervor. In dem von ihnen als *emergente Diskriminierung* bezeichneten Prozess werden durch die Heranziehung komplexer und nichtrepräsentativer Kategorien strukturelle Nachteile für bestimmte Nutzer:innengruppen im Zuge von Profilbildung syste-

misch verstärkt. Da diese Profilbildung oftmals nicht gezielt erfolgt, sondern an implizite Merkmale anonymisierter Datensätze anknüpft, wird sie häufig nicht vom klassischen Antidiskriminierungsrecht erfasst (Mann/Matzner 2019, S. 7). Die Verbindung beider Rechtsregime in Form eines kollektivistisch informierten Datenschutzrechts erscheint angesichts der gruppenbezogenen Funktionsweisen von KI-basierten Systemen durchaus vielversprechend.

3.4 Ausweitung des Zeithorizonts

Ein weiterer Vorschlag zur Ergänzung des Datenschutzes personenbezogener Daten im konkreten Zeitpunkt ihrer Erfassung und Verarbeitung ist das Konzept der *Predictive Privacy* (Mühlhoff 2021). Mühlhoff erläutert die inhärent diskriminierenden Funktionsweisen prädiktiver Algorithmen und zeigt die ethischen und politischen Probleme auf, die aus diesen Vorhersagen erwachsen: Nicht nur negiert eine wahrscheinlichkeitsbasierte Gleichbehandlung die Autonomie und Entscheidungsfreiheit der einzelnen Gruppenmitglieder, sondern sie wirkt auch langfristig in Form performativer Effekte auf die Entscheidungsfindung Einzelner zurück (Mühlhoff 2021, S. 13). Das hat dem Autor zufolge die Wirkung, dass „Predictive systems produce and stabilize precisely the kinds of social differences and inequalities that they claim to merely detect in the world." (Ebd., m.w.N.) Diese Verzerrung, die bei der Überbrückung der *Prediction Gap* – also der Lücke zwischen einer auf Trainingsdaten basierten Wahrscheinlichkeit zu einer auf ein konkretes Individuum gerichteten Vorhersage – entsteht, verschärft noch einmal das zuvor im Anschluss an Parisi dargestellte Problem der verzerrenden Eigendynamik algorithmischer Systeme. Die weit überwiegende Anzahl der *Machine Learning*-Algorithmen basiert auf prädiktiver Analytik und erfüllt somit regelmäßig nicht die Voraussetzungen einer privatheitsschonenden und autonomiefördernden Datenverarbeitung. Daher schlägt er eine Erweiterung des Datenschutzrechts auf solche Daten vor, die aus prädiktiver Analytik hervorgehen und als Grundlage für weitere Analysen dienen (Mühlhoff 2021, S. 14). Somit wäre für die Verwendung und Verarbeitung prädiktiver Modelle ebenso eine Rechtsgrundlage oder ausdrückliche Zustimmung der von dieser Methode betroffenen Individuen erforderlich, wie es derzeit für die Verarbeitung personenbezogener Daten in allen anderen Fällen bereits notwendig ist.

Das Konzept prädiktiver Privatheit stellt gewissermaßen eine Vorstufe der in Art. 22 DSGVO behandelten automatisierten Entscheidungsfindung sowie des Profilings dar. Diese Norm schützt Rechtssubjekte davor, einer

ausschließlich auf automatisierter Datenverarbeitung basierten Entscheidung unterworfen zu werden. Sie unterliegt jedoch engen Anforderungen, die, um den Wirkungsbereich der prädiktiven Analytik zu umfassen, erweitert werden müssten. Dafür spricht, dass aus Nutzer:innenperspektive – insbesondere im Internet – häufig nicht klar ersichtlich ist, welche Daten im aktuellen Zeitpunkt oder in der Zukunft verarbeitet werden, und ob dieser Prozess rechtliche Auswirkungen im Verordnungssinne hat. Außerdem sind die individuellen Reaktions- und Informationsmöglichkeiten häufig überkomplex formuliert und für ein Laienpublikum kaum vermittelbar. Daran wird deutlich, dass über das Art. 22 DSGVO regulierte Endresultat ‚Entscheidung' hinausgehend bereits die im Vorfeld des Ergebnisses stattfindenden prädiktiven Datenanalysen für einen effektiven Individualrechtsschutz in den Blick genommen werden sollten.

3.5 Zwischenfazit

Die vorangehenden Ausführungen verdeutlichen aktuelle Herausforderungen, denen sich das subjektzentrierte Datenschutzregime der DSGVO durch die zunehmende Dominanz von datengetriebenen Geschäftsmodellen und KI-basierten Technologien ausgesetzt sieht. Bereits die herrschende Rechtslage weist Definitions- und Auslegungsprobleme auf, die auf den Ansatz der Technologieneutralität zurückgeführt werden können und durch Zweifelsregeln sowie die pauschale Erweiterung des Anwendungsbereichs kompensiert werden. Dadurch entsteht allerdings nicht die wünschenswerte Rechtssicherheit, sondern vielmehr ein recht instabiles Gleichgewicht, das zeitnah in eine Überforderung des Datenschutzregimes oder zumindest ein Leerlaufen des Rechtsschutzes aufgrund einer unübersichtlichen, schwer zu durchdringenden Rechtslage zu kippen droht. Darüber hinaus erscheint im Lichte der Einwilligungsregeln, die meist für Laien nur schwer bis nicht verständlich sind sowie der hochkomplexen Verarbeitungskonstellationen (vgl. Roßnagel u.a. 2020) eine vollständige Verlagerung der Zustimmungsverantwortung auf individuelle Nutzer:innen nicht besonders effektiv zu sein, was einmal mehr den Mehrwert einer Erweiterung des Datenschutzrechts mit gruppenbezogenen Rechten betont. Einen ersten praktischen Schritt in diese Richtung stellt die Möglichkeit für Verbraucher:innen dar, im Rahmen der EU-Verbandsklagerichtlinie (EU 2020/1828) auch für DSGVO-Verstöße niedrigschwellig entschädigt zu werden. Ebenso sinnvoll wäre eine Ausweitung des Datenschutzrechts auf die Verarbeitungsschritte, die auf die erste Datenerfassung und -verarbeitung folgen, um effektiven Schutz beim Einsatz prädiktiver

Modelle zu gewährleisten. Diese Aspekte zeigen Problemfelder auf, die spezifisch für datenbasierte, selbstlernende KI-Systeme sind. Sie unterstreichen den Bedarf für technologiespezifische Datenschutzregelungen und ein kontextsensibles Privatheitsverständnis (Nissenbaum 2009).

4. *Anwendungsbeispiel: Partizipative Technologieentwicklung in ‚Smart Cities 3.0'*

Der folgende Abschnitt konkretisiert die theoretischen Ausführungen des vorangegangenen Teils exemplarisch anhand der Entwicklung einer digitalen städtischen Infrastruktur und schlägt vor, die identifizierten Probleme des Datenschutzrechts in ein Modell demokratischer Technologieentwicklung einzubetten. Diese Einbettung dient dem Zweck, die Legitimität konkreter technischer Lösungen zu erhöhen und die gesellschaftliche Sensibilität für das inhärent Politische an technologischen Infrastrukturen zu schärfen. Nach einer einführenden Illustration des Themenkomplexes anhand des Szenarios eines Planungsprozesses einer *Smart City* wird der Ansatz der partizipativen Technologieentwicklung aus demokratietheoretischer Perspektive eingehender beleuchtet.

Die bisherige Entwicklung sogenannter *Smart Cities* lässt sich in mehrere Generationen einteilen (Bria/Morozov 2018, S. 5). Die erste Generation teilweise streng kritisierter Konzepte zur Digitalisierung urbaner Räume basierte auf einem technikzentrierten, kommerziell motivierten Stadtentwicklungsmodell, das sich beispielsweise in Gestalt vermeintlich intelligenter Mülleimer manifestiert hat, deren Einbettung in Abfallmanagement-Systeme eher aufgrund ihrer umfassenden Überwachungssysteme Schlagzeilen produzierte als wegen ihrer positiven Auswirkungen auf die Nachhaltigkeit. Ähnlich fragwürdig sind die am Reißbrett geplanten und durch umfassende Public-Private-Partnerships querfinanzierten *Smart Cities* der zweiten Generation, wie sie das Beispiel der Megastadt Songdo in Südkorea veranschaulicht (Halpern/Günel 2017). Die in diesem Zuge entstandenen umfassenden Datensätze, auf die nur begrenzte Personenkreise innerhalb der Betreiberfirmen oder Stadtverwaltungen zugreifen können, haben dazu geführt, dass die datenintensive, KI-gestützte technische Einbettung von städtischen Infrastrukturen in Verruf geraten ist. Neue Modelle der *Smart City* 3.0 versuchen diesem Schicksal entgegenzuwirken, indem sie auf offene Daten und partizipative Modelle der ko-kreativen, bürger:innennahen Technikentwicklung setzen (Bria/Morozov 2018, S. 26).

Beispiele für die dritte Generation digital souveräner Städte sind u.a. Wien und Barcelona, die als Inspiration für die derzeit in Deutschland ge-

förderten Entwicklungs- und Strategieprozesse dienen. Intelligente Städte sind also nicht nur paradigmatisch für die negativen Auswirkungen von KI und Big Data, sondern können auch als ein Ermöglichungsraum für die kooperationsfördernden, demokratischen Potentiale dieser Techniken verstanden werden. Was zunächst als planerisch- politische Herausforderung ohne rechtlichen Bezug erscheinen mag, steht tatsächlich insofern eng in Zusammenhang mit den oben beschriebenen Problemen des Datenschutzrechts, als dass die dort thematisierten Anpassungsbedarfe erst entdeckt werden können, wenn die Wirkweisen von im öffentlichen Raum verwendeten Technologien überhaupt mit betroffenen Personengruppen besprochen und reflektiert werden: Im Rahmen einer ihrem Namen gerecht werdenden intelligenten Stadtentwicklung muss also zwangsläufig auch auf einen passenden Rechtsrahmen und Konzepte der Datengovernance eingegangen werden, die Freiheiten einzelner Datensubjekte schützen und ausweiten.

4.1 Szenario: Entscheidungsprobleme und Risiken intelligenter Infrastrukturen

Die Ermöglichung dieser Potentiale erfordert eine Auseinandersetzung mit zahlreichen Entscheidungen, die im Rahmen der digitalen Infrastrukturentwicklung in urbanen Räumen zu treffen sind. Beispielhaft soll das anhand eines Gedankenexperiments – dem Bau einer intelligenten Brücke als Bestandteil einer vernetzten städtischen Infrastruktur – illustriert werden. Ein partizipativer Beteiligungsprozess könnte dafür die Perspektiven der durch Los bestimmten Mitglieder eines Bürger:innengremiums in die Planung und Umsetzung der Brücke einbeziehen.

Eine erste Illustration der Politizität digitaler Technologien bietet bereits die Frage, welche Funktion die Brücke erfüllen soll. Während das auf den ersten Blick offensichtlich scheint – Brücken dienen dem sicheren Überqueren von Flüssen – könnten zusätzlich aber auch die Strömungsbewegungen des Gewässers sensorisch aufgezeichnet und ggf. automatisierte Warnsysteme implementiert werden, die den Verkehr bei drohender Gefahr, z. B. durch einen ansteigenden Wasserspiegel, in Echtzeit umleiten.

Die technischen Möglichkeiten sind auch für die Einbindung der Brücke in die Sicherheitsarchitektur der Stadt relevant. Nicht nur die Steuerung des Straßenverkehrs liegt hier als Bezugspunkt nahe, sondern auch der Einsatz KI-basierter Techniken zur Überwachung des öffentlichen Raums sowie zahlreiche Herausforderungen des automatisierten Fahrens. Die damit einhergehenden Fragen und Probleme sollten vor einer Imple-

mentierung steuernder Systeme breit angelegten Beteiligungsprozessen zugeführt werden.

Im Bereich der Nachhaltigkeit könnte eine intelligente Brücke beispielsweise durch *Predictive Maintenance,* d.h. automatisierte Wartungsprozesse, Vorteile für Umwelt und Stadtgesellschaft bewirken. Ebenso könnte ein intelligentes Nachhaltigkeitsmanagement eine Verschaltung der Brückennutzung mit anderen Ressourcen bedeuten, was den Erhalt und Betrieb wiederum in Abhängigkeit zu anderen Finanzierungsposten des Systems bringen würde. Darüber hinaus könnte eine solche Brücke auch die Wasserqualität des Flusses messen, die verarbeiteten Daten auswerten und aufbereiten und ggf. sogar den Sauerstoffgehalt des Wassers in Reaktion auf die Befunde beeinflussen.

Die Vielfalt dieser Struktur- und Funktionsentscheidungen hängt eng mit Entscheidungen über die Gestaltung der Datenarchitektur bzw. der Datengovernance zusammen (vgl. Micheli u. a. 2020). Dabei geht es um die Frage, welche Daten auf welche Weise und an welchem Ort gespeichert und verarbeitet werden sollen, die Bestimmung der gewünschten Verarbeitungsweise sowie die Bemessung angemessener Löschfristen. Zur Vermeidung von Datensilos, d.h. isolierten, nur eingeschränkt interoperablen Datensätzen in privater oder öffentlicher Hand, sind mehrere Modelle denkbar und mittlerweile im städtischen Kontext auch gut erprobt. Das Datenmanagement in sog. Datenpools, Datenkooperativen oder Treuhändermodellen ist zentraler Gegenstand des aktuellen Entwurfs der EU-Kommission zum Data Governance Act (2020/767 final). In der Suche nach einem passenden Modell sollten alle beteiligten Stakeholder und Akteure einbezogen werden – nicht zuletzt, um einen angemessenen Privatheitsschutz zu gewährleisten. Diese Einbeziehung von Betroffenen ergänzt die Durchführung einer Datenschutz-Folgeabschätzung durch Expert:innen und öffnet nicht nur den Raum für eine kritische Auseinandersetzung, sondern fördert im Fall einer erfolgreichen Umsetzung auch die Akzeptanz in der Bevölkerung.

Diese beispielhafte Darstellung ließe sich noch fortführen, insbesondere hinsichtlich der Einbettung einzelner Bausteine in komplexere digitale Infrastrukturen eines ganzen urbanen Systems. Für alle hier angedeuteten Felder sind datengestützte und KI-basierte technische Verfahren essentiell, damit sie einen funktionalen Mehrwert generieren und das jeweils erwünschte Wissen produzieren können. Ob die im Einzelnen adaptierten Lösungen tatsächlich das Prädikat der Intelligenz verdienen, lässt sich allerdings nicht allein anhand der Anzahl digitalisierter Prozesse oder der Menge der erhobenen Daten bestimmen. Vielmehr ist ihr gesellschaftlicher Mehrwert im Einzelnen abhängig von einer sinnvollen und robusten

Einbettung in bestehende Systeme, wozu auch die bereits vorhandenen menschlichen Ressourcen zu zählen sind. Ein für soziale und politische Strukturen und Arbeitsprozesse blinder Solutionismus droht, die negativen Auswirkungen intelligenter Infrastrukturen auf den Schutz von Privatheit und individueller Autonomie zu verstärken.

Privatheitsrisiken im Bereich der Planung, Entwicklung und Umsetzung intelligenter Städte entstehen zunächst, wenn sie maßgeblich der Privatwirtschaft überlassen werden. Öffentliche Träger allein verfügen aber bislang nur selten über die finanziellen Mittel oder die Expertise, technologische Innovationen in einem mit dem privaten Sektor vergleichbaren Tempo und Ausmaß zu entwickeln. Die Auswirkungen der derzeit in der Umsetzung befindlichen EU-Gesetzgebung zum digitalen Binnenmarkt könnten, sofern der Balanceakt zwischen Innovationsförderung und Rechtsicherheit gelingt, durchaus positive Schwerpunkte für eine gemeinwohlorientierte Datenwirtschaft setzen.

Ein zweifelhafter Rückschluss aus dem Privatisierungsdilemma könnte hingegen darin liegen, dass der Staat sich am besten selbst um die im Rahmen der *Smart City*-Infrastrukturen erfassten Daten kümmern solle. Aber auch diese Forderung bietet Anlass zu Bedenken: Immer umfangreichere Überwachungspraktiken werden unter den Schutzzweck der öffentlichen Sicherheit subsumiert und in der bereits angesprochenen prädiktiven Polizeiarbeit umgesetzt. Das allseitige Risiko einer Überwachung von unternehmerischer und staatlicher Seite sowie durch Bürger:innen untereinander in datafizierten Gesellschaften bietet Anlass zu der beunruhigenden Frage, wer eigentlich vor wem zu beschützen ist (Bächle 2016, S. 182).

An dieser Stelle lohnt ein Rückblick an die zuvor ausgeführte Kritik der Zentrierung des geltenden Datenschutzrechts auf *personenbezogene* Daten. Für nahezu alle Daten, die von der im obigen Szenario beschriebenen intelligenten Brücke erfasst und verarbeitet werden, ließen sich bereits aus der Verbindung weniger Datenpunkte maßgeschneiderte Profile und Vorhersagen erstellen. Hinzu kommt, dass auch eine Anonymisierung die Möglichkeit der Profilbildung und Aussonderung Einzelner nie vollständig eliminiert. Gleichzeitig ist eine wirksame Einwilligung in derart umfassende Datenerfassung und -verarbeitung in öffentlichen Räumen nur schwer konstruierbar. Technische Lösungen, die für die beschriebenen Probleme bereits entwickelt sind und eingesetzt werden, sind *Privacy Enhancing Technologies* oder dezentrale Speicherungs- und Verschlüsselungslösungen auf der Ebene der Datengovernance. Art. 25 DSGVO (*Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*) verankert ihre Implementierung im Verordnungstext. Eine verpflichtende Umsetzung dieser beiden Standards könnte das Datenschutzniveau

deutlich erhöhen. Eine aktive Auseinandersetzung mit den Schutzgehalten und Risiken der technischen Lösungen im Einzelnen findet auf der Ebene der auftraggebenden Stelle mit der verpflichteten Durchführung einer Datenschutz-Folgeabschätzung (Art. 35 DSGVO) bereits häufig statt. Diese Auseinandersetzung könnte aber im Rahmen einer demokratischen Technologieentwicklung weitergeführt werden, indem die Frage danach, welcher Schutz im jeweiligen Kontext überhaupt gebraucht bzw. gewünscht wird, an den weiteren Betroffenenkreis gestellt wird. In dieser Auseinandersetzung kreuzen sich die beiden hier eingenommenen Perspektiven: Partizipative Gestaltungsformate stellen oftmals einen geeigneten Raum dar, um zivilgesellschaftlichen Einschätzungen über Risikolagen, den daraus entstehenden Konstellationen zu schützender Rechtsträger:innen sowie der Dauer der jeweiligen Datenschutzvorkehrungen in die Entwicklung einzubeziehen.

Eine Antwort auf die Frage, wer vor wem zu schützen ist, verbirgt sich im Kontext der Datenverarbeitung und den spezifischen Eigenschaften der jeweils angewandten Technologien. Zugrunde liegt dem immer der Gedanke, dass die subjektiven Entscheidungsmöglichkeiten Einzelner möglichst umfassend erhalten werden sollten, damit nicht vorrangig vermeintlich objektive, datengestützte und auf korrelativen Modellen beruhende Analysen als Grundlage für die Gestaltung öffentlicher Räume und die darin implementierten Steuerungslogiken herangezogen werden. Dieser Ansatz ist auch an die von der EU-Kommission jüngst vorgeschlagene risikobasierte KI-Regulierung anschlussfähig.

4.2 Demokratische Technologieentwicklung für intelligente Städte

Die im vorigen Teilabschnitt verdeutlichten politischen und gesellschaftlichen Effekte digitaler Infrastrukturen intensivieren also den politischen Entscheidungsdruck nicht erst im Zeitpunkt ihres Einsatzes, sondern bereits während ihrer Planung und Entwicklung. Dadurch wächst der Bedarf einer demokratischen Auseinandersetzung mit dem Design intelligenter Technologien, um ihren normativen Wirkungen im Rahmen eines integrativen und gemeinwohlorientierten Digitalisierungsprozesses Rechnung zu tragen.

Demokratische Technologieentwicklung beschreibt eine öffentliche Auseinandersetzung mit den regelnden und steuernden Wirkungsweisen der eingesetzten Technik auf individuelle und kollektive Handlungs- und Autonomieräume. Das muss nicht bedeuten, dass im Sinne umfassender Transparenzanforderungen jedes einzelne technische Detail eines Systems

für die Gesamtbevölkerung erklärbar gemacht werden muss. Vielmehr ist eine Sensibilisierung dafür, wann und auf welche Weise individuelle Entscheidungen von algorithmischen Systemen überschrieben bzw. eingeschränkt werden, erforderlich, um überhaupt ausmachen zu können, inwiefern die konstitutionelle Ordnung durch sie unter Druck gerät und wie damit umzugehen ist (Müller-Mall 2020).

Modelle der kooperativen Stadtentwicklung finden sich in planungsrechtlichen Beteiligungsverfahren, die durch Methoden des in der Technologieentwicklung seit den 70er Jahren etablierten *Participatory Design* ergänzt werden können. Dabei wird das Wissen der Akteure, die von einer konkreten Technologie betroffen sind, für den Technikentwicklungsprozess fruchtbar gemacht. Praktisch bedeutet das die gemeinsame Auseinandersetzung von Nutzer:innen und Entwickler:innen mit den zu lösenden Problemen, verfügbaren Ressourcen und technischen Möglichkeiten. Im Kontext einer *Smart City* kann das z.B. in Stadtlaboren und anhand von modellhaften Prototypen geschehen. So fällt die Ermittlung konkreter Potentiale und Risiken von Technologien für das Gemeinwesen leichter (Williams 2020) und ergänzt die Einschätzungen von Expert:innen, beispielsweise in der Form von Datenschutz-Folgeabschätzungen, um wertvolles Wissen. Auf das Datenschutzrecht bezogen bedeutet es, dass die oben illustrierten individuellen und kollektiven Interessen bezüglich bestimmter Datenverarbeitungsvorgänge besser verstanden, eingeordnet und bewertet werden können. Statt die Abwägung einzelner Belange in den vermeintlich objektiven Raum einer algorithmischen Black Box zu verlegen, deren Funktion in erster Linie auf die proprietären Gewinninteressen großer Technologieunternehmen zugeschnitten ist, kann im Rahmen von Beteiligungsverfahren erforscht und herausgearbeitet werden, an welchen Stellen der Einsatz von Künstlicher Intelligenz überhaupt gesellschaftlich erwünscht ist, und wo eine manuelle bzw. menschlich gesteuerte Verarbeitung vorzuziehen ist (Keymolen/Voorwinden 2020). So wird überhaupt auch erst ein *Design for all*, also eine inklusive Technologie- und Stadtentwicklung möglich. Die Funktionen von Systemen wie der datengestützten Brücke müssen also von iterativen, diskursiven Prozessen begleitet werden. Das ist ohne offene Daten, wirksamen Persönlichkeitsschutz und freie Software nicht möglich, die damit einen zentralen Bestandteil jedes demokratischen Datenmodells bilden sollten.

5. Fazit und Ausblick

Die hier skizzierten theoretischen Gedanken und methodischen Ansätze lassen sich mit deliberativen und experimentellen Ansätzen der Demokratietheorie verbinden. Viele der aktuell in der Umsetzung befindlichen *Smart City*-Strategien greifen auf gemeinwohlorientierte Methoden zurück und haben sich damit bereits in der praktischen Umsetzung positiv bewährt. Eine demokratische Nutzung von KI erfordert im Kontext öffentlicher Infrastrukturen also sowohl eine Kollektivierung von (Privatheits-)Risiken als auch eine diskursive Verankerung im Gemeinwesen. Die Bedeutung des ersten Aspekts für die Nutzung von Künstlicher Intelligenz ist nicht zu unterschätzen, um eine mit Privatheitsinteressen verträgliche Innovation zu gewährleisten. Partizipative Methoden an sich werden noch nicht die im ersten Teil des Beitrags herausgearbeiteten strukturellen Probleme des Datenschutzrechts zu lösen vermögen. Dennoch ist eine gemeinwohlorientierte, inklusive Auseinandersetzung mit den Schutzmöglichkeiten und -modalitäten des Datenrechts eine essentielle Komponente der Einbettung digitaler Infrastrukturen in demokratische Gemeinwesen. Während eine Monopolisierung von Daten in privater oder öffentlicher Hand nicht in der Lage ist, das erwünschte Maß an gesellschaftlichem Vertrauen in datafizierte öffentliche Räume hervorzubringen, bieten die hier vorgestellten Ansätze dafür essentielle Experimentierräume und Einflussmöglichkeiten.

Literatur

Artikel-29-Datenschutzgruppe (2007): Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 01248/07/DE.

Bächle, Thomas Christian (2016): *Digitales Wissen, Daten und Überwachung zur Einführung.* Hamburg: Junius.

Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) im Bundesamt für Bauwesen und Raumordnung (BBR) (2021): Smart City Charta. Digitale Transformation in den Kommunen nachhaltig gestalten. URL: https://www.smart-city-dialog.de/wp-content/uploads/2021/04/2021_Smart-City-Charta.pdf (besucht am 03.11.2021).

Coletta, Claudia und Kitchin, Rob (2017): Algorhythmic governance: Regulating the ‘heartbeat’ of a city using the Internet of Things. *Big Data & Society* 4(2). doi: 10.1177/2053951717742418.

Falco, Gregory (2019): Participatory AI: Reducing AI Bias and Developing Socially Responsible AI in Smart Cities. *Conference Paper. The 22nd IEEE International Conference on Computational Science and Engineering.* URL: https://www.researchgate.net/publication/333916704 (besucht am 10.01.2022).

Floridi, Luciano (2014): Open data, data protection, and group privacy. *Philosophy and Technology*, 27(1), S. 1-3. doi: https://doi.org/10.1007/s13347-014-0157-8.

Halpern, Orit und Günel, Gökce (2017): FCJ-215 Demoing unto Death: Smart Cities, Environment, and Preemptive Hope. *The Fibreculture Journal* 29, S. 51-73. doi:10.15307/fcj.29.215.2017.

Hildebrandt, Mireille. 2020. *Law for Computer Scientists and Other Folk.* Oxford: Oxford University Press.

Hoffmann-Riem, Wolfgang (2019): Die digitale Transformation als Herausforderung für die Legitimation rechtlicher Entscheidungen. In: Unger, Sebastian und von Ungern-Sternberg, Antje (Hrsg.): *Demokratie und künstliche Intelligenz*. Tübingen: Mohr Siebeck, S. 130-157.

Keymolen, Esther und Voorwinden, Astrid (2020): Can we negotiate? Trust and the rule of law in the smart city paradigm. *International Review of Law, Computers and Technology*, 34(3), S. 233-253.

Koops, Bert-Jaap (2008): Criteria for Normative Technology. In: Brownswood, Roger und Yeung, Karen (Hrsg.): *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes.* Oxford/Portland: Hart Publishing, S. 157-174.

Matzner, Tobias und Mann, Monique (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society* 6(2), doi: 10.1177/2053951719895805.

Mayer-Schönberger, Viktor und Cukier, Kenneth (2013): *Big Data. A Revolution that will transform how we live, work and think*. Boston/New York: Harcourt.

Micheli, Marina; Ponti, Marisa, Craglia, Max und Suman, Anna Berti (2020): Emerging models of data governance in the age of datafication. *Big Data & Society* 7(2). doi: 10.1177/2053951720948087.

Mittelstadt, Brent (2017): From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology* 30, S. 475-494. doi: 10.1007/s13347-017-0253-7.

Morzov, Evgenji und Bria, Francesca (2018): *Rethinking the Smart City. Democratizing Urban Technology*. New York: Rosa-Luxemburg-Stiftung. URL: https://rosalux.nyc/rethinking-the-smart-city/ (besucht am 07.01.2022).

Mühlhoff, Rainer (2021): Predictive privacy: towards an applied ethics of data analytics. *Ethics and Information Technology* 23, S. 675-690. doi: 10.1007/s10676-021-09606-x.

Müller-Mall, Sabine (2020): *Freiheit und Kalkül. Die Politik der Algorithmen.* Ditzingen: Reclam.

Nikitas, Alexandros; Michalakopoulou, Kalliopi; Tchouamou Njoya, Eric und Karampatzakis, Dimitris (2020): Artificial Intelligence, Transport and the Smart City: Definitions and Dimensions of a New Mobility Era. *Sustainability* 12(7), S. 2789-2808. doi: 10.3390/su12072789.

Nissenbaum, Helen (2009): *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Stanford: Stanford University Press.

Madsen, Anders Koed (2018): Data in the smart city: How incongruent frames challenge the transition from ideal to practice. *Big Data & Society* 5(2). doi: 10.1177/2053951718802321.

Oracle (2021): Was ist Big Data? URL: https://www.oracle.com/de/big-data/what-is-big-data/ (besucht am 23.09.2021).

Parisi, Luciana (2018): Das Lernen lernen oder die algorithmische Entdeckung von Informationen. In: Engemann, Christoph und Sudmann, Andreas (Hrsg.): *Machine Learning – Medien, Infrastrukturen und Technologien der Künstlichen Intelligenz.* Bielefeld: transcript, S. 93 – 114.

Purtova, Nadezhda (2018): The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* 10(1), S. 40-81. doi: 10.1080/17579961.2018.1452176.

Roßnagel, Alexander u.a. (2020): White Paper Einwilligung. Möglichkeiten und Fallstricke aus der Konsumentenperspektive. Karlsruhe: Forum Privatheit und Selbstbestimmung in der digitalen Welt.

Solove, Daniel J. und Schwartz, Paul M. (2011): The PII Problem. Privacy and a New Concept of Personally Identifiable Information. *N.Y.U. Law Review* 86, S. 1814-1894.

Srnicek, Nick (2017): *Platform capitalism*. Cambridge: Polity.

Staab, Philipp (2019): *Digitaler Kapitalismus. Markt und Herrschaft in der Ökonomie der Unknappheit*, Berlin: Suhrkamp.

Sweeney, Latanya (2000): Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh. URL: https://dataprivacylab.org/projects/identifiability/index.html (besucht am 10.01.2022).

Williams, Sarah (2020): *Data Action. Using Data for Public Good.* London: MIT Press.