Januar 2018 · Dr. Nicola Jentzsch

Dateneigentum – Eine gute Idee für die Datenökonomie?

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Die Digitalisierung der deutschen Wirtschaft ist in den kommenden Jahren ein Hauptziel der deutschen Politik. So versucht die Bundesregierung, die Verwertung von persönlichen Daten in verschiedenen Branchen anzukurbeln, um die Abwanderung digitaler Wertschöpfung ins Ausland zu verringern. In diesem Kontext wird die Einführung eines Eigentumsrechts an Daten diskutiert, wobei persönliche Daten Material- oder Immaterialgütern gleichgestellt werden sollen.

Unternehmen und/oder Personen sollen damit die Möglichkeit erhalten, Daten besser monetarisieren zu können. Auch die Verwendung und Verwertung persönlicher Daten soll besser kontrolliert werden können. Dies soll Investitionen in die Datenerschließung absichern und datengetriebene Innovation ankurbeln. Unternehmen sollen personenbezogene Daten einfacher für neue Geschäftsmodelle nutzen können. Aber erfüllen sich diese Versprechungen durch Dateneigentum?

Derzeit geht die öffentliche Debatte zu dem Thema größtenteils an vorhandenen wissenschaftlichen Erkenntnissen vorbei. Aus ökonomischer Sicht ist sehr fraglich, ob Dateneigentumsrechte Märkte tatsächlich effizienter machen und für die richtigen Anreize sorgen. Zentral ist dabei die Frage, ob andere wirklich effektiv von der Nutzung der Daten ausgeschlossen werden können oder dies eher die Ausnahme als die Regel ist. Ökonomen klassifizieren Güter in Privat-, Club- und Gemeingüter. Es lässt sich feststellen, dass Daten und Informationen je nach Kontext unterschiedliche Eigenschaften annehmen und daher kaum dem Idealbild des Privat- oder Clubgutes entsprechen.

Sobald sie aber Eigenschaften öffentlicher Güter zeigen (Nicht-Ausschluss vom Konsum und Nicht-Rivalität im Verbrauch) gilt, dass Märkte *kein* Mechanismus sind, um eine optimale Menge an Informationen bereitzustellen. Märkte könnten durch Dateneigentum dann nicht effizienter funktionieren, da durch Externalitäten und Freifahrertum Anreizprobleme hervorgerufen werden.

In den Rechtswissenschaften entwickelt man derzeit Ansätze, die Analogien zum Material- und Immaterialgüterrecht bemühen. Im ersten Fall sollen Daten Sachen gleichgestellt werden. Im zweiten dient das Urheberrecht als Pate. So sollen Dateneigentümer ein ausschließliches Nutzungsrecht erhalten und Lizenzen für Datennutzung vergeben können. Aus *rechtlicher Sicht*

besteht aber das Problem, dass sich Daten und Informationen juristisch nicht eindeutig einer Partei zuordnen lassen. Daher lehnen viele Rechtsexperten eigentumsrechtliche Überlegungen ab. Unter anderem sieht das Bundesverfassungsgericht persönliche Informationen als ein Abbild einer sozialen Realität, das *gerade nicht* einem Betroffenen allein zugeordnet werden kann. Daten und Informationen zeigen außerdem übergreifende Eigenschaften, da das eine nicht ohne das andere bestehen kann.

Neben *ökonomischen und rechtlichen* Aspekten stellt sich die Frage, ob Dateneigentum *technisch* gesehen unter Marktbedingungen überhaupt umsetzbar ist. Unternehmen, die sich digital transformieren, indem sie Big-Data-Architekturen implementieren, definieren auf der Ebene der IT-Systeme Eigentümerrechte. Diese sind nicht mit juristischen Eigentumsrechten zu verwechseln. Vielmehr legen Unternehmen fest, welche Personen oder Personengruppen Zugriffs- und Entscheidungsbefugnisse bezüglich der Datensätze erhalten. Auf der Ebene des einzelnen Unternehmens können solche Rechte festgelegt werden. Allerdings heißt dies nicht, dass diese *unternehmensübergreifend* verwaltet werden können, zum Beispiel im Falle eines Datentransfers. Hier gehen die Meinungen unter Experten weit auseinander: Manche glauben, BlockChain-basierte Technologien bergen dafür Potential, andere vertreten die Ansicht, dass keine zentrale Kontrolle von Daten und Informationen oder entsprechenden Eigentumsrechten möglich ist.

Auch aus Sicht des Datenschutzes würde eine Verankerung von Eigentumsrechten aufgrund der entstehenden Marktdynamik keine Garantie für *mehr* Privatsphäre sein. Es könnte sogar das Gegenteil bewirkt werden: Wird das ökonomische Eigeninteresse der Datenpreisgabe protegiert, könnte dies dazu führen, dass immer mehr Menschen Daten über sich veröffentlichen, um einen ‚guten Deal' zu bekommen. InsurTech, Telematik und persönliche Big-Data-Plattformen sind Beispiele von Geschäftsmodellen, die diese Tendenzen befördern. Dies könnte zu einem sozialen Zwang der Preisgabe führen mit entsprechend negativen Auswirkungen auf die Privatsphäre aller.

Inhaltsverzeichnis

Einleitung 1

Daten als Informationsgüter: Ist ein Eigentum möglich? 2

Rechtliche Vorstöße zum Dateneigentum 2

Ökonomische Ansätze: Privat-, Club- oder Gemeingut? 6

Dateneigentum: Technisch umsetzbar? 8

Erosion der Privatsphäre durch Marktdynamik 10

Rechtliche Ansätze gegen Erosionstendenzen 13

Ökonomische Erkenntnisse zu Erosionstendenzen 14

Schluss 16

Referenzen 18

Impressum 22

Einleitung

Dateneigentum – dieses Schlagwort wird von seinen Befürwortern als Allheilmittel verschiedener Wettbewerbsprobleme propagiert. Durch seine Einführung – beispielsweise über ein Datengesetz – sollen Investitionen von Unternehmen in Datenerschließung abgesichert und Anreize für mehr Innovation gesetzt werden. Unter anderem hofft manch einer in der Automobilindustrie darauf, dass sich durch Dateneigentum die Position im internationalen Wettbewerb absichern oder verbessern lässt. Vorschläge dieser Art kursieren seit letztem Jahr auf Ministeriumsebene, insbesondere Bundesverkehrsminister Alexander Dobrindt (CSU) setzte sich für ein Datengesetz ein, in dem ein solches Eigentumsrecht geregelt ist. Sind die damit verbundenen Hoffnungen berechtigt? Oder entpuppt sich „Dateneigentum“ bei näherer Betrachtung als Pseudo-Lösung, die ungeeignet ist, die deutsche Wirtschaft voranzubringen?

In diesem Impuls soll Dateneigentum einer kritischen interdisziplinären Kurzprüfung unterzogen werden. Dateneigentum bedeutet, stark verkürzt, dass personenbezogene Daten quasi wie Material- oder Immaterialgüter behandelt werden. Dies geschieht durch Konkretisierung und Zuweisung von Verfügungsrechten an eine der Marktparteien, also Verbraucher oder Unternehmen. Verfügungsrechte bezeichnen die Rechte der Datenerschließung und -verarbeitung, einschließlich ihrer Nutzung, Übertragung und Löschung. Im Kontext dieses Impulses bezeichnen Daten den Rohstoff (d.h. Items in Datenbanken), während sich der Begriff der ‚Informationen’ auf die gewonnenen Analyseresultate bezieht.

Derzeit werden von verschiedenen Stakeholdern Pro- und Contra-Argumente bezüglich des Dateneigentums gesammelt. Hierbei läuft der politische Diskurs zum einen größtenteils an den bereits bestehenden wissenschaftlichen Erkenntnissen vorbei. Zum anderen wird er parallel in rechtlichen, ökonomischen und technischen Experten-Silos geführt. Dies führt dazu, dass die Interaktionen dieser Gebiete unbeachtet bleiben. Allein die Frage, ob Dateneigentum unter Marktbedingungen technisch implementierbar und administrierbar ist, bleibt unbeantwortet.

In diesem Impuls werden zunächst die rechtlichen Analogien zum Material- und Immaterialgüterrecht Ansätzen gegenüber gestellt, die diese Überlegungen komplett ablehnen. Die ökonomische Argumentation wiederum zielt darauf ab, dass mit Privateigentum an Daten eine effizientere Ressourcenallokation über Marktmechanismen erreicht werden kann. Hier stellt sich die

Frage, ob Daten überhaupt als Privateigentum konzipiert werden könnten, ob sie Club- oder Gemeingüter sind. Neben den rechtlichen und ökonomischen Erkenntnissen zum Thema werden hier auch kurz technische Ansätze erläutert. Dabei geht es um die Implementierung von Verfügungsrechten auf IT-Systemebene im Rahmen der unternehmerischen Data Governance.

Dateneigentum würde der Datenökonomie also, sofern in einem Datengesetz geregelt, neben der bereits in der Umsetzung befindlichen EU-Datenschutzgrundverordnung, einen weiteren Regulierungsrahmen überstülpen. Dies wirft nicht nur Fragen der rechtlichen Konsistenz, sondern auch Fragen des Persönlichkeitsschutzes in Bezug auf Privatsphäre auf. Derzeit finden sich unter Experten aus Unternehmen, zivilgesellschaftlichen Organisationen und Datenschutzverbänden kaum Stimmen, die ein Dateneigentum, egal welcher Art, befürworten.

Daten als Informationsgüter: Ist ein Eigentum möglich?

Die derzeitige Rechtslage in Deutschland bezogen auf Verfügungsrechte an persönlichen Daten kann getrost als Flickenteppich bezeichnet werden. So entstammen Verfügungsrechte dem Bundesdatenschutzgesetz, dem Urheberrechtsgesetz und dem Schutz von Datenbankwerken. Weitere rechtliche Regelungen finden sich im Gesetz gegen den unlauteren Wettbewerb (zum Beispiel Betriebs- und Geschäftsgeheimnis), dem Telemediengesetz oder dem Intelligente Verkehrssysteme Gesetz. Ein kompletter Scan der gesetzlichen Regelungen würde den Umfang des Impulses sprengen, daher hier nur der Hinweis, dass Ähnliches zumindest für Daten aus vernetzten Fahrzeugen bereits geleistet worden ist.[1] Es lässt sich festhalten, dass für verschiedene Datenarten je nach Kontext unterschiedliche Verfügungsrechte gelten und dies von Branche zu Branche variiert.

Rechtliche Vorstöße zum Dateneigentum

Erste Denkanstöße zum Thema Dateneigentum wurden schon vor Jahrzehnten gegeben: Die Debatte ist also alt, auch wenn sie immer wieder aufflammt. In den USA reicht die Debatte bis in die 1960er Jahre zurück und entsprang

1 Zum Beispiel: Bundesministerium für Verkehr und Digitale Infrastruktur (2017); Schaufenster Elektromobilität (2016), Arbeitsgruppe “Digitaler Neustart” (2017).

dort ursprünglich juristischen Erwägungen.[2] Es kann also getrost davon ausgegangen werden, dass viele der Pro- und Contra-Argumente bereits vor Jahrzehnten in Fachkreisen diskutiert wurden und viele der ökonomischen Implikationen bereits bekannt und analysiert sind.

Befürworter des Dateneigentums beabsichtigen die Schaffung einer Analogie zum Sacheigentum im Materialgüterrecht.[3] Daten sollen beispielsweise Sachen gleichgestellt werden.[4] So könnte ein Datengesetz den Zugang zu Daten für Unternehmen und Behörden ebenso regeln wie das berechtigte Datenschutzinteresse der Bürger. Je nach Stakeholder variiert es, welcher Marktpartei das Eigentum überantwortet werden soll. Das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) jedenfalls benennt jene Partei, die in die datenbasierte Wertschöpfung (Erschließung, Analyse und Nutzung) investiert.[5] Dies wäre im Falle von vernetzten Fahrzeugen beispielsweise die Automobilindustrie.

Die Befürworter sehen das Dateneigentum als notwendige Bedingung für die Schaffung eines effizienten Datenmarktes, in dem das freie Spiel von Angebot und Nachfrage die optimale Datenmenge bereitstellt. Gleichzeitig sollen über Eigentumsrechte Investitionen abgesichert und Innovationen in Unternehmen incentiviert werden.

Artverwandte Vorschläge beziehen sich auf das Immaterialgüterrecht**.** „Immaterialgüterrechte entstehen durch Erfüllung der Tatbestandsvoraussetzungen des jeweiligen Spezialgesetzes, etwa Eintragung in das Markenregister (zum Beispiel § 4 Nr. 1 MarkenG), Veröffentlichung im Patentblatt (§ 58

2 Litman, J. (2000). Information Privacy/Information Property. Stanford Law Review (online), http://www-personal.umich.edu/~jdlitman/papers/infoprivacy.pdf; Samuelson, P. (2000). Privacy as Intellectual Property? Stanford Law Review 52 (5): 1125–1174; Schwartz, P.M. (2004). Property, Privacy, and Personal Data, Harvard Law Review 117 (2055): 2056-2128; Westin, A. (1967). Privacy and Freedom (Athenum: New York).

3 Bürgerliches Gesetzbuch, Buch 3 - Sachenrecht (§§ 854 - 1296), Abschnitt 3 - Eigentum (§§ 903 – 1011).

4 Bundesministerium für Verkehr und Digitale Infrastruktur (2017). Wir brauchen ein Datengesetz in Deutschland! Strategiepapier Digitale Souveränität, https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html.

5 BMVI (2017). „Eigentumsordnung“ für Mobilitätsdaten? - Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.html?nn=12830; S. 3-4.

Abs. 1 S. 3 PatG), die Entstehung des Werks durch einen schöpferischen Akt (§ 2 Abs. 2 UrhG) oder die Herstellung einer Datenbank (§ 87a UrhG).“[6]

Unter dem urheberrechtlichen Blickwinkel werden Lizenzierung- oder Treuhandmodelle entwickelt, bei denen Verwertung und Nutzung der Daten getrennt verlaufen können. Ein Lizenzierungsmodell ermöglicht dem Urheber ein ausschließliches Nutzungsrecht an seinem Werk (den Daten), das zeitlich befristet ist. Der Urheber kann Dritten Nutzungs- und Verwertungsrechte einräumen oder ihnen die Nutzung der Daten untersagen.[7] Ähnliches ist bei der Lizenzierung von Datenbanken bereits möglich.[8]

Beim Treuhandmodell soll eine Daten-Treuhand, zum Beispiel DEDATE, als öffentlich-rechtliche Körperschaft die Spielregeln für die Nutzung und Verwertung der Daten festlegen und gegebenenfalls Nutzungsentgelte nehmen.[9]

Nahe verwandt mit diesem Ansatz ist das „Datenverwertungsrecht.“ Vertreter der Patenschaft des Urheberrechts für ein solches Verwertungsrecht sind beispielsweise Schwartmann und Hentsch.[10] Die Autoren konstatieren, dass die Verwertung personenbezogener Daten zwar Teil der Nutzung für Geschäftszwecke eines Unternehmens sein kann, aber ein *Eigentumsschutz* oder ein bestimmtes *Verwertungsrecht* leiten sich daraus aber nicht ab. Sie sind der Ansicht, dass ein echtes Datenverwertungsrecht fehlt und damit fehlt auch eine spezifische Kategorisierung der Verwertungsarten. Ein Da-

6 Zdanowiecki, K. (2015). Digitalisierte Wirtschaft / Industrie 4.0, Gutachten der Noerr LLP im Auftrag des BDI zur rechtlichen Situation, zum Handlungsbedarf und zu ersten Lösungsansätzen, https://bdi.eu/media/themenfelder/digitalisierung/downloads/20151117_Digitalisierte_Wirtschaft_Industrie_40_Gutachten_der_Noerr_LLP.pdf, S. 23.

7 Die zeitliche Befristung unterscheidet diese Kategorie von der des Dateneigentums (analog zum Sacheigentum).

8 Hottelet, U. (2015). IT-Recht: Das Eigentum an Daten wird zur Stolperfalle für Unternehmen, automotiveIT – Business. Strategie. Technologie, 06/07 2015, http://www.it-rechtsinfo.de/wp-content/uploads/2015/07/automotiveIT.pdf, S. 31.

9 Bitkom (2014). Leitfaden Big-Data-Technologien – Wissen für Entscheider, https://www.bitkom.org/Bitkom/Publikationen/Big-Data-Technologien-Wissen-fuer-Entscheider.html, S. 149.

10 Schwartmann, R. und C.-H. Hentsch (2015). Eigentum an Daten – Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV (5): 221-230.

tenverwertungsrecht könnte außerdem die Regelung von Eigentumsanteilen im Falle von mehreren Eigentümern ermöglichen.[11]

Abweichend von den hier skizzierten Ansätzen halten einige Autoren „Dateneigentum“ für eine *Fehlkategorisierung* des Problems.

So wird darauf verwiesen, dass Daten, Informationen und Wissen jeweils *eigene Kategorien* darstellen, denen sich eigentumsanaloge Vorstellungen kaum überstülpen lassen.[12] Individualistische Zuschreibungen (von Informationen zu Parteien) liefen fehl, weil Informationen zwischen Menschen entstünden.[13] Datenschutz erfordere daher, so Albers, ein „Denken in sozialen Relationen, in Prozessen und in Kontexten“ und sei als Bündel von Rechtsbindungen und Rechtspositionen anzusehen.

Ganz ähnlich wird dies vom Bundesverfassungsgericht gesehen, wonach personenbezogene Informationen ein Abbild der sozialen Realität darstellen und *gerade nicht* dem Betroffenen alleine zugeordnet werden können.[14] Roßnagel beschreibt, dass informationelle Selbstbestimmung keineswegs ein „eigentumsähnliches Herrschaftsrecht über persönliche Daten“ begründe und auch nicht als Bündel von Verfügungsrechten (*property rights*) zu charakterisieren sei.[15] Informationelle Selbstbestimmung schütze Freiheit[16] und sei die Grundlage einer Kommunikationsordnung.

Der Rechtsprofessor Kilian konstatiert, dass klassisches Eigentum seit dem römischen Recht nur an körperlichen Gegenständen begründet wer-

11 Welchering, P. (2015). Bereitstellung persönlicher Informationen gegen Geld. In: Deutschlandfunk (online), http://www.deutschlandfunk.de/private-daten-bereitstellung-persoenlicher-informationen.684.de.html?dram:article_id=338239.

12 Albers, M. (2017). Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, Informationelle Selbstbestimmung im digitalen Wandel, In: Friedewald, M., Lamla, J., Roßnagel, A. (Hrsg.), S. 11-35.

13 Roßnagel (2007) bringt das Beispiel, dass Gesundheitsdaten weder Eigentum des Patienten noch des Arztes seien. Auch in der Forschung werden Daten als Multiple Subjects’ Personal Data bezeichnet (Gnesi et al. 2014).

14 BVerfGE 65, 1, 43 f. (Volkszählungsurteil).

15 Roßnagel, A. (2007). Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, http://library.fes.de/pdf-files/stabsabteilung/04548.pdf, S. 111.

16 BVerGE 65, 1 (44).

den könnte.[17] Möglicherweise ließe sich aber ein neues, *eigentumsähnliches Recht an personenbezogenen Daten* erkennen, das eigenständig neben Material- und Immaterialgüterrechten bestehe (sogenanntes *Persönlichkeitsrecht sui generis*).

Ökonomische Ansätze: Privat-, Club- oder Gemeingut?

Daten und Informationen entziehen sich gewissermaßen auch der ökonomischen Logik des Privatgutes, denn je nach Kontext können sie Eigenschaften von Clubgütern oder öffentlichen Güter besitzen. Bei Privatgütern ist es möglich, souverän über die Verwendung, Nutzung und Zerstörung zu bestimmen. Dies sind die sogenannten „Monopolrechte" gegenüber Dritten. Klassischerweise als Konzept auf physische Güter angewandt, können andere Parteien von der Nutzung eines Privatgutes ausgeschlossen werden.

Bei Clubgütern hingegen können Dritte von der Nutzung (aufgrund rechtlicher, organisatorischer oder technischer Maßnahmen) ausgeschlossen werden. Dies wäre beispielsweise der Fall bei Kreditauskunfteien, die das Prinzip der *closed user group* umsetzen. Der Ausschluss Dritter ist aber *nie perfekt*, wie u. a. Hackerangriffe oder andere Datenlecks zeigen.[18] Bei öffentlichen Gütern reduziert der Konsum nicht die verfügbare Menge der Ressource für andere Marktteilnehmer (sogenannte Nicht-Rivalität). Zusätzlich lassen sich andere nur unter hohen Kosten oder gar nicht vom Konsum ausschließen (sogenannte Nicht-Ausschließbarkeit). Beispiele wären Luft oder öffentliche Sicherheit.

Öffentliche Güter werden auch als Gemeingüter oder Kollektivgüter bezeichnet. Für sie gilt, dass über den Markt *keine Bereitstellung der optimalen Menge* möglich ist, da auf beiden Marktseiten multiple Anreizprobleme bestehen (zum Beispiel Externalitäten oder Freifahrertum). Auch ergeben sich über Marktmechanismen keine Selbstkorrekturtendenzen.[19] Beispielsweise

17 Quelle: Eigentum an personenbezogenen Daten? Ein Denkanstoß von Herrn Prof. em. Dr. Dr. hc. Wolfgang Kilian im Rahmen der Vorlesung Informationsrecht, https://www.uni-muenster.de/Jura.itm/hoeren/eigentum-an-personenbezogenen-daten-ein-denkanstoss-von-herrn-prof-em-dr-dr-hc-wolfgang-kilian-im-rahmen-der-vorlesung-informationsrecht.

18 Für die Unmöglichkeit 100% IT-Sicherheit zu garantieren gibt es extrem viele Beispiele, unter anderem die Datenlecks großer IT-Firmen wie Uber, Yahoo, Target und Equifax.

19 Die Entscheidung über die Erstellung öffentlicher Güter ist in Demokratien im Regelfall das Ergebnis eines kollektiven Willensbildungsprozesses.

erlauben persönliche Daten Rückschlüsse auf das betroffene Datensubjekt und *gleichzeitig* auch Rückschlüsse auf Unbeteiligte (sogenannte Informationsexternalitäten).[20] Dies wird untenstehend näher erläutert.

Neue Ansätze konzipieren die Privatsphäre als öffentliches ‚Gut' (sogenanntes *public good* oder *privacy commons* genannt)[21] und die Reduktion derselben als öffentliches ‚Schlecht' (*public bad*).[22] Einzelpersonen können durch monetäre Kompensation allerdings jederzeit zur Preisgabe von Daten veranlasst werden. Dies ist selbst dann der Fall, wenn durch die Preisgabe des Einzelnen Marktdynamiken entstehen, die zur kompletten Auflösung der Privatsphäre aller führen. Die Preisgabe eines immer präziseren Persönlichkeitsprofils ungeahnter Tiefe[23] könnte letzten Endes in die sogenannte ‚Scoring Society' führen, in der jeder zu verschiedenen Zwecken permanent gescored wird. Aus der Logik dieser Ansätze würde man die Schaffung eines Dateneigentums entweder ablehnen oder dessen Limitierung fordern, wo das öffentliche Gut „Privatsphäre" unterminiert wird.

Dateneigentum impliziert also nicht automatisch effiziente Märkte, da Daten durchaus Eigenschaften öffentlicher Güter besitzen, selbst wenn Unternehmen technische Absicherungen vornehmen. Insgesamt gesehen stehen und fallen die Eigenschaften von persönlichen Daten als Informationsgüter mit den technischen, administrativen und rechtlichen Absicherungen. Hin-

20 Jentzsch, N. (2007). Financial Privacy – An International Comparison of Credit Reporting Systems, Springer-Verlag, Heidelberg), 2nd Revised Edition.

21 Privatsphäre wird von Schwartz (2004: 2089) als Raum anonymer Transaktionen definiert, der über Restriktionen hergestellt wird, welche die Verfügbarkeit von Daten limitieren, s. Schwartz, P.M. (2004). Property, Privacy, and Personal Data, Harvard Law Review 117 (2055): 2056-2128.

22 Fairfield, J. und C. Engel (2015). Privacy as a Public Good, 65 Duke Law Journal 385: 389–390, S. 385; Peppet, S.R. (2011). Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future. Northwestern University Law Review 105: 1153-1204.

23 So können aufgrund einiger weniger Facebook Likes bestimmte Charaktereigenschaften von Personen, darunter politische Präferenzen und sexuelle Orientierung, prognostiziert werden, Kosinski, M. D. Stillwella und T. Graepel (2013). Private traits and attributes are predictable from digital records of human behavior, PNAS 110 (15): 5802 – 5805.

zu kommt, dass der Wert von Daten kaum objektiv feststellbar ist und nach Marktmechanismus und Verkaufspartei variiert.[24]

Dateneigentum: Technisch umsetzbar?

Bei den technischen Ansätzen sollten zwei Ebenen, die ineinander übergreifen, unterschieden werden. Die eine Ebene ist die der Data Governance im Einzelunternehmen. Die andere ist die der Implementierung dieser Governance über Verfügungs- und Zugriffsrechte auf IT-Systemebene. Dort ist es möglich, Zuweisung von Verfügungsrechten an Mitarbeiter vorzunehmen, die allerdings unabhängig von juristischen Zuschreibungen sind und am Besten als ‚unechte Eigentumsrechte' charakterisiert werden.

Zur Data Governance in Unternehmen gehört beispielsweise die Festlegung von Rollen der Mitarbeiter. Beispiele hierfür sind „Dateneigentümer" (*data owner*) oder „Datenverwalter" (*data steward*). ‚Eigentum' weist einer Person (oder einer Personengruppe) im Unternehmen die Entscheidungsbefugnis über die Daten zu, um Verantwortlichkeiten herzustellen. Wie gesagt, dies ist nicht mit Eigentum im *juristischen Sinne* zu verwechseln.

Auf dieser Ebene wird wie folgt unterschieden:[25]

> **Zentralisiertes Eigentümer-Modell *(centralized ownership model)***:
> Eine Person oder eine Personengruppe erhält die Eigentümerrolle für die gesamten Datenressourcen eines Unternehmens. Es entsteht ein zentraler Kontrollpunkt.
>
> **Dezentralisiertes Eigentümer-Modell *(decentralized ownership model)***:
> Hier werden die Eigentümerrollen verschiedenen Personen oder Personengruppen zugewiesen. Es entstehen mehrere Kontrollpunkte.

Solche Befugnisse müssen in IT-Systemen über Authentifizierungs- und Autorisierungsprotokolle umgesetzt werden, in Hadoop beispielsweise über

24 Ein Überblick über Experimentalmethoden, Marktpreise und andere Methoden der Wert- und Preisevaluation findet sich in Jentzsch, N. (2016). State-of-the-Art of the Economics of Cyber-Security and Privacy. IPACSO Deliverable 4.1. Waterford Institute of Technology, February, https://www.econstor.eu/dspace/bitstream/10419/126223/1/Jentzsch_2016_State-Art-Economics.pdf.

25 Siehe auch SearchData Management (2018), Data governance: Information ownership policies and roles explained, http://searchdatamanagement.techtarget.com/feature/Data-governance-Information-ownership-policies-and-roles-explained.

das Kerberos-Protokoll. Hierbei wird der Nutzer dem System gegenüber authentifiziert und die von ihm verwendeten Dienste autorisiert. Dies erlaubt eine technische Umsetzung der zugeschriebenen Rollen und der Verfügungsrechte über die Daten.

In diesem Zusammenhang kann erwähnt werden, dass durch Anwendungen wie *Cloudera Navigator* automatisch die gesamten Audit Logs einer Plattform gesammelt werden können. Dies ermöglicht die Erstellung eines Dashboards, mit dem die Datennutzung im Unternehmen nachvollziehbarer wird.[26] Ein solches Dashboard kann potentiell auch externen Parteien zugänglich gemacht werden und die Transparenz von Vorgängen im Unternehmen erhöhen.

Für die unternehmensinterne Data Governance sind Herkunftsnachweise von Daten wichtig. Herkunftsnachweis kann administrativ oder technisch umgesetzt werden. So existiert ein Forschungszweig zu kryptographischen Herkunftsnachweisen. Als technischer Ansatz soll hier nur ein Konzept quasi exemplarisch genannt werden: Das ISAEN-Konzept.[27] Dieses Konzept soll eine Kontrolle der persönlichen Daten ermöglichen. Sie werden hierzu mit Hash-Werten versehen, die keine Identifizierung des Datensubjekts erlauben. Dann werden Datentransaktionen mit einer auf der BlockChain basierenden Technologie protokolliert. Der Nutzer kann von nun an Zugriffe auf seine Daten autorisieren.

Die Meinungen, ob sich Eigentümerrechte technisch umfassend umsetzen lassen, gehen unter Experten weit auseinander. Auf Unternehmensebene lassen sich Verfügungsrechte zwar implementieren, aber ein *unternehmensübergreifendes Management* von Verfügungsrechten ist derzeit nicht möglich, da einheitliche Standards (u.a. des Identitätsmanagements) fehlen. Ein solches Management könnte unter Anwendung von BlockChain-basierten Technologien stattfinden, die allerdings von einigen Experten für unreif gehalten werden. Andere bezweifeln ihre Eignung für hochfrequente Transaktionen. Auch gibt es keinen global integrierten Grid des Identitätsmanagements (sogenanntes *identity grid*). Eine Zentralisierung der Transaktionen persönlicher Daten und Informationen, bzw. ihre zentrale Kontrolle, kann derzeit also nicht stattfinden.

---

26 Die Autorin bedankt sich bei Michael Mock (Fraunhofer IAIS) für diesen Hinweis.

27 ISAEN (Individual Personal Data Audible Adress), die Autorin bedankt sich bei Benjamin Güldenring (FU Berlin) für diesen Hinweis. Quelle: ftp://ftp.cencenelec.eu/CEN/News/2016/WS/ISAEN/ProjectPlan-20160620.pdf.

Erosion der Privatsphäre durch Marktdynamik

Das ökonomische Eigeninteresse Einzelner an der Preisgabe persönlicher Daten kann zu einer Marktdynamik führen, in der Verbraucher unter den Druck geraten, ihre Daten preisgeben zu „müssen." In der wirtschaftswissenschaftlichen Forschung ist dieses Phänomen als ‚*Unraveling*'-Gleichgewicht bekannt, also ein Gleichgewicht, in dem die Privatsphäre erodiert beziehungsweise sich auflöst.[28] Der Grund hierfür ist, dass manche Kunden bestimmte Eigenschaften über sich signalisieren wollen, zum Beispiel ein geringes Versicherungs- oder Kreditrisiko. Das kann dazu führen, dass alle anderen, die dies nicht tun (wollen) mit ‚schlechten Risiken' im Markt gepoolt werden. Es wird dann zur dominanten Strategie des Einzelnen, Angaben über sich preiszugeben, um sich von anderen, vermeintlich schlechteren Kunden, zu differenzieren. Ein Beispiel soll dies veranschaulichen:

> Eine Versicherungsfirma bietet Fitness-Tracker an, die Kunden tragen können, um nachzuweisen, wie gesund sie leben.[29] Auf Basis dieser Daten – biometrische Informationen, Gesundheits- und Lifestyledaten – kann die Versicherung personalisierte Versicherungsprämien setzen. Menschen mit gesünderem Lebensstil wird ein Preisnachlass gewährt. Der Sportlichste und Gesündeste im Pool der potentiell Versicherbaren wird bei diesem Angebot zugreifen, um den Preisnachlass zu erhalten. Der Zweitsportlichste sieht dies voraus, er erhält vielleicht nicht den gleichen Preisnachlass wie der Sportlichste, will sich aber trotzdem von den unsportlicheren Menschen unterscheiden. Auch er greift zu.

28 Grossman, S.J. und O.D. Hart (1980). Disclosure Laws and Takeover Bids, The Journal of Finance 35 (2): 323-334; Hermalin, B.E. und M.L. Katz (2006). Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy. Quantitative Marketing and Economics 4 (3): 209–39; Peppet, S.R. (2011). Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future. Northwestern University Law Review 105: 1153-1204.

29 Olson, P. (2014). Wearable Tech Is Plugging Into Health Insurance, Forbes (June 19, 2014) https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#6a7ec6bb18bd.

> So verfährt jeder weitere Neukunde. Theoretisch gesehen kommt der Prozess dann zum Stillstand, wenn alle ihre Informationen offengelegt haben.[30]

Die individuell rationale Entscheidung für eine Preisgabe von Informationen führt über die Externalität der Einzelhandlung auf Unbeteiligte[31] zu einem kollektiven Zwang der Preisgabe. Die Verbraucher geraten in eine Zwickmühle: Keine Informationen preiszugeben ist ein Signal, sie preiszugeben auch.

Das Phänomen ist theoretisch und empirisch nachgewiesen, auch wenn es in experimentellen Märkten im Labor nicht zur vollständigen Auflösung der Privatsphäre aller kommt, wie weiter unten erläutert wird.

Nach Peppet ist *Unraveling* unter bestimmten Bedingungen möglich. Zum einen muss es sich um *verifizierbare Informationen* handeln und Mimikry ein Ding der Unmöglichkeit sein.[32] In dem hier beschriebenen Kontext heißt dies, dass sich keiner als sportlich darstellen kann, obwohl er es nicht ist. Durch die Erfassung biometrischer Daten durch Endgeräte (u.a. Wearables) ist Mimikry tatsächlich quasi unmöglich.[33] Auch wenn sich dies zunächst wie ein antiutopisches Gruselmärchen anhört, gibt es in der Realität bereits Geschäftsmodelle, die das Potential haben, *Unraveling*-Tendenzen zu befördern:

Pay-as-you-drive (PAYD): Versicherungsunternehmen nutzen zunehmend Telematik (Blackboxen, Apps), um das Fahrverhalten von Versicherten zu vermessen und verhaltensbasierte, individuelle Tarife zu setzen. So werden Daten über Bremsverhalten, Geschwindigkeiten und Uhrzeiten der Fahr-

30 Dies gilt auch für wettbewerblich organisierte Märkte, in denen Preise und Produkte personalisiert werden. Dazu ausführliche Diskussion in Jentzsch, N. (2017b). Wohlfahrts- und Verteilungsaspekte personalisierter Preise und Produkte, Untersuchung, Modellen und Strategien der Personalisierung, http://library.fes.de/pdf-files/wiso/13457-20170704.pdf.

31 In der technischen Literatur wird dies unter dem Begriff des „Inferenz-Risikos“ diskutiert, s. Acs, G., C. Castelluccia, D. Le Métayer (2016). Testing the robustness of anonymization techniques: acceptable versus unacceptable inferences – Draft Version, https://fpf.org/wp-content/uploads/2016/11/Acs_CL-DPL16-v4.pdf.

32 Peppet, S.R. (2011). Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future. Northwestern University Law Review 105: 1153-1204.

33 Smedley, T. (2015). Wearables could make it impossible to keep your hangover secret at work, The Guardian (30.9.2015), https://www.theguardian.com/sustainable-business/2015/sep/30/wearables-companies-smart-devices-health-wellbeing-privacy.

ten gesammelt.[34] Fahrer können über diese Daten gescored werden. Um sich von schlechten und riskanten Fahrern zu unterscheiden, würden die guten Fahrer für PAYD-Tarife optieren. Allerdings dürfte es in dem Zusammenhang nur eine Frage der Zeit sein, bis diese Daten auch zur psychometrischen Vermessung der Fahrer benutzt werden, da die Einwilligung eine ‚alles-oder-nichts' Entscheidung ist.

Personal Information Management Platforms (PIMS): Diese Plattformen versprechen Nutzern den Rückgewinn ihrer Souveränität, also der Verfügungshoheit über persönliche Daten durch eigenverantwortliches Einwilligungsmanagement. Dies wird ausführlich in Jentzsch (2017a) diskutiert.[35] PIMS sollen es Nutzern erlauben, ihre Daten zu zentralisieren,[36] im Dashboard darzustellen oder sie an ausgewählte Parteien zu übermitteln/zu verkaufen. Das damit entstehende allumfassende Datenprofil wird von Peppet als „Persönlichkeits-Prospekt" bezeichnet. Die Existenz eines solchen Profils sieht er als eine notwendige Bedingung für das Auslösen der Erosionstendenzen. Mit der Bereitstellung dieses persönlichen ‚Big Data' Speichers durch PIMS können Unternehmen Verträge schreiben, die Nutzer incentivieren, den Zugriff auf ihre Daten zu erlauben, um billigere Handy-Tarife, Kreditkartendeals oder Versicherungsverträge zu bekommen.

Insurance Technology (InsurTech): Unterschiedliche Versicherungsunternehmen bieten bereits jetzt verhaltensbasierte Versicherungstarife an. So führte die italienische Versicherung Generali in Deutschland 2016 ihre

34 Fahrer können auf Basis einer relativ kurzen Zeitspanne anhand ihres Fahrverhaltens eindeutig identifiziert werden, s. Enev, M., A. Takakuwa, K. Koscher und T. Kohno (2016). Automobile Driver Fingerprinting, Proceedings on Privacy Enhancing Technologies 2016 (1): 34–51; und Greenberg, A. (2016). A Car's Computer Can 'Fingerprint' You in Minutes Based on How You Drive, Wired, https://www.wired.com/2016/05/drive-car-can-id-within-minutes-study-finds/.

35 Jentzsch, N. (2017a). „Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds" – Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz, Gutachten für die Stiftung Datenschutz, https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Gutachten_Die_persoenliche_Datenoekonomie_Anhang_2_final.pdf.

36 Darunter Versicherungs- und Bankdaten, Profile aus Elektrizitäts- oder Wasserversorgern und aus sozialen Netzen wie Facebook, LinkedIn und Twitter.

Vitality-Tarife ein.[37] Für diese Kombination aus Berufsunfähigkeits-, Erwerbsunfähigkeits- oder Risikolebensversicherung werden Daten wie Besuche von Fitness-Studios, Gesundheitstests und Lebensmittelkonsum gesammelt. Gesündere und aktivere Menschen bekommen Gutscheine (zum Beispiel für einen Café Latte) und unter bestimmten Umständen auch bessere Preise auf ihre Versicherungspolice. Ein weiteres Beispiel ist das US-amerikanische Unternehmen Oscar. Es verteilt Fitness-Tracker an Versicherte. Ein Algorithmus errechnet auf Basis der Daten, unter anderem wie viele Schritte eine Person pro Tag machen sollte.[38]

Es ist beobachtbar, dass die Incentivierung der Datenpreisgabe zunächst einer positiven Logik folgt (‚Gesundheitsprogramm', bzw. ‚Belohnung verantwortungsvoller Fahrer'). Allerdings kann nicht ausgeschlossen werden, dass Unternehmen die Daten auch nutzen, um unprofitable Kunden loszuwerden (sogenanntes *customer divestment*), Produkte zu personalisieren, Preise zu erhöhen oder Kunden psychometrisch zu vermessen, um psychologische Schwächen auszunutzen und ihnen das *next best offer* zu machen.

Rechtliche Ansätze gegen Erosionstendenzen

Rechtlich gesehen gibt es zwei Ansätze, die Erosionstendenzen entgegenwirken: (1) die Einschränkung der Nutzung bestimmter persönlicher Informationen und (2) ein Totalverbot der Erschließung und Nutzung bestimmter Daten (zum Beispiel des genetischen Codes).

In Europa gibt es eine Reihe von Informationskategorien, die in der EU-Datenschutzgrundverordnung besonderen Schutz zu genießen scheinen. So wird die Verarbeitung von Informationen über rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen oder der Genetik oder Biometrie sowie der Gesundheit in Art.9, Abs. 1 der EU-DS-GVO[39] zunächst untersagt, um sie dann einer ganzen Reihe von Ausnahmen

37 Frankfurter Allgemeine Zeitung (2016). Joggen für die geringe Versicherungsprämie, http://www.faz.net/aktuell/finanzen/meine-finanzen/versichern-und-schuetzen/versicherer-generali-fuehrt-vitality-tarife-in-deutschland-ein-14299998.html.

38 Lapowsky, I. (2014). This Insurance Company Pays People to Stay Fit, Wired Business (12.08.2014), https://www.wired.com/2014/12/oscar-misfit/.

39 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

zu unterwerfen. Eine dieser Ausnahmen, vielleicht die wichtigste, ist, dass solche Informationen mit der ausdrücklichen Einwilligung des Betroffenen verarbeitet werden können (Art. 9, Abs. 2 (a)). Eine Einwilligungserklärung, selbst wenn diese freiwillig auf informierter Basis abgegeben wurde, ist aber keine Grundlage für Souveränität und *schützt nicht* vor der Erosion der Privatsphäre.

Auch in den USA gibt es Regelungen gegen die Nutzung bestimmter sensibler Informationskategorien. Sie sollen eine ökonomische Diskriminierung verhindern.[40] Im *Fair Credit Reporting Act* existiert beispielsweise ein Verbot für *Consumer Reporting Agencies* (Kreditauskunfteien) medizinische Informationen weiterzugeben (§ 604 - 15 U.S.C. § 1681b, g, (1)). Auch dieses Verbot wird durch Ausnahmeregelungen wie die Einwilligung quasi ausgehebelt. Es ist realistisch anzunehmen, dass manche Unternehmen ein Interesse am genetischen Code haben. In den USA hat man versucht, Diskriminierung auf der Basis des Codes vorzubeugen. So verbietet der *Genetic Information Nondiscrimination Act* (29 CFR Part 1635) Arbeitgebern, genetische Information zu erfragen, zu verlangen oder diese anzukaufen.[41] Dies gilt auch für genetische Familiengeschichten. Nur in bestimmten Ausnahmefällen, beispielsweise als Teil eines vom Arbeitgeber angebotenen Gesundheitsdienstes, kann der Arbeitgeber genetische Daten auf freiwilliger Basis erfragen. Dies soll Situationen vorbeugen, die von Machtasymmetrien gekennzeichnet sind und in denen Personen Anfragen nach ihren Daten kaum abschlägig beantworten können.

Ökonomische Erkenntnisse zu Erosionstendenzen

Grundsätzlich handelt es sich bei dem hier benannten Erosionsproblem um ein Phänomen, das sich aus den Informationsasymmetrien zwischen Marktparteien ergibt. In der Vergangenheit stellten sich diese Asymmetrien so dar, dass beispielsweise eine Versicherung ein unvollständiges Bild über das Risiko eines Neukunden hatte. Informationsasymmetrien werden in der öko-

40 „Verbotene Variablen“ (sogenannte prohibited bases) könnten allerdings durch andere Variablen in Datensätzen reflektiert werden, dazu Barocas und Selbst (2015).

41 Genetische Information wird als irrelevant für die Arbeitsleistung angesehen, s. U.S. Equal Employment Opportunity Commission (s. https://www.eeoc.gov/laws/types/genetic.cfm).

nomischen Theorie unter anderem mit Signalspielen modelliert.[42] Hermalin und Katz zeigen im Übrigen mit ihrem Modell, dass es egal ist, bei welcher Marktpartei die Verfügungsrechte über Informationen verankert werden. Zur Erosion der Privatsphäre wird es unter verschiedenen Eigentumsregimen kommen.

Empirisch gesehen gibt es nur vereinzelte Arbeiten, die das Phänomen in Laborexperimenten untersuchen.[43] Diese Experimente zeigen, dass der Auflösungsprozess in Gang kommt. Die Rate der Offenlegung durch die Experimentalteilnehmer fällt allerdings geringer aus als theoretisch vorhergesagt. Sie liegt bei 40 bis 60 Prozent. Insbesondere, wenn es sich um einen sensiblen Kontext wie Gesundheit handelt, reduzieren sich die Effekte. Die Autoren erklären dies unter anderem mit den in ihrem Experiment als hoch angenommenen Verifikationskosten (Kauf eines teuren Gesundheitszertifikats). Des Weiteren kommt es nur mit rationalen Spielern in der Theorie zur kompletten Auflösung der Privatsphäre. Menschen in Märkten handeln aber bekanntermaßen nicht immer rational.

Die Preisgabe persönlicher Daten erhöht theoretisch gesehen die allokative Effizienz im Markt.[44] Allerdings lässt diese Beobachtung keine Schlüsse über die Fairness oder Gerechtigkeit der resultierenden Ressourcenverteilung zu. In der Forschung sind derzeit keine Ansätze erkennbar, die zeigen, wie durch Technologie Individuen *in ihrem Wahlverhalten* so beeinflusst werden können, dass sie das soziale Gut Privatsphäre nicht dem eigenen ökonomischen Vorteil opfern.

42 Grossman, S.J. und O.D. Hart (1980). Disclosure Laws and Takeover Bids, The Journal of Finance 35 (2): 323-334; Hermalin, B.E. und M.L. Katz (2006). Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy. Quantitative Marketing and Economics 4 (3): 209–39.

43 Benndorf, V., D. Kübler und H.-T. Normann (2015). Privacy Concerns, Voluntary Disclosure of Information, and Unraveling: An Experiment, European Economic Review 75 (2015): 43–59.

44 Informationen werden ihren produktivsten Zwecken zugeführt, es gibt keine Fehlallokationen von Ressourcen.

Schluss

Ein zentrales Thema der Datenökonomie ist die Ausgestaltung der Verfügungsrechte über persönliche Daten. In diesem Impuls soll aus der Vogelperspektive ein neuer Blick auf das Thema eröffnet werden. Hierzu werden rechtliche, ökonomische und technische Ansätze zusammengeführt. So lässt sich manch erhellende Einsicht gewinnen: Juristisch gesehen entstehen Daten und Informationen in sozialen Relationen und lassen sich *gerade nicht* einer Partei zuordnen.

Die Einführung eines Dateneigentums scheint auch ökonomisch gesehen kaum Sinn zu machen: Weder kann davon ausgegangen werden, dass Märkte dadurch effizienter funktionieren, noch dass die richtigen Innovationsanreize gesetzt werden. Das Thema scheint vielmehr ein datenpolitischer Wiedergänger, der sich bei näherem Hinschauen als Pseudo-Lösung entpuppt.

Selbst aus Verbrauchersicht würde eine Verankerung von Eigentumsrechten aufgrund der Marktdynamiken keine Garantie für mehr Privatsphäre darstellen, ganz abgesehen von der Administrierbarkeit. Dateneigentum stärkt *nicht automatisch* die Souveränität des Dateneigentümers. Dies sind nur einige der Gründe, warum es kaum Stimmen innerhalb von Fachkreisen gibt, die Dateneigentum tatsächlich protegieren.

Unabhängig vom Dateneigentum scheinen wir zunehmend in Marktdynamiken zu geraten, bei denen die Offenlegung persönlicher Daten unter Zugzwang geschieht. Dies ist insbesondere dort der Fall, wo sich durch umfassende Datenpreisgabe ein vermeintlich „guter Deal“ machen lässt, wie in der Versicherungswirtschaft. Hier muss unbedingt eine gesellschaftliche Diskussion darüber stattfinden, ob dies für bestimmte Informationssegmente gesellschaftlich erwünscht ist, für andere aber dagegen nicht.

Statt sich auf Dateneigentum zu fokussieren, sollte die Politik andere Ansätze verfolgen und fördern, insbesondere technische Ansätze für Datenschutz und -kontrolle. Hierzu gehört unter anderem die Forschung im Bereich der Visualisierung von Datenverarbeitungsvorgängen für Verbraucher und Aufsichtsbehörden und die Förderung von Projekten zu kryptographischen Herkunftsnachweisen von Daten.

Auch wenn wir am Anfang der gesellschaftlichen Debatte einer neuen Datenpolitik stehen, zeigt das Beispiel des Dateneigentums, dass es an der Zeit ist, ernsthaft interdisziplinär an solche Themen heranzugehen. Pseudo-Lö-

sungen müssen schneller erkannt und verworfen werden, damit wir in der Entwicklung einer sinnvollen Datenpolitik für Deutschland endlich vorankommen.

Referenzen

Acs, G., C. Castelluccia, D. Le Métayer (2016). Testing the robustness of anonymization techniques: acceptable versus unacceptable inferences – Draft Version, https://fpf.org/wp-content/uploads/2016/11/Acs_CL-DPL16-v4.pdf.

Albers, M. (2017). Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, Informationelle Selbstbestimmung im digitalen Wandel, In: Friedewald, M., Lamla, J., Roßnagel, A. (Hrsg.), S. 11-35.

Arbeitsgruppe "Digitaler Neustart" (2017). Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder - Bericht vom 15. Mai 2017, https://www.justiz.nrw/JM/schwerpunkte/digitaler_neustart/index.php.

Barocas, S. und A.D. Selbst (2015). Big data's disparate impact, SSRN Scholarly Paper, Rochester, Social Science Research Network, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899 .

Benndorf, V., D. Kübler und H.-T. Normann (2015). Privacy Concerns, Voluntary Disclosure of Information, and Unraveling: An Experiment, European Economic Review 75 (2015): 43–59.

Bitkom (2014). Leitfaden Big-Data-Technologien – Wissen für Entscheider, https://www.bitkom.org/Bitkom/Publikationen/Big-Data-Technologien-Wissen-fuer-Entscheider.html.

BMVI (2017). „Eigentumsordnung" für Mobilitätsdaten? - Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive, https://www.bmvi.de/SharedDocs/DE/Publikationen/ DG/eigentumsordnung-mobilitaetsdaten.html?nn=12830 .

Enev, M., A. Takakuwa, K. Koscher und T. Kohno (2016). Automobile Driver Fingerprinting, Proceedings on Privacy Enhancing Technologies 2016 (1): 34–51.

Fairfield, J. und C. Engel (2015). Privacy as a Public Good, 65 Duke Law Journal 385: 389–390.

Gnesi S., Matteucci I., Moiso C., Mori P., Petrocchi M. und M. Vescovi (2014). My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Sub-

jects Personal Data. In: Preneel B., Ikonomou D. (eds) Privacy Technologies and Policy. APF 2014. Lecture Notes in Computer Science, vol 8450. Springer.

Greenberg, A. (2016). A Car's Computer Can 'Fingerprint' You in Minutes Based on How You Drive, Wired, https://www.wired.com/2016/05/drive-car-can-id-within-minutes-study-finds/.

Grossman, S.J. und O.D. Hart (1980). Disclosure Laws and Takeover Bids, The Journal of Finance 35 (2): 323-334.

Hermalin, B.E. und M.L. Katz (2006). Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy. Quantitative Marketing and Economics 4 (3): 209–39.

Hottelet, U. (2015). IT-Recht: Das Eigentum an Daten wird zur Stolperfalle für Unternehmen, automotiveIT – Business. Strategie. Technologie, 06/07 2015, http://www.it-rechtsinfo.de/wp-content/uploads/2015/07/automotiveIT.pdf.

Jentzsch, N. (2017a). „Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds" – Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz, Gutachten für die Stiftung Datenschutz, https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Gutachten_Die_persoenliche_Datenoekonomie_Anhang_2_final.pdf.

Jentzsch, N. (2017b). Wohlfahrts- und Verteilungsaspekte personalisierter Preise und Produkte, Untersuchung, Modellen und Strategien der Personalisierung, http://library.fes.de/pdf-files/wiso/13457-20170704.pdf.

Jentzsch, N. (2016). State-of-the-Art of the Economics of Cyber-security and Privacy. IPACSO Deliverable 4.1. Waterford Institute of Technology, February, https://www.econstor.eu/dspace/bitstream/10419/126223/1/Jentzsch_2016_State-Art-Economics.pdf.

Jentzsch, N. (2007). Financial Privacy – An International Comparison of Credit Reporting Systems, Springer-Verlag, Heidelberg), 2nd Revised Edition.

Kosinski, M. D. Stillwella und T. Graepel (2013). Private traits and attributes are predictable from digital records of human behavior, PNAS 110 (15): 5802 – 5805.

Litman, J. (2000). Information Privacy/Information Property. Stanford Law Review (online), http://www-personal.umich.edu/~jdlitman/papers/infopriv acy.pdf.

Samuelson, P. (2000). Privacy as Intellectual Property? Stanford Law Review 52 (5): 1125–1174.

Schaufenster Elektromobilität (2016). EP21: Zivil- und datenschutzrechtliche Zuordnung von Daten vernetzter Fahrzeuge, http://schaufenster-elektromobilitaet.org/de/content/dokumente/dokumente_1/dokument_details_18432.html.

Schwartmann, R. und C.-H. Hentsch (2015). Eigentum an Daten – Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV (5): 221-230.

Schwartz, P.M. (2004). Property, Privacy, and Personal Data, Harvard Law Review 117 (2055): 2056-2128.

Westin, A. (1967). Privacy and Freedom (Athenum: New York).

Welchering, P. (2015). Bereitstellung persönlicher Informationen gegen Geld. In: Deutschlandfunk (online) http://www.deutschlandfunk.de/private-daten-bereitstellung-persoenlicher-informationen.684.de.html?dram:article_id=338239.

Peppet, S.R. (2011). Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future. Northwestern University Law Review 105: 1153-1204.

Roßnagel, A. (2007). Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, http://library.fes.de/pdf-files/stabsabteilung/04548.pdf.

Zdanowiecki, K. (2015). Digitalisierte Wirtschaft / Industrie 4.0, Gutachten der Noerr LLP im Auftrag des BDI zur rechtlichen Situation, zum Handlungsbedarf und zu ersten Lösungsansätzen, https://bdi.eu/media/themenfelder/digitalisierung/downloads/20151117_Digitalisierte_Wirtschaft_Industrie_40_Gutachten_der_Noerr_LLP.pdf.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern die Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über die Autorin

Nicola Jentzsch ist Leiterin des Datenökonomie-Projekts der Stiftung Neue Verantwortung. Sie ist eine Ökonomin, die Ansätze der Wettbewerbs- und Verhaltensökonomie im Gebiet Privatsphäre und Cybersicherheit verbindet. Im Datenökonomie-Projekt werden ökonomische, technische und juristische Aspekte analysiert, um innovative datenpolitische Ansätze zu entwickeln. Nicola forscht seit mehr als 15 Jahren zu verschiedenen Themen der Datenökonomie, derzeit arbeitet sie an Themen des Wettbewerbs in digitalen Märkten (Personalisierung), Datenschutz, sowie Big Data Analytics (Machine Learning, Privacy-Kriterien und Privacy-Garantien). Vor der Stiftung Neue Verantwortung arbeitete Nicola mehrere Jahre am DIW Berlin. Sie hat über Wettbewerb und Regulierung von Kreditauskunfteien an der Freien Universität Berlin am FB Wirtschaftswissenschaft promoviert und war Research Fellow an der Yale University und der Georgetown University.

Nicola hat in den vergangenen Jahren die Europäische Kommission, die Europäische Agentur für Netz- und Informationssicherheit (ENISA), die Weltbank und Zentralbanken in mehreren afrikanischen und asiatischen Ländern beraten. Sie ist Gewinnerin eines Google Research Awards. Ihre Forschung hat sie in internationalen ökonomischen Fachzeitschriften publiziert (u.a. IJIO, JEBO, JIMF).

So erreichen Sie die Autorin

Dr. Nicola Jentzsch
Projektleiterin Datenökonomie
njentzsch@stiftung-nv.de
+49 (0)30 81 45 03 78 92

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de