

VERBRAUCHER ALS „EIGENTÜMER“ VON MOBILITÄTSDATEN?

Stellungnahme zur BMVI-Studie „Eigentumsordnung für Mobilitätsdaten?“ vom 2. August 2017

27. November 2017

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Mobilität und Reisen

Markgrafenstraße 66
10969 Berlin

mobilitaet@vzbv.de

INHALT

I. ZUSAMMENFASSUNG	3
II. EINORDNUNG DER STUDIE	5
III. STELLUNGNAHME	6
1. Grundrechtsgeltung	6
2. Datenschutz	7
3. Anonymität und Personenbezug von Daten	9
4. Diskriminierung von durch Merkmale definierte Gruppen	11
5. Legitimer Anspruch auf ökonomischen Mehrwert?	12
6. Transparenz, demokratische und rechtliche Kontrolle	13
7. Weitere gesamtgesellschaftliche Aspekte	15
8. Weitere rechtliche Anpassungen statt Datengesetz	15

I. ZUSAMMENFASSUNG

Der Verbraucherzentrale Bundesverband (vzbv) begrüßt das Ziel der im Auftrag des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) erstellten und während des Zukunftsforums Datensouveränität am 2. August 2017 vorgestellten Studie "‘Eigentumsordnung‘ für Mobilitätsdaten?", Wege in Richtung eines neuen Datenrechts aufzuzeigen. Die Stellungnahme des vzbv nimmt eine verbraucher- und datenschutzpolitische Bewertung der Studie vor und benennt Defizite in der Behandlung des Themas sowie sich daraus ergebende Fragen.

Die Studie liefert einen guten und weitgehend umfassenden **Überblick** über die ökonomische und rechtswissenschaftliche Diskussion zum Thema „Dateneigentum“ in Deutschland. Sie beschränkt sich auf die Untersuchung, welche rechtlichen Defizite sie sieht, um digitale Daten unternehmerisch wirtschaftlich zu verwerten. Dieser Ansatz ist legitim und die Vorschläge sind diskussionswürdig.

Die Studie unternimmt nicht ausdrücklich den Versuch, digitale Grundrechte der Betroffenen oder auch speziell **Verbraucherbelange** sowie generell Gemeinwohlbelange zu beschneiden. Sie beschreibt im Detail, welche eigentumsähnlichen Bezüge zu Daten hergestellt werden können. Dabei verkürzt sie aber in ihren Schlussfolgerungen die rechtliche Verfügungsmacht der datenschutzrechtlich Betroffenen und negiert letztlich überhaupt die eigentumsähnliche Stellung der Betroffenen, während sie im Hinblick auf die Wirtschaft ein ökonomisches Potential, auch durch künftige Normierungen, bejaht. Nach Auffassung des vzbv bilden Datenschutz und Innovation keinen Gegensatz, sondern lassen sich vereinbaren. Datenschutz muss als ein Baustein in der Wertschöpfungskette digitaler Geschäftsmodelle verstanden werden.

Die Studie behandelt nur am Rande die Frage, wie im Fall von **widersprüchlichen Interessenlagen** umgegangen werden soll. Es wird lediglich ein rechtlicher Rahmen benannt. Dessen normative Konkretisierung wird aber vollständig der Politik überlassen, ohne dass durch das Verfassungsrecht vorgegebene Abwägungskriterien näher benannt werden.

Zu kurz kommen in der Studie **Allgemeinwohlbelange**, die bei einer Normierung von Verfügungsrechten über Daten umfassend berücksichtigt werden müssen.

Es muss verhindert werden, dass sich das „Recht des Stärkeren“ und das „Recht des Schnelleren“ durchsetzt.¹ Bei der Diskussion um Dateneigentum und um ein Datengesetz darf es letztlich nicht nur um Fragen ökonomischer Macht und Wertigkeit gehen, sondern es muss auch die Sozialpflichtigkeit der Daten im Auge behalten werden.

Wegen des Ungleichgewichts in dem Vertragsverhältnis zwischen Verbraucher² und Unternehmen ist es aber eine Illusion zu glauben, dass der Verbraucher insofern „gerechte Preise“ aushandeln könnte.

¹ Spiecker, Beilage 1 zu K&R Heft 7/8/2017, 4 f.

² Die gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

Die ökonomische Relevanz von (personenbeziehbaren) Verbraucherdaten ist evident und wird oftmals beschworen, jedoch wurden die Zusammenhänge bisher nur ansatzweise untersucht. Dies hat zur Folge, dass weder die Betroffenen noch staatliche Instanzen (zum Beispiel Kartell- und Steuerbehörden) eine valide Bewertung vornehmen können.

Die wissenschaftliche **Erforschung von datengetriebenen Geschäftsmodellen** sowie von deren möglicher Regulierung muss daher vorangebracht werden. Darüber hinaus muss die Aufklärung und Sensibilisierung der Verbraucher im Bereich Daten verstärkt werden.

Der Gesetzgeber muss verhindern, dass Unternehmen den Aufwand sozialisieren und die Gewinne privatisieren. Gerade im Kfz-Bereich werden die Kosten bisher von den Kfz-Nutzenden (Investition ins Auto, Kraftstoff, etc.) oder von der Allgemeinheit der Steuerzahler (Verkehrsinfrastruktur, digitale Infrastruktur, etc.) getragen und nicht von den Unternehmen, die diese Daten kommerziell für sich nutzen wollen.

Wegen ihrer hohen sozialen Relevanz besteht an diesen Daten ein hoher öffentlicher Informations- und Kontrollbedarf. In der Konsequenz hält der vzbv ein teilweise auch in Programmen politischer Parteien vorgesehenes **Datengesetz** letztlich für ungeeignet, um die Allgemeinwohlbelange sowie die persönlichkeitsrechtlichen und die ökonomischen Belange von Individuen adäquat abzubilden. Ein solches Gesetz kann der Komplexität der mit Daten verbundenen Rechtsbeziehungen nicht gerecht werden. Adäquat erscheint dagegen eine Weiterentwicklung der bestehenden Regelungen zu den Nutzungs- und Verfügungsrechten an Daten, mit denen keine Ausschließlichkeitsrechte hieran begründet werden. Bei diesen Nutzungsrechten wird schon heute differenziert zwischen den jeweiligen Datenarten, den Verarbeitungs- und Nutzungszwecken. Nur so kann der hohen Arbeitsteilung und Vernetzung entsprochen werden, wie sie generell in unserer Informationsgesellschaft und zunehmend auch im Kfz-Bereich bestehen.³ Statt ein neues Datengesetz braucht es Rechtsanpassungen an die Rahmenbedingungen digitaler Datenverarbeitung. Der Eigentumsbegriff führt dabei in die Irre.

Darüber hinaus sind aus datenschutz- und verbraucherschutzrechtlicher wie auch aus gesamtgesellschaftlicher demokratischer und rechtsstaatlicher Sicht Rechtsänderungen erforderlich:

- ❖ Normierung von Herstellerpflichten
- ❖ Der bisher rechtlich zugestandene Schutz von Daten als Betriebs- und Geschäftsgeheimnis oder auf der Grundlage des Urheberrechtes muss dahingehend modifiziert werden, dass Dritt- bzw. Gemeinwohlinteressen hinreichend Geltung verschafft werden kann
- ❖ Im Interesse der Verhinderung von Monopolstrukturen sind rechtliche Regelungen zu schaffen, die bei Erreichen einer bestimmten Marktmacht zum Teilen von verfügbaren Daten verpflichtet

³ Hilty, SZ 11.09.2017, S. 20.

- ❖ Etablierung einer transparenten Selbstregulierung im Kfz-IT-Bereich
- ❖ Festlegung von Standardisierungsverfahren und die Erarbeitung von Standards, zum Beispiel zur Sicherstellung der Kommunikationsfähigkeit der Kfz-IT-Systeme
- ❖ Festlegung von spezifischen Zulassungs- und Zertifizierungsverfahren für den Bereich der Kfz-IT.

II. EINORDNUNG DER STUDIE

Die im Auftrag des BMVI erstellte Studie knüpft an die Diskussion über die kommerzielle Nutzung von Daten, die im Rahmen der Digitalisierung aller Lebens- und Wirtschaftsbereiche entstehen, an, die seit einigen Jahren in Europa geführt wird. Sie ist geprägt vor der Wahrnehmung, dass insbesondere US-Unternehmen, mit der Digitalisierung **erfolgreiche Geschäftsmodelle** entwickelt haben und praktizieren (S. 71 f.)⁴. Diese inspirieren und provozieren deutsche und europäische Unternehmen sowie die Politik zu einer wirtschaftlichen beziehungsweise politischen Antwort. Grundidee ist, dass digitale Daten das „Öl des 21. Jahrhunderts“ sind, aus dem eine Wertschöpfung generiert werden soll und aber auch Allgemeinwohlaspekte vorangebracht werden sollen. Zentraler technischer Ansatz ist „Big Data“, also die Erfassung, Zusammenführung, komplexe Auswertung und (ökonomische) Nutzung großer Datenmengen.⁵ Während der Digitalmarkt im Internet und beim Mobile Computing weitgehend von US- und asiatischen Unternehmen dominiert wird, gehören deutsche Unternehmen in der Automobilbranche zu den Weltmarktführern. Diese Marktstellung soll dadurch bewahrt werden, dass erfolgreiche Geschäftsmodelle bei der Kfz-Digitalisierung etabliert werden.

Die Diskussion über Dateneigentum knüpft an der ökonomischen Verwertbarkeit digitaler Daten an. Diese Diskussion wird insbesondere unter dem Stichwort der „**Datensouveränität**“ geführt (S. 3, 78 ff.). Dieser Begriff ist (bisher) rechtlich nicht definiert und wird in unterschiedlichen Bedeutungszusammenhängen verwendet. Digitale Souveränität lässt Assoziationen zum Datenschutzrecht aufkommen sowie zum vom Bundesverfassungsgericht in der Volkszählungsentscheidung 1983 grundrechtlich begründeten „Recht auf informationelle Selbstbestimmung“⁶. Subjekt dieser informationellen Selbstbestimmung ist ausschließlich der von einer Datenverarbeitung erfasste oder erfassbare Mensch, dem der datenschutzrechtlich Verantwortliche als Datenverarbeiter gegenübersteht. Dagegen wird in der Studie das Subjekt der „Datensouveränität“ nicht eindeutig benannt; als deren Träger wird eher an das Daten verarbeitende Unternehmen im wirtschaftlichen Kontext gedacht (S. 3). Als Gegenpol wird oft der Betroffene mit seinen Datenschutzansprüchen genannt, aber auch ausländische Unternehmen,

⁴ Seitenangaben im vorliegenden Text beziehen sich auf die im Auftrag des BMVI erstellte Studie „Eigentumsordnung für Mobilitätsdaten?“

⁵ Kritisch hierzu Weichert/Schuler, Datenschutz contra Wirtschaft und Big Data?

⁶ BVerfG U. v. 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419 ff.

wie zum Beispiel Google, Facebook, Apple, Amazon oder Microsoft, sowie ausländische Geheimdienste mit Zugriff auf inländisch verarbeitete Daten wie zum Beispiel der US-Dienst National Security Agency (NSA).

Hinsichtlich der Datennutzung bestehen innerhalb der deutschen Wirtschaft **widersprüchliche Interessen**. Im Bereich der Kfz-Daten kann dieser Interessenwiderspruch dadurch gekennzeichnet werden, dass auf der einen Seite die Kfz-Hersteller stehen, die zumeist den ersten Zugriff auf Kfz-Daten haben. Dies ist jedenfalls dann der Fall, wenn die Kfz-Daten nicht nur im Auto selbst oder bei den jeweiligen Diensteanbietern gespeichert werden, sondern über die Server der jeweiligen Kfz-Hersteller geleitet und dort abgelegt werden. Dem stehen Unternehmen gegenüber, die im eigenen Interesse oder im (gegebenenfalls nur vermeintlichen) Interesse der Betroffenen Anspruch auf die Kfz-Daten erheben. So beanspruchen zum Beispiel Kfz-Hersteller die Daten aus Unfällen für sich, um den verunfallten Fahrer in eine Vertragswerkstätte des Herstellers zu lenken, während Kfz-Versicherungen mit Hilfe solcher Daten diese gerne in ihre Vertragswerkstätten lenken würden.⁷

III. STELLUNGNAHME

1. GRUNDRECHTSGELTUNG

Die Studie benennt zunächst korrekt wichtige, für die Datenverarbeitung möglicherweise relevante **Grundrechte** (Eigentumsrecht, Berufsfreiheit, Recht auf informationelle Selbstbestimmung, Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, Telekommunikationsgeheimnis, S. 43 f.). Nicht bzw. nur ganz am Rande erwähnt werden weitere bedeutende Grundrechte, wie zum Beispiel die Forschungsfreiheit und die Meinungsfreiheit (Art. 5 GG).

Verkürzt dargestellt wird die verfassungsrechtliche Sicht auf das bei der Kommerzialisierung im Vordergrund stehende **Verhältnis zwischen Privaten**, indem zwar auf die Drittwirkung der Grundrechte im Privatrechtsverkehr hingewiesen wird, diese gelte aber „allenfalls“, also nur besten- oder schlimmstenfalls? (S. 45). Angesichts des Ungleichgewichts der Vertragsparteien im Bereich der digitalen Daten ist diese zur eingeschränkten Ausnahme deklarierte Situation nach den Kriterien des Bundesverfassungsgerichts aber in der Praxis der Regelfall.⁸

Persönlichkeitsrechtliche Erwägungen werden demgegenüber vollständig ausgeblendet. Den eigenen Normvorschlag relativierend werden dann in der Studie kritische Erwägungen hierzu vorgetragen und eine eindeutige Positionierung vermieden (S. 109).

⁷ Versicherungswirtschaft und Autohersteller streiten um Daten, www.versicherungsbote.de 18.08.2017.

⁸ BVerfG, B. v. 23.10.2006 – 1 BvR 2017/02; MMR 2007, 93.

2. DATENSCHUTZ

Die Studie befasst sich generell mit datenbasierten Geschäftsmodellen und enthält damit Aussagen, die für personenbeziehbare wie auch für nicht-personenbeziehbare Daten gelten. Aus Verbraucher- und Datenschutzsicht besonders relevant sind die Geschäftsmodelle, die selbst personenbezogen sind oder zumindest **auf personenbeziehbaren Daten beruhen**. Es kommt nicht nur darauf an, ob das Geschäftsmodell gegenüber dem Verbraucher selbst personalisiert ist. Von hoher Relevanz sind auch Geschäftsmodelle, die auf personenbeziehbaren Daten beruhen, die im Rahmen der Verarbeitung mehr oder weniger wirksam anonymisiert wurden. Die ökonomische Werthaltigkeit, die letztlich auf das Verhalten von Betroffenen als Konsumenten zurückgeht, ist in all diesen Fällen unbestreitbar.

Die Diskussion, inwieweit **Verbraucher** Ihre Daten (zum Beispiel gegen unentgeltliche Nutzungsmöglichkeit eines Dienstes) **kommerziell vermarkten** können, wird schon seit vielen Jahren geführt (vgl. S. 48).⁹ Spiros Simitis war hiergegen mit einer grundrechtsdogmatischen Argumentation und dem Verweis auf die soziale und die Kommunikationsdimension des Rechts auf informationelle Selbstbestimmung viele Jahre erfolglos zu Felde gezogen.¹⁰ Tatsächlich findet seit Jahren in einem riesigen Marktsegment (insbesondere bei Telemediendiensten) ein solcher vertraglicher Austausch statt. Dieser muss für die Betroffenen nicht schädlich sein. Es kann im Interesse des Betroffenen liegen, dass Dritte ihre Daten kommerziell nutzen. So kann es zum Beispiel im Betroffeneninteresse liegen, dass durch diese Nutzung eine Qualitätsverbesserung der Produkte erfolgt oder Betroffene – etwa im Rahmen einer Werbemaßnahme – gezielt angesprochen werden.

Wegen des Ungleichgewichts in diesem Vertragsverhältnis zwischen Verbraucher und Unternehmen ist es aber eine Illusion zu glauben, dass der Verbraucher insofern gerechte „Preise“ aushandeln könnte.¹¹

Dies liegt u.a. auch daran, dass der Wert personenbezogener Daten extrem volatil ist und zumeist stark von individuellen Merkmalen wie zum Beispiel der Kaufkraft des Betroffenen abhängt. Die „Bepreisung“ von Datensätzen setzt so regelmäßig ein sehr weitgehendes „**Profiling**“ (vgl. Art. 4 (4) DSGVO)¹² voraus. Diese Mechanismen werden von der Studie nicht benannt, geschweige denn genauer hinterfragt und untersucht.

Die Studie kommt aus der Erwägung, dass es sich bei dem Datenschutzrecht vorrangig um ein Abwehrrecht handle und wegen dessen Kommunikationsbezogenheit zu der

⁹ Dazu grundrechtsdogmatisch Weichert in Taeger/Wiebe, Informatik-Wirtschaft-Recht, Regulierung in der Wissensgesellschaft (Festschrift Kilian), 2004, S. 281-298.

¹⁰ Simitis in Simitis, BDSG, 8. Aufl. 2014, § 4a Rn. 5 ff. m. w. N.

¹¹ Die Studie weist auf S. 49 auf die beschränkte Verhandlungsmöglichkeit auf Augenhöhe hin.

¹² Definition lt DSGVO: „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“

im Ergebnis falschen Schlussfolgerung, dass das Datenschutzrecht dem Betroffenen **„keine positive Verfügungsbefugnis an die Hand“** gäbe (S. 50, relativierend S. 91 ff.). Daraus wird dann die aus Grundrechtssicht problematische Konsequenz gezogen, dass Datenschutzerwägungen allenfalls als Einschränkung und Belastung (2. Ebene) der ökonomischen Verwertung eine Rolle spielen können. Eine solche Bewertung wird der Bedeutung des Datenschutzes im Verhältnis zur Bedeutung von ökonomischen Rechten (Eigentumsschutz, Berufsfreiheit) in einer demokratischen Gesellschaft nicht gerecht.

Datenschutz und Innovation bilden keinen Gegensatz, sondern lassen sich vereinbaren. Datenschutz muss als ein Baustein in der Wertschöpfungskette digitaler Geschäftsmodelle verstanden werden.

Dessen ungeachtet ist der Ansatz der Studie, **durch staatliche Regulierung einen „gerechten Markt“** anzustreben, im Grundsatz richtig. Dieser Ansatz wird heute schon durch eine Vielzahl von Gesetzen, etwa durch das Datenschutz-, das Wettbewerbs- und das Verbraucherrecht verfolgt. Eine Modernisierung dieses Rahmens erfolgte aktuell im Bereich des Datenschutzes durch die europäische Datenschutz-Grundverordnung (DSGVO) und ist in naher Zukunft für die elektronische Kommunikation in einer ePrivacy-Verordnung geplant.

Die Studie erwähnt zwar die **Datensparsamkeit** als Datenschutzgrundsatz (S. 47), zieht aber hieraus keinerlei rechtliche Konsequenzen. Die aktuelle Praxis besteht darin, dass dieser Grundsatz dadurch unbeachtet bleibt, dass bei einer Datenverarbeitung eine Vielzahl von Zwecken definiert werden, die zu einer weit gehenden „Erforderlichkeit“ von Daten führt, die dann für diese Zwecke wie auch anderweitig kommerziell genutzt werden können. Ohne dies explizit zu machen, stützt damit die Studie die Tendenz zur Datenmaximierung, die als zentrale Grundlage für (kommerzielle) Big-Data-Lösungen gesehen wird. Der Umstand, dass „Privacy by Default“ durch Art. 25 DSGVO als zwingende europarechtliche Vorgabe zu berücksichtigen ist, wird ignoriert; dieser Grundsatz wird als Handlungsalternative zum Dateneigentum dargestellt (S. 86, 112 f.).

Die Studie thematisiert an vielen Stellen die Problematik der **datenschutzrechtlichen Einwilligung**, die faktisch aber zumeist Bestandteil einer für die Verbraucher intransparenten gegenseitigen Vertragsbeziehung ist. Diese Problematik wird durch die in der Praxis weit verbreitete, von Unternehmen vorgegebene Alternative „Alles oder nichts“ (take it or leave it) gekennzeichnet (insbesondere unter 4.2.1 Convenience vs. Privatheit, S. 70 f.). Die im Hinblick auf die Fragestellung der Studie dringend gebotene Abgrenzung zwischen (einseitiger) Einwilligung und (mehrseitigem) Vertragsverhältnis wird nicht vorgenommen. Lediglich auf einer operativen Ebene wird dies in der Studie thematisiert, wenn zur Stärkung der „Verbrauchermacht“ bei der Kommerzialisierung der Daten das Koppelungsverbot (Art. 7 Abs. 4 DSGVO) hervorgehoben wird (S. 5, 125).

Hinsichtlich der Akteure wird wohl bei den Fallstudien, nicht aber bei den rechtlichen Schlussfolgerungen in der Studie eine **Differenzierung zwischen Fahrer, Mitfahrer, Halter und Eigentümer** vorgenommen. Dies mag für die grundsätzliche Behandlung

des Studienthemas unproblematisch sein. Da insofern aber auch unterschiedliche ökonomisch relevante Rollen der Betroffenen verbunden sind, sind sämtliche Rollen von datenschutzrechtlich „Betroffenen“, also neben dem Halter der Fahrer, der Mitfahrer und der Kfz-Eigentümer (der nicht mit dem Halter identisch sein muss) bei der weiteren Diskussion über ein „Dateneigentum“ relevant. Während die Zuordnung eines Kfz zum Halter straßenverkehrsrechtlich eindeutig ist, trifft dies für den Eigentümer oder Fahrer nur eingeschränkt und für den Mitfahrer nicht zu. Zu diesen können familiäre Bindungen (Familienfahrzeug) oder vertragliche Beziehungen bestehen. Zum Fahrer besteht oft eine arbeitsvertragliche, zum Mitfahrer oft eine verbrauchervertragliche (zum Beispiel Beförderungsvertrag) Beziehung.

Von der Studie als datenschutzrechtlich unproblematisch identifiziert werden Dienste mit anonymisierten Daten, wobei aber zu Recht thematisiert wird, dass der Begriff der Anonymität unklar ist (S. 21, 48, 91, 93).

In der Studie werden die Begriffe Anonymisierung und Pseudonymisierung immer nebeneinander verwendet, ohne hierzu weitere Klärungen einzufordern.

3. ANONYMITÄT UND PERSONENBEZUG VON DATEN

Die Studie differenziert bei den rechtlichen Zuordnungen persönlichkeitsrechtlich korrekt zwischen personenbezogenen/-bezieharen und anonymen Daten. Vorausgesetzt, aber nicht vertieft behandelt oder geklärt wird von der Studie die rechtlich äußerst strittige Frage, wann ein datenschutzrechtlich relevanter Personenbezug besteht. Hierzu werden eine objektive, eine relative sowie vermittelnde Ansichten vertreten.¹³ Hinsichtlich der ökonomischen Auswertung spielt die Frage der rechtlich anerkannten, d. h. **wirksamen Anonymisierung** eine zentrale Rolle, da mit der Annahme einer Anonymisierung datenschutzrechtliche Zuordnungen und damit auch persönlichkeitsrechtlich bedingte Nutzungsrechte ausgeschlossen werden.

Die Frage der Anonymisierung wird in der Studie erwähnt, wenn auch nicht, wie es angemessen gewesen wäre, vertieft. Nicht behandelt wird die für die Kommerzialisierung von Kfz-Daten spezifischere Frage, wann bei **Daten über die Sache Kfz** ein Personenbezug anzunehmen ist (allgemein dazu S. 48).

Von Seiten der Kfz-Hersteller wird bisher geltend gemacht, dass es sich bei im Kfz gespeicherten Daten nicht um personenbezogene, sondern um **rein technische Daten** handle. Dem wird teilweise entgegen gehalten, dass alle technischen Daten einen Bezug zu einem Kfz haben, das seinerseits praktisch immer zu konkreten natürlichen Personen in Beziehung steht. Hieraus könne geschlossen werden, dass sämtliche im Kfz verarbeiteten Daten einen Personenbezug haben und dass das Datenschutzrecht in jedem Fall anwendbar sei.

¹³ Die Studie geht von einem sehr „relativen“ Begriff des Personenbezugs aus, wenn sie Offline-Technikdaten des Kfz als nichtpersonenbezogen deklariert (S. 23, ausführlicher S. 93). An anderer Stelle, S. 48, weist sie, ohne aber daraus rechtliche Konsequenzen zu ziehen, auf die der objektiven Theorie zuneigenden Rechtsprechung des EuGH (U. v. 19.10.2014 – C-584/14) hin.

Beide Auslegungen werden dem Datenschutzrecht nicht gerecht. Dieses zielt darauf ab, den materiellen Schutz des allgemeinen Persönlichkeitsrechts bei der (v. a. digitalen) Verarbeitung von Daten zu sichern. Bei Sachdaten ist also ein persönlichkeitsrechtlicher Bezug nötig. **Sachbezogene Daten** sind nur insoweit als personenbezogen anzusehen, als sie eine Sache identifizieren und eine Personen-Sache-Beziehung charakterisieren.¹⁴ Eine Beziehung zu einer Person kann sich über ein Inhaltselement, ein Zweckelement oder ein Ergebniselement zu der Person ergeben.¹⁵

Ein **Inhaltselement** ist bei einem im Kfz anfallenden Datum gegeben, wenn dieses Auskunft über das Verhalten oder über Umstände einer Person gibt. Das Verhalten eines Fahrers bezieht sich zum Beispiel auf das Öffnen und Schließen der Kfz-Tür, auf das Steuern, Beschleunigen und Bremsen, auf die Verwendung der Kfz-Bedienelemente oder auf zurückgelegte Kilometer während eines bestimmten Zeitraums. Das Verhalten des Halters wird zum Beispiel registriert bei der Inspektion des Kfz oder bei der Zulassungsprüfung. Umstandsdaten sind zum Beispiel Angaben über Rahmenbedingungen bei einer konkreten Fahrt durch einen Fahrer.

Das **Zweckelement** zielt auf eine Nutzungsmöglichkeit der Kfz-Daten in Bezug auf die Person, zum Beispiel zur Kontrolle des Fahrerverhaltens oder zur Überprüfung des Umgangs des Halters mit seinem Kfz. Der Zweck kann sich auf ein konkretes Verhalten beziehen sowie auf die Feststellung eines Zu- oder Umstands. Dabei kann es um die Sicherheit (Anlegen des Sicherheitsgurtes), den persönlichen Komfort (angenehme Innentemperatur), um Warnungen oder Hinweise (zum Beispiel Füllstand des Tanks) oder das Anbieten von Wahlmöglichkeiten gehen.

Das **Ergebniselement** steht oft eng mit dem Zweckelement im Zusammenhang. Es ist gegeben, wenn die Datenverarbeitung eine reale Wirkung gegenüber dem Betroffenen hat. Dieser kann in der Überwachung des Fahrers (zum Beispiel durch dessen Arbeitgeber als Halter) oder des Halters (zum Beispiel Kontrolle des Kfz-Zustands durch den TÜV) liegen. Effekte können die Beeinflussung des Verhaltens, des Zustands oder der äußeren Umstände einer natürlichen Person sein. Ein Personenbezug besteht, wenn ein technisches Datum geeignet ist, dem Betroffenen vorgehalten zu werden, etwa anlässlich eines Unfalls oder bei Berechnung eines Versicherungstarifs.

Rein technische Daten ohne Personenbezug liegen im Kfz vor, wenn auf Grund der Sensorik im Auto Daten erhoben, ausgewertet und verwendet werden, ohne dass über diese eine Beziehung zu einer natürlichen Person hergestellt werden kann. Dies ist zum Beispiel bei Sensorsystemen der Fall, die die Einspritzmenge in den Motor regulieren. Werden in diesem Sinn rein technische Daten jedoch mit personenbeziehbaren Daten kombiniert, so ergeben sich hieraus wieder personenbezogene Daten.

¹⁴ BVerwG U. v. 24.03.2010 – 6 A 2/09, Rn. 35, DVBl 2010, 1308; Dammann in Simitis, BDSG, 8. Aufl. 2014; § 3 Rn. 59.

¹⁵ Art. 29-Arbeitsgruppe, Stellungnahme 4/2007, WP 136; Weichert in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2016, § 3 Rn. 20; Dammann in Simitis (Fn. 15) § 3 Rn. 59.

4. DISKRIMINIERUNG VON DURCH MERKMALE DEFINIERTE GRUPPEN

Die Nutzung anonymisierter Daten kann mit Bezug auf die Betroffenen weiterhin von ökonomischem Wert sein. Dies ist insbesondere der Fall, wenn es auf eine **direkte Zuordnung zu einer konkreten Person nicht zwingend** ankommt, so wie dies bei der Werbung oder auch bei Sicherheitsvorkehrungen der Fall ist.

In diesen Fällen sind keine eindeutigen „Treffer“ für die (ökonomische) Relevanz erforderlich, es genügt eine **Trefferquote mit hinreichender Wahrscheinlichkeit**. Für die Werbeansprache sind Responsequoten von wenigen Prozent wirtschaftlich schon von hohem Nutzen. Bei der Berechnung des Kreditrisikos ist ein ökonomisch sinnvoller Einsatz gegeben, wenn die höchsten Ausfallrisiken vermeiden werden können. Im Bereich der Sicherheit ist gar ein Einmaltreffer hinsichtlich eines Störers oder Gefährders ein (wirtschaftlicher) Erfolg, wenn von diesem Treffer eine große (wirtschaftliche) Gefährdung ausgeht. Dessen ungeachtet erfolgt die Adressierung einer Werbe-, einer Vertragsabschluss- oder einer Sicherheitsmaßnahme nicht nur gegenüber diesen Treffern, sondern gegenüber allen, die von der Maßnahme angesprochen werden. Mit dieser Ansprache kann im günstigen Fall eine (nur geringfügige) Belästigung verbunden sein (etwa bei unerwünschten Werbeanzeigen); in vielen Fällen kann damit aber auch eine massive **individuelle Rechtsbeeinträchtigung** etwa in Form einer merkmalsbezogenen Diskriminierung erfolgen.

Von der Studie nicht adressiert wird die rechtliche Fragestellung dieser **Gruppendiskriminierung**, die sich auf die Gruppenzugehörigen individuell auswirken kann. Als Beispiel aus dem Mobilitätsbereich sei der TomTom-Fall benannt: Der Mobilitätsdiensteanbieter (Navigationsdienst) konnte anhand der anonymisierten Bewegungsdaten seiner Nutzer feststellen, an welchen Straßenabschnitten die zulässige Höchstgeschwindigkeit regelmäßig überschritten wird. Diese (unstreitig anonymen) Auswertungsdaten übermittelte TomTom der Polizei, die an diesen Orten Geschwindigkeitskontrollen platzierte, mit denen oft diejenigen erfasst und wegen überhöhter Geschwindigkeit sanktioniert wurden, die zuvor – anonymisiert – die Datengrundlage für die Lokalisierung der Kontrollstellen geliefert hatten, da sie öfters den gleichen Straßenabschnitt mit einem vergleichbaren Fahrverhalten passierten.¹⁶ Ökonomisch war dieses Vorgehen für die Polizei äußerst sinnvoll, da mit einem begrenzten Aufwand ein Höchstmaß an Bußgeldern erlangt wurde. Für TomTom war der Verkauf dieser Daten an die Polizei kurzfristig vorteilhaft. Mittelfristig erwies sich die Veröffentlichung dieses Falls, also die Herstellung von Transparenz, für das Unternehmen als geschäftsschädigend, da das Vertrauen von deren Kunden, dass mit der Datenbereitstellung für sie keine nachteiligen Folgen verbunden ist, beeinträchtigt wurde. Was in diesem Fall als gesellschaftlich wünschenswertes Ergebnis erscheinen mag (gezielte Sanktionierung von Verstößen gegen das Straßenverkehrsrecht), kann in anderen Fällen aus demokratischer und freiheitlicher Sicht unerwünscht sein: Normabweichendes Verhalten ist für eine freiheitliche demokratische Gesellschaft insbesondere im Hinblick auf politische Betätigung, aber auch für eine freie Marktwirtschaft im Hinblick auf Konsumverhalten konstituierend.

¹⁶ TomTom verkauft anonymisierte Bewegungsprofile an Polizei, DANA 2/2011, 86.

Das TomTom-Beispiel zur Kollektivdiskriminierung weist auf ein rechtliches Problem hin, das vom bisherigen Recht nicht oder zumindest nicht befriedigend behandelt und das von der Studie überhaupt nicht adressiert wird: Diskriminierung erfolgt heute nicht mehr nur anhand von anerkannten Diskriminierungsmerkmalen (Alter, Geschlecht, Religion, Ethnie...), sondern auch wegen der Zugehörigkeit zu einer Gruppe, die möglicherweise über einen **komplexen Merkmalsmix** definiert wird. Diese Diskriminierung basiert auf dem Umstand, dass die Algorithmen von Big-Data-Analysen keine Kausalitäten feststellen können, sondern lediglich mathematisch-statistische Korrelationen. Dies führt zwangsläufig dazu, dass von algorithmusbasierten Entscheidungen Menschen betroffen sind, die keinerlei Grundlage oder Auslöser für diese Entscheidung gegeben haben.

5. LEGITIMER ANSPRUCH AUF ÖKONOMISCHEN MEHRWERT?

Die Grundannahme der Studie, dass Datengenerierung einen **zu honorierenden Aufwand** verursacht, trifft – abgesehen von den derzeit schon bestehenden „Datenrechten“ – regelmäßig nicht zu.

Bei der Erstellung von Software wird eine urheberrechtliche Leistung erbracht, indem ein Werk geschöpft wird. Bei Leistungsschutzrechten ist zumindest eine Leistung erforderlich (S. 50 ff.). Das Leistungsschutzrecht des Datenbankherstellers (§ 87a Abs. 1 S. 1 UrhG) zielt nur auf die für die Erstellung einer Datenbank erforderlichen Aufwendungen ab. Der unternehmerische Geheimschutz (§ 17 UWG) bezieht sich nicht auf durch Sensoren produzierte Kfz-Daten, sondern in spezifischen Fällen auf daraus abgeleitete Erkenntnisse (S. 57 f.). Im **Kfz generierte Daten** können allenfalls als Nebenprodukt aus dem sachrechtlichen Eigentum (§ 903 BGB, vgl. § 99 BGB) verstanden werden. Dieses Eigentum liegt bei Kfz jedoch beim Kfz-Eigentümer, der oft mit dem Halter und Fahrer identisch ist und zumindest zu diesem in einer Beziehung steht, nicht aber zum Kfz-Hersteller oder anderen Unternehmen. Interessanterweise wird der Eigentumsbezug von der Studie nicht zum Kfz-Eigentümer hergestellt, sondern zum Rechenzentrumsbetreiber, der im Auftrag eines Diensteanbieters (in der Regel der Kfz-Hersteller) die Hardware für Speicherung und Weiterverarbeitung der erhobenen Daten verwaltet (S. 61). Am ehesten könnte, wie auch die Studie erkennt, dem „Skribent“ in Person des Fahrers gemäß „lege lata“ ein Verfügungsrecht über die Kfz-Daten zugesprochen werden, der zugleich regelmäßig der datenschutzrechtlich „Betroffene“ ist. Um dieses Ergebnis zu verhindern und nicht diesen, sondern dem Hersteller ein Eigentumsrecht zuzuordnen, behilft sich die Studie mit der waghalsigen Fiktion, dass der Fahrer im Auftrag seines Arbeitgebers oder des Kfz-Herstellers den „Skripturakt“ durchführe (S. 104).

Das Anfallen von Daten ist in der Regel ein **zwangsläufiges Nebenprodukt** der Erbringung eines digitalen Dienstes. Beim Kfz entstehen die Daten regelmäßig nebenbei durch den Gebrauch des Kfz, etwa über aus funktionalen Gründen verbaute Sensoren oder durch die Bedienung des Fahrers oder sonstiger Insassen. Die Speicherung derart anfallender Daten sowie deren standardisierte Auswertung verursachen zumeist nur noch geringe wirtschaftliche Kosten. Diese stehen in keinem Verhältnis zu dem durch die Nutzung dieser Daten entstehenden Mehrwert. Die Kosten für den Verarbeitungsaufwand reduzieren sich zumeist im Verhältnis zur verarbeiteten Datenmenge, also je umfangreicher die Daten sowie die Zahl der Datensätze (der Betroffenen) werden. Je

größer die Menge der Daten ist, desto komplexere Auswertungsmöglichkeiten eröffnen sich, woraus Geschäftsmodelle entwickelt werden können. Diese Erfahrung wird bei der Verarbeitung von Internetdaten gemacht. Ein einmaliger, unter Umständen etwas größerer Aufwand für die Entwicklung und Programmierung einer neuer Applikation erweist sich durch deren weltweiten Einsatz als äußerst profitabel. Die Kosten pro verarbeitetem Datensatz zum Beispiel für Amazon, Google, Facebook oder Uber tendieren gegen Null; die mit diesem Datensatz erzielbaren Profite zum Beispiel auf dem Werbemarkt sind dagegen präzise bezifferbar und beachtlich. Sie sind die Grundlage für den hohen Marktwert dieser Unternehmen.¹⁷

Mit dem Umfang (Quantität) und der sozialen Relevanz (Qualität) der Datenverarbeitung steigen die dadurch verursachten **gesellschaftlichen Kosten**, die zum Beispiel für die staatliche Aufsicht (Datenschutzaufsicht, Straßenverkehrsaufsicht, Kommunikationskontrolle zwischen den Kfz), durch Bildungs- oder durch Infrastrukturmaßnahmen (Bereitstellen der Car2X-Kommunikationseinrichtungen) entstehen. Diese Kosten werden von der Studie nicht thematisiert. Gerade im Kfz-Bereich werden diese Kosten bisher von den Kfz-Nutzenden oder von der Allgemeinheit der Steuerzahler getragen und nicht von den Unternehmen, die diese Daten kommerziell für sich nutzen wollen.

Der Gesetzgeber muss daher verhindern, dass Unternehmen den Aufwand sozialisieren und die Gewinne privatisieren.

6. TRANSPARENZ, DEMOKRATISCHE UND RECHTLICHE KONTROLLE

Während es sich bei dem TomTom-Beispiel (s. o. 3.4) um einen zumindest nachträglich transparent gemachten, für jeden Menschen nachvollziehbaren Vorgang handelte, besteht im Hinblick auf **Big-Data-Anwendungen**, mit denen ein besonders hoher Mehrwert erzielt werden kann, generell ein gesteigertes Transparenz- und Kontrollproblem: Basiert die Entscheidung für eine (hoheitliche oder wirtschaftliche) Maßnahme (im TomTom-Beispiel die Geschwindigkeitskontrolle) nicht auf einer nachvollziehbaren „Wenn-dann-Datenauswertung“, sondern auf einem zum Beispiel per künstliche Intelligenz (KI) generierten komplexen Algorithmus, so kann dies dazu führen, dass die Gründe für diese Entscheidung nicht mehr kontrolliert und die Verantwortlichkeiten nicht mehr festgestellt werden können, weil der selbstlernende Algorithmus nicht nachvollziehbar protokolliert wurde. So könnte zum Beispiel ein Algorithmus zur Verkehrsschildererkennung aufgrund von widersprüchlichen Daten auf Basis der Sensorik, Kartierung, car-to-car-Kommunikation oder anderen Datenströmen eine falsche Entscheidung treffen. Selbst im Fall einer nachvollziehbaren Protokollierung kann oft keine einem Menschen oder einer Institution zuordenbare (rechtliche) Verantwortlichkeit begründet werden. Die Verantwortlichkeit für die Programmierung künstlicher Intelligenz (KI) begründet im bestehenden Rechtsregime nicht zwangsläufig die (rechtliche) Verantwortlichkeit für eine auf dieser Grundlage getroffene (rechtlich relevante) Entscheidung. Selbst für den Fall einer theoretisch begründbaren Haftung des Programmierers

¹⁷ Mayer-Schönberger/Ramge, KN 21./22.10.2017, Sonntag S. 2, mit Verweis auf dies., Das Digital, Wertschöpfung und Gerechtigkeit im Datenkapitalismus, 2017.

bleibt das praktische Problem bestehen, dass wegen der Arbeitsteilung bei komplexen Programmcode-Generierungen eine Verantwortungszuordnung oft nicht möglich ist.

Das Protokoll- und Transparenzdilemma bei über KI generierte Daten betrifft nicht nur die direkt von einer Verarbeitung Betroffenen, also insbesondere die Verbraucher. Davon tangiert sein können und sind regelmäßig auch die staatliche Aufsicht, die gerichtliche Kontrolle sowie die **demokratische Kontrolle durch Parlamente**. Dieses Problem wurde schon früh durch Lawrence Lessig in einem Aufsatz mit dem Titel „Code is Law“ benannt, wonach anstelle von demokratisch legitimierten Instanzen Algorithmen für die Freiheitsrechte relevante Entscheidungen treffen.¹⁸ Dieses Kontroll- und Verantwortlichkeitsdilemma, das bei Geschäftsmodellen in der Zukunft zunehmend besteht, wird in der Studie nicht thematisiert. Das Ergebnis sind Profite aus „Dateneigentum“, das letztlich unkontrollierbar und unverantwortlich ist.

Dieser Effekt wird durch ein aktuell bestehendes Rechtsproblem verstärkt: Bisher ist es durch die Rechtsprechung des Bundesgerichtshofes (BGH) anerkannt, dass sozial relevante Algorithmen als **Betriebs- und Geschäftsgeheimnisse** zumindest für die Betroffenen nicht offenkundig-, d. h. auskunftspflichtig sind.¹⁹ Auch für eine staatliche Aufsicht können sich hier praktische oder rechtliche Kontrollprobleme oder -konflikte ergeben. Diese Problematik wird in der Studie nicht ausdrücklich und unzureichend thematisiert. Es bedarf insofern der gesetzlichen Regulierung einer Offenlegungspflicht und einer rechtlichen Zuordnungspflicht in Bezug auf grundrechtlich bzw. generell gesellschaftlich relevante Algorithmen.²⁰

Aufsichtsbehördliche, verbraucherrechtliche, demokratische und gerichtliche Kontrolle **verbietet Ausschließlichkeitsrechte** an digitalen Daten, insbesondere, wenn diese von hoher ökonomischer Bedeutung sind.

Wegen ihrer hohen sozialen Relevanz besteht an diesen Daten ein hoher öffentlicher Informations- und Kontrollbedarf.

Die Studie schlägt als Lösung für das zentrale verbraucherpolitische Anliegen nach Transparenz und Verständlichkeit für die Betroffenen die Regulierung durch einen „Daten-Ausweises“ vor. Dort soll benannt werden, welche Datenarten für welche Zwecke genutzt werden (S. 4, 123). Der Daten-Ausweis wird auch zur Grundlage für mögliche Einwilligungen von datenschutzrechtlich Betroffenen herangezogen.

Wie das Instrument des „Daten-Ausweises“ konkret umgesetzt werden soll, wird nicht näher ausgeführt.

¹⁸ Lessig, Code is Law, <http://harvardmagazine.com/2000/01/code-is-law.html>; dazu auch Boehme-Neßler NJW 2017, 3031, .

¹⁹ Bundesgerichtshof (BGH), U. v. 28.01.2014 – VI 156/13, NJW 2014, 1235; dazu ausführlich ULD/GP-Forschungsgruppe, Scoring nach der Datenschutznovelle 2009, S. 44 ff.

²⁰ Charta der Digitalen Grundrechte der Europäischen Union, <https://digitalcharta.eu/>.

7. WEITERE GESAMTGESELLSCHAFTLICHE ASPEKTE

Open Access (Open Data) wird in der Studie vorrangig unter dem Aspekt der wirtschaftlichen Weiterverwendungsmöglichkeit erörtert, nicht unter dem aus Demokratie-sicht viel wichtigeren Motiv der Kontrolle staatlicher oder wirtschaftlicher Macht. Ebenso wenig wird Open Access thematisiert als eine Grundvoraussetzung individueller Selbstbestimmung in einer Informationsgesellschaft.

Wirtschaftliche Nutzungsrechte und "Eigentum" von Daten werden nicht als ökonomische und politische Machtbeziehungen verstanden, was sie tatsächlich sind. Dadurch können sich **Wettbewerbsverzerrungen** ergeben. Das Kartellrecht beginnt gerade erst damit, sich mit den damit verbundenen Angebotsbeschränkungen und Preisnachteilen für die Verbraucher zu befassen. In der Studie wird diese Diskussion nicht aufgegriffen.

In der Studie wird kaum berücksichtigt, inwieweit Daten eine nicht nur ökonomisch zu verstehende Funktion für das Gemeinwohl zukommt. Diese Gemeinwohlfunktion ist auch darin zu sehen, dass Daten (über Forschung) dem allgemeinen **wissenschaftlichen Fortschritt** nutzbar gemacht werden können und sollen. Die dadurch erlangten Erkenntnisse sind eine wesentliche Grundlage für einen informationell selbstbestimmten Umgang des Einzelnen mit seiner Umwelt wie für die Gesamtgesellschaft im demokratischen Meinungsbildungsprozess.

Bei der Diskussion um Dateneigentum und um ein Datengesetz darf es letztlich nicht nur um Fragen ökonomischer Macht und Wertigkeit gehen, sondern es muss auch die Sozialpflichtigkeit der Daten im Auge behalten werden. Aus Datenschutz- und Verbraucherschutz-sicht ist diese Perspektive wichtig.

8. WEITERE RECHTLICHE ANPASSUNGEN STATT DATENGESETZ

Richtig und unterstützungswürdig sind weitere einzelne **Anpassungen des bestehenden Rechts** an die Rahmenbedingungen digitaler Datenverarbeitung. Dabei ist aber das Anknüpfen an das aus dem Sachenrecht stammende Rechtsinstitut des Eigentums nicht sinnvoll und führt fast zwangsläufig zur ungenügenden Berücksichtigung von sonstigen Grundrechts- und Demokratiebelangen.

Neben einzelnen in der Studie angesprochenen Rechtsänderungen (zum Beispiel Verbesserung des Integritätsschutzes durch Haftungs- oder Strafnormen, S. 114 f.) sind aus datenschutz- und verbraucherschutzrechtlicher wie auch aus gesamtgesellschaftlicher demokratischer und rechtsstaatlicher Sicht folgende Rechtsänderungen nötig:

- ❖ Mit der Normierung von Herstellerpflichten – auch im Bereich der Kfz-Datenverarbeitung – im Sinne von Produktqualitätsanforderungen können Transparenz- und Qualitätsverbesserungen, Sicherheit und mehr Wettbewerbsgerechtigkeit erreicht werden.²¹

²¹ So auch Martin-Jung, Der programmierte Absturz, SZ 19.10.2017, 13.

- ❖ Der bisher rechtlich zugestandene Schutz von Daten als Betriebs- und Geschäftsgeheimnis oder auf der Grundlage des Urheberschutzes, die zugleich eine soziale oder für Dritte (zum Beispiel datenschutzrechtlich) beachtliche Relevanz haben, muss dahingehend modifiziert werden, dass Dritt- bzw. Gemeinwohlinteressen hinreichend Geltung verschafft werden kann.
- ❖ Statt normativ ökonomische Ausschließlichkeitsrechte zu begründen, ist es im Interesse der Verhinderung von Monopolstrukturen wie im Interesse eines „gerechten Marktes“ sinnvoller, rechtliche Regelungen zu schaffen, die bei Erreichen einer bestimmten Marktmacht zum Teilen von verfügbaren Daten verpflichtet.²²
- ❖ Durch die rechtliche Etablierung einer transparenten Selbstregulierung im Kfz-IT-Bereich, können schnell zielorientierte Lösungen erreicht werden, bei denen zugleich die öffentlichen und Verbraucherbelange berücksichtigt werden.
- ❖ Durch die Festlegung von Standardisierungsverfahren und die Erarbeitung von Standards, zum Beispiel zur Sicherstellung der Kommunikationsfähigkeit der Kfz-IT-Systeme, können Funktionalität und Sicherheit verbessert werden und zugleich die Voraussetzungen für die Datenportabilität zugunsten der Verbraucher (vgl. Art. 20 DSGVO) geschaffen werden.
- ❖ Durch die normative, gegebenenfalls obligatorische Festlegung von spezifischen Zulassungs- und Zertifizierungsverfahren, wie sie im Straßenverkehrsbereich generell üblich und bekannt sind, für den Bereich der Kfz-IT kann die bei den Verbrauchern und oft auch bei den Aufsichtsbehörden nicht bestehende Fachexpertise durch unabhängige Sachverständige zur Geltung gebracht werden. Dies gilt insbesondere für den Einsatz von „künstlicher Intelligenz“ bei für die Gemeinschaft oder Dritte relevanten Entscheidungen.

²² So auch Mayer/Schönberger/Ramge, KN 21./22.10.2017, Sonntag S. 2.