DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

zur Frage des „Eigentums“ an Daten und Informationen

Stellungnahme Nr.: 75/2016 **Berlin, im November 2016**

Mitglieder des Ausschusses

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender, Berichterstatter)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierekoven, Nürnberg
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Michael Friedmann, Hannover
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg (Berichterstatter)
- Rechtsanwalt Prof. Niko Härting, Berlin (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München
- Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

Zuständig in der DAV-Geschäftsführung

- Rechtsanwältin Nicole Narewski, Berlin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Verteiler Europa

Europäische Kommission
- Generaldirektion Kommunikationsnetze, Inhalte und Technologien
- Generaldirektion Justiz

Europäisches Parlament
- Ausschuss Bürgerliche Freiheiten, Justiz und Inneres
- Ausschuss Recht
- Ausschuss Binnenmerkt und Verbraucherschutz

Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen
Rat der Europäischen Anwaltschaften (CCBE)
Vertreter der Freien Berufe in Brüssel

Verteiler Deutschland

Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie

Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
GRUR
BITKOM
DGRI

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Redaktion NJW

Juve-Verlag
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 66.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Der DAV begleitet die Diskussion über die Entwicklung eines eigenständigen Dateneigentums auf europäischer Ebene. Mit dieser Stellungnahme gibt er einen Überblick zur in Deutschland geltenden Rechtslage.

Einleitung

Zunehmend wird in den letzten Jahren darüber diskutiert, ob es neben ohnehin schon gegebenen diversen Rechten an Daten oder Datensammlungen ein eigenständiges „Eigentum“ an Daten geben soll, das unabhängig ist vom Eigentum am Datenträger. Solche Diskussionen finden sich, wenn es um die Rechte an Fahrzeugdaten („Connected Cars“) geht oder um die automatische Ansammlung von Daten bei anderen mit dem Internet verknüpften „Smart Devices“ („Internet der Dinge“). Die Rechtsfrage ist auch für den Austausch von bzw. Zugang zu Daten der Industrie 4.0 relevant.

Die EU-Kommission befasst sich derzeit im Rahmen ihrer Strategie für den Digitalen Binnenmarkt mit der Frage, ob es gesetzlicher Regelungen zum „Dateneigentum“ bedarf. Sie hat angekündigt, diese Überlegungen im Januar 2017 in einem Legislativvorschlag zu „Unjustified data location restrictions“ und voraussichtlich einem nicht legislativen Instrument zu den Themen Dateneigentum und Haftung im Rahmen der „Free Flow of Data Inititiative“ vorzustellen. Der DAV begrüßt die derzeit begonnene Prüfung und hält dazu fest:

1.

Das geltende Recht in den Mitgliedstaaten ist durch eine Vielzahl von Schutz-Ausschließlichkeitsrechten an Daten unterschiedlicher Art gekennzeichnet. Noch können keine konkreten Vorschläge zum Thema Dateneigentum gemacht werden. Doch sollen im Folgenden verschiedene Fragestellungen am Beispiel des geltenden Rechts dargestellt werden. Diese werden in der Folge anhand der in Deutschland

geltenden Rechtslage dargestellt, die in vielen, aber nicht in allen Bereichen europarechtlich geprägt ist.

- Zunächst gibt es das Eigentum am Datenträger. Ob daraus ein „Erstnutzungsrecht“ des Eigentümers an „sachgenerierten“ Daten folgt, ist umstritten. Der Eigentümer eines Smartphones, Tablets oder PCs ist aber grundsätzlich berechtigt, über Daten, soweit diese sich in Form von z.B. elektromagnetischen oder optischen Speicherzuständen auf einem Datenträger befinden (§ 93 BGB), die dem zivilrechtlichen Eigentum zugewiesenen Herrschaftsrechte auszuüben. Die Befugnisse des Hardwareeigentümers können allerdings durch konfligierende Rechtspositionen wie Datenschutz, Geheimnisschutz, Schutzrechte des UrhG, Recht am eigenen Bild, Fernmeldegeheimnis etc. eingeschränkt sein.

- Seit es das Softwarerecht gibt, wird in Deutschland diskutiert, ob Software eine Sache ist (§ 90 BGB). Der Bundesgerichtshof hat Software (und damit auch Daten) vertragsrechtlich meist wie eine Sache behandelt.

- Davon unabhängig gibt es ein Schutzrecht für Datenbanken aufgrund der Datenbankrichtlinie 96/9/EG der EU (und entsprechender Normen des deutschen Urheberrechts, §§ 87 a ff. UrhG), dessen Reichweite im vorliegenden Kontext durch die Rechtsprechung aber erst noch geklärt werden muss. Merkmal dieses Schutzrechtes ist es, dass es nur die Datenbank selbst schützt, nicht die darin enthaltenen (Einzel-) Daten; es schützt demzufolge nur gegen wesentliche Entnahmen (nach der deutschen Rechtsprechung nicht bei Entnahmen unter 10%). Es bleibt abzuwarten, ob diese im Interesse der Informationsfreiheit grundsätzlich zu begrüßende Beschränkung auch im vorliegend diskutierten Kontext interessengerecht ist. Denn die in einer Datenbank enthaltenen Daten verkörpern unabhängig vom Umfang einer vorgenommenen Entnahme durchweg einen wirtschaftlichen Wert.

- Weiterhin sind manche Datensammlungen in Software integriert. Dieses kann in den Grenzen der zulässigen Schaffung von Datenschnittstellen und kompatiblen Programmen (§§ 69a Abs. 2, 69e UrhG) ebenfalls zu einem mittelbaren Schutz über den Urheberrechtsschutz der Computerprogramme führen (§§ 69 a ff. UrhG), der durch die Richtlinie über der Rechtsschutz von

Computerprogrammen 2009/24/EG im Detail vorgeprägt ist. Ob die §§ 69a ff. UrhG darüber hinaus auch für Datensammlungen greifen, die aus Programmen ausgelagert und getrennt abgespeichert sind, aber für den Programmablauf entscheidend sind, wird derzeit diskutiert, ist aber zu bezweifeln.

- Daten, die zugleich Betriebsgeheimnisse bzw. vertrauliches Know-how darstellen, können zudem nach den Gesetzen über den unlauteren Wettbewerb (in Deutschland § 17 UWG) bzw. den künftigen Rechten entsprechend der Richtlinie 2016/943/EU zum Schutz von Geschäftsgeheimnissen geschützt sein.

- Soweit es sich um personenbezogene Daten, Bildnisse von natürlichen Personen oder das gesprochene Wort handelt, gibt es darüber hinaus Rechte der Personen, über welche die Daten gespeichert werden. Diese Rechte der Betroffenen überlagern sämtliche vorgenannten Rechte. Sie stellen allerdings keine eigentumsähnliche Position dar. Vielmehr handelt es sich um Verfügungs- und Abwehrrechte gegen die Erhebung und Verwendung personenbezogener Daten. Soweit Daten dem Fernmeldegeheimnis unterliegen ist der Telekommunikationsdiensteanbieter in seiner Verfügungsbefugnis über die Daten eingeschränkt.

- In Deutschland erkennen manche juristische Autoren darüber hinaus ein eigenes absolutes Recht an Daten im Sinne des § 823 Abs. 1 BGB an; unklar ist aber, wem dieses Recht zuzuordnen ist. Deliktsrechtlich geschützt werden kann im deutschen Recht zudem nur die Vertraulichkeit und Integrität von Daten, ohne dass sich Ausschließlichkeitsrechte auf diese Weise begründen lassen.

- Wiederum in Deutschland bleibt daneben auch abzuwarten, inwieweit sich Ansprüche nach § 823 Abs. 1 BGB auch basierend auf dem vom deutschen Bundesverfassungsgericht anerkannten Recht auf Integrität und Vertraulichkeit der IT-Systeme ergeben können. Auch hier kann es nur um den Schutz der Integrität von Daten gehen, das Deliktsrecht kann keine Ausschließlichkeitsrechte begründen.

- Ein Schutz von Daten kann sich schließlich auch aus §§ 823 Abs. 2 BGB, § 202a, 303a StGB ergeben. Auch hier geht es ausschließlich um die

Vertraulichkeit und Integrität von Daten, nicht jedoch um Ausschließlichkeitsrechte.

Die Regelungen der §§ 202a und 303a StGB (Ausspähen von Daten und Datenveränderung) sind zwar im Grundsatz äußerst taugliche Schutzinstrumente für die Integrität von Daten und neben dem Schutz personenbezogener Daten und dem Know-how-Schutz der wichtigste Schutzaspekt. Unklar und umstritten ist jedoch, wem eine daraus abgeleitete potenziell strafrechtlich begründete „Datenverfügungsbefugnis“ zustehen sollte. Diskutiert werden der Sacheigentümer (und somit der Eigentümer des jeweiligen Datenträgers), was aber aufgrund vertraglicher Nutzungen von IT-Systemen ein oft untaugliches Kriterium ist, der sog. Skribent ("Schreibende") und – v.a. im Arbeits-, Dienst- und Auftragsverhältnis –bzw. derjenige, der die Speicherung veranlasst bzw. bewirkt hat. Auch das Abstellen auf den Skriptur- bzw. Speicherakt erlaubt aber nicht das Einstellen von sonstigen Wertungskriterien (z.B. Systemverantwortung i.S. der Produktsicherheit). Allgemein ist dieses auch eine Schwäche der §§ 202a und 303a StGB, die als Strafrechtsnorm wortlautgebunden sind und daher nur in begrenztem Maße Wertungen zugänglich ist. Der Skriptur- bzw. Speicherakt kann bilateral (etwa im Verhältnis Arbeitgeber, Auftraggeber und/oder Hardwareeigentümer) zu brauchbaren Abgrenzungskriterien zu führen, aber nicht ohne weiteres im Sinne einer absoluten Verfügungsbefugnis gegenüber jedermann.

2. Herausgabeansprüche

Eine besondere Schwäche zumindest der deutschen Rechtslage liegt darin, dass es für Daten keine dinglichen Herausgabeansprüche gibt. Ausgewichen wird auf vertragliche Ansprüche teils in Kombination mit § 242 BGB bzw. (soweit personenbezogene Daten betroffen sind) mit § 11 BDSG. Unabhängig hiervon kann die tatsächliche Herrschaft über Daten bzw. datenerzeugende Gegenstände ein Vermögenswert sein, der über das Bereicherungsrecht kondiktionsfähig ist. Allerdings sind diese Ansprüche weder absolut noch insolvenzfest.

Daneben kommen mitunter Herausgabeansprüche nach §§ 667, 670, 675 BGB in Betracht, die immerhin teils insolvenzfest sind, aber ihrem Tatbestand nach nur ausnahmsweise greifen. In Zukunft ergeben sich vergleichbare Ansprüche für personenbezogene Daten des Betroffenen, die dieser dem Verantwortlichen zur Verfügung gestellt hat, auch aus Art. 20 DSGVO („Datenübertragbarkeit“ bzw. „Portabilität“). Möglicherweise sind diese Ansprüche auch insolvenzfest. Sie betreffen aber nur einen kleinen Ausschnitt der gespeicherten Daten.

3.

Die Interessenlage der Beteiligten ist höchst komplex:

- Integritätsschutz: In manchen Konstellationen geht es darum, Daten vor Veränderungen zu schützen, um ihre Integrität zu bewahren. Dieses Interesse wird in Deutschland z.B. durch § 303a StGB geschützt.

- Vertraulichkeitsschutz: In anderen Konstellationen geht es darum, Daten vertraulich zu halten und/oder dafür zu sorgen, dass nur der „Berechtigte“ sie verwenden kann. Diesem Schutz dienen z.B. § 202a StGB oder auch §§ 17, 18 UWG. Letztendlich geht es beim Vertraulichkeitsschutz hier eher um den Schutz von Informationen, nicht nur von Daten.

- Wirtschaftliche Zuordnung: Oft stellt sich weniger die Frage des Schutzes von Daten als die Frage der wirtschaftlichen Berechtigung zur Nutzung und Verwertung von Daten sowie die Frage nach Ausschließlichkeitsrechten. So ist es im Zusammenhang mit „Connected Cars“ nicht zu leugnen, dass es für dabei entstehende Datensammlungen Datenbankrechte geben kann. Ob immer Datenbankrechte entstehen oder dies z.B. daran scheitert, dass die Daten bei der Nutzung technischer Einrichtungen anfallen und es daher keine Investitionen für die Datenbeschaffung gibt, ist gerichtlich noch nicht entschieden und einzelfallabhängig. Gibt es solche Rechte, stellt sich die Frage, wer denn Inhaber der Datenbankrechte an diesen Datensammlungen ist. Dies kann sowohl der Automobilhersteller sein, wenn er die Daten bei sich oder auch im Auto auf Basis von ihm gestellter entsprechender Software sammelt. Dies kann aber auch ein Serviceprovider sein, wenn er die Daten nicht nur vermittelt, sondern auch

sammelt und für eigene Zwecke verwendet. Darüber hinaus können Rechte an den Daten auch dem Fahrer eines Autos zustehen, weil dieser sie beim Fahren sammelt. Möglicherweise stehen sie auch dem Eigentümer des Fahrzeugs zu, weil ihm das Speichermedium gehört. Ggf. kommt auch der Halter des Fahrzeugs in Betracht, der ja oft (z.B. bei Leasingfahrzeugen) nicht der Eigentümer ist. Ähnliche Fragen gibt es für andere Rechte und bei anderen tatsächlichen Konstellationen. Gerade bei komplexen Situationen ist weder die ökonomische Situation noch die Rechtslage klar. Dies gilt umso mehr im Hinblick auf die Überlagerung der Rechtezuordnung durch das Datenschutzrecht, das beispielsweise bei einem Personenbezug von Fahrzeugdaten dem Eigentümer des Fahrzeugs, dem Halter, dem Fahrer und sogar einem Beifahrer Abwehrrechte gewährt gegen die Nutzung und Verwertung von Fahrzeugdaten.

4.

Wenn Fragen des „Dateneigentums“ diskutiert werden, geht es vielfach nicht um Ausschließlichkeitsrechte an Daten, sondern um den Versuch, Herrschafts- oder sogar Exklusivrechte an Informationen zu begründen. Insofern ist Vorsicht geboten, zumal in einer offenen Gesellschaft die Informationsfreiheit einen hohen Stellenwert (vgl. Art. 10 EMRK, Art. 11 EU-GrCh, Art. 5 Abs. 1 Satz 1 GG) hat.

5.

Eine unklare Rechtslage fordert oft den Gesetzgeber. Im Bereich „Dateneigentum“ bzw. der „Ausschließlichkeitsrechte an Informationen“ sind aber die juristischen Ansätze noch weitgehend ungeklärt. Die Europäische Kommission untersucht derzeit die Interessenlage. So stellt sich etwa die Frage, inwieweit die Verantwortlichkeit für die Produktsicherheit mit Blick auf entsprechende Systemdaten bei der Schaffung und Zuordnung von Rechten beachtet werden sollte.

Hier muss noch viel rechtsdogmatische und rechtstatsächliche Arbeit geleistet werden, um zu interessengerechten Lösungen zu kommen. Erste Rückmeldungen aus der Industrie und Wirtschaft deuten darauf hin, dass die praktisch auftretenden Probleme

sich (noch) vertraglich lösen lassen. Die Freiheit der Vertragsgestaltung ist insofern ein wichtiges Instrument zur Herstellung von Rechtsklarheit. Daher ist der Ansatz der Europäischen Kommission im Rahmen ihrer „Free flow of data Initiative“ zu begrüßen, derzeit zunächst nicht gesetzgeberisch tätig zu werden. Eine zu frühe gesetzliche Regelung könnte leicht zu praxisuntauglichen und/oder interessenwidrigen Lösungen kommen. Insbesondere könnte es gefährlich sein, durch Monopolrechte einzelnen Anbietern exklusive Rechte zuzuweisen.

Dass der Datenaustausch elementar für den Wettbewerb ist, liegt auf der Hand. Grenzen werden nach geltendem Recht bereits gesetzt. Dies gilt insbesondere für den Schutz personenbezogener Daten durch das Datenschutzrecht. Auf dem Gebiet des Softwareschutzes spiegeln sich die Interessenkonflikte etwa in den bereits zitierten deutschen Normen der §§ 69a Abs. 2, 69e UrhG.

Es empfiehlt sich, zunächst die weitere Diskussion abzuwarten, die Rechtslage auch in anderen EU-Mitgliedstaaten zu untersuchen und erst danach gesetzgeberische Lösungen zu entwickeln. Die deutsche Anwaltschaft wird sich mit den Ergebnissen der „Free Flow of Data Initiative“ der Kommission befassen und hierzu weitere Stellungnahmen abgeben.