www.jusletter-it.eu

Christine Möhrke-Sobolewski

«Intelligenter Verkehr» – und Datenrechte

Wem gehören die Daten von Auto und Strasse?

The article takes up essential aspects of some of the conference's speeches that particularly formulate discursive approaches for answering the question of data ownership. Along with a short introduction of the current state of debate in case law and literature, safety aspects of individual and mass transport are discussed, the interaction of data and creation of value is outlined, and questions regarding the procedural usage of data in terms of access rights in civil and criminal procedures and according to data protection are asked. Finally, above mentioned is summarized in a short conclusion. (ah)

Category: Conference Proceedings
Region: Germany; Switzerland
Field of law: Data Protection; Robotic

Citation: Christine Möhrke-Sobolewski, «Intelligenter Verkehr» – und Datenrechte, in: Jusletter IT 24 November 2016

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

I. Einleitung

[Rz 1] Die Frage nach dem Recht an Daten steht seit einigen Jahren im Mittelpunkt kontroverser Diskussionen[1]. Doch sehr oft blieben die rechtlichen Vorstellungen der verschiedenen Standpunkte eher unklar. Nicht nur der rechtliche Begriff von Daten blieb unbestimmt, sondern auch die daraus folgenden Konsequenzen. Erst in jüngerer Zeit, mit dem Einzug der Digitalisierung in viele Lebensbereiche ändert sich dies, denn nun gibt es konkrete Anknüpfungspunkte, die sich jedermann vorstellen kann. Der Digitalisierung des Strassenverkehrs kommt dabei eine Schlüsselstellung zu, denn hier produziert fast jeder Daten, die theoretisch Teil eines Big Data-pools sein könnten. Die Auseinandersetzungen verdeutlichen, dass die traditionellen Rechtskonzepte die Diskussion noch bestimmen, aber nicht wirklich passen: So wird etwa im Zusammenhang mit Fahrzeugdaten das den strafrechtlichen Normen der §§ 202a–202c deutsches Strafgesetzbuch (StGB) sowie des von § 303a StGB zugeordnete Rechtsgut der «Verfügungsbefugnis über Informationen» zum Anknüpfungspunkt genommen, um in Bezug auf Big Data-Anwendungen die Idee eines zivilrechtlichen Dateneigentums zu begründen.[2] Ein anderer Vorschlag zur Begründung einer eigentumsrechtlichen Zuordnung von Daten knüpft an das Rechtssystem des Immaterialgüterschutzes an. Urheberrechtliche Verwertungsrechte zum Vorbild zu nehmen, habe den Vorteil,[3] dass die für das Privatrecht notwendige Differenzierung bereits vorstrukturiert sei und auf diese Weise eine bedarfsgerechte Lösung für einen Handel mit Daten sowie eine interessengerechte Alternative für einen modernen und effektiven Datenschutz in der digitalen Gesellschaft gefunden werden könnte.

---

1 Thomas Hoeren, Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (487); Michael Dorner, Big Data und «Dateneigentum» – Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (618); Malte Grützmacher, Dateneigentum – ein Flickenteppich, CR 2016, 485 ff.; Herbert Zech, Daten als Wirtschaftsgut – Überlegungen zu einem «Recht des Datenerzeugers», CR 2015, 137 ff.; Gerrit Hornung/Thilo Goeble, «Data Ownership» im vernetzten Automobil, CR 2015, 265 ff.; Sven-Erik Heun/Simon Assion, Internet(recht) der Dinge, CR 2015, 812; OLG Dresden, NJW-RR 2013, 27; Jens Schefzig, Wem gehört das neue Öl? – Die Sicherung der Rechte an Daten, K&R 2015, Beihefter 3/2015, 3 ff.; Rolf Schwartmann/Christian-Henner Hentsch, Parallelen aus dem Urheberrecht für ein neues Datenverwertungsrecht, PinG 2016, 117 ff.; Louisa Specht/Rebecca Rohmer, Zur Rolle des informationellen Selbstbestimmungsrechts bei der Ausgestaltung eines möglichen Ausschließlichkeitsrechts an Daten, PinG 2016, 127 ff.

2 Hoeren (Fn. 1), 486 ff.

3 Schwartmann/Hentsch (Fn. 1), 117 (126).

[Rz 2] Diskussionen um ein mögliches Dateneigentum kommen aber nicht umhin, sich auch über die Rolle des informationellen Selbstbestimmungsrechtes bei der Ausgestaltung eines möglichen Ausschließlichkeitsrechts an Daten auseinanderzusetzen. Das informationelle Selbstbestimmungsrecht ist als höchstpersönliches Recht ausgestaltet.[4] Es ist als Ausfluss des allgemeinen Persönlichkeitsrechts in Verbindung mit der Menschenwürdegarantie entwickelt und gerade nicht als übertragbares, nicht vererbliches und nicht der Zwangsvollstreckung unterliegendes Recht ausgestaltet.[5] Dieses Rechtsdenken steht quer zu vielen Ideen von Dateneigentum.

[Rz 3] Hierin liegt der Vorteil der Anknüpfung an das Urheberrecht, das dem Urheber einen verfassungsrechtlichen Schutz sowohl aus der Menschenwürde in Verbindung mit der Eigentumsgarantie gewährt und die wirtschaftliche Grundlage der Monetarisierung kreativer Arbeit darstellt. Damit geht das Urheberrecht viel weiter als das Datenschutzrecht, weil die urheberrechtlichen Verwertungsrechte sowohl urheberpersönlichkeits- wie auch vermögensrechtlichen Gehalt aufweisen.[6]

[Rz 4] Bereits diese unterschiedlichen Ansätze zeigen das Spektrum der Fragen auf, die sich bei der Digitalisierung eines Lebensbereiches stellen und sie waren Gegenstand der Tagung «Intelligenter Verkehr – Rechtsfragen» unter Leitung von Sabine Gless (Universität Basel) und Wolfgang Wohlers (Universität Basel). Die Veranstaltung widmete sich also der Frage nach der Herrschaft über Daten, die durch Digitalisierung des Strassenverkehrs und insbesondere den Einsatz von (hoch)automatisierten Fahrzeugen generiert werden.

II. Sicherheitsaspekte im intelligenten Verkehr

1. Datensicherheit und Risikomanagement

[Rz 5] Eine Antwort auf die Frage zu finden, wem Daten gehören, wird im Zusammenhang mit «intelligentem Verkehr» umso dringender, je mehr Daten produziert und je mehr Schlüsse aus diesen Daten gezogen werden können. Wir stehen am Beginn einer Umwälzung im öffentlichen Verkehr. Wo im Jahr 2013 in Deutschland nur knapp 200000 Nutzer Carsharing in Anspruch nahmen, stieg diese Zahl im Jahr 2016 bereits auf über 1,2 Mio Nutzer.[7] Ein Durchbruch für autonomes Fahren wird für das Jahr 2030 bereits angenommen.[8] Die Digitalisierung ermöglicht umfassende Vernetzung und ist Grundlage für ein deutlich verändertes Mobilitätsverhalten.[9] Elektronische Datenverarbeitung wird Grundlage für den Mobilitätsumbruch sein: eine Vielzahl von Daten wird durch das Lenken, Bremsen, Führen eines Fahrzeugs generiert. Die Daten wiederum lassen eine Vielzahl von Schlüssen auf den Fahrer, den Zustand des Fahrzeugs, Fahrzeug-

4 BVerfG, Urteil vom 15. Dezember 1983 – Volkszählung.

5 Specht/Rohmer (Fn. 1), 127 (128).

6 Schwartmann/Hentsch (Fn. 1), 117 (126); Beck-OK UrhG, 14. Aufl, Stand 1. Oktober 2016, Kroitzsch/Götting, § 15 Rn. 1.

7 http://www.carsharing.de/sites/default/files/uploads/grafik_entwicklung_carsharing_deutschland_2016_gesamt_ohne_logo_0.pdf (alle Internetadressen zuletzt besucht am 6. November 2016).

8 http://www.pwc.de/de/pressemitteilungen/2015/pwc-prognose_autonomes-fahren-setzt-sich-zwischen-2025-und-2030-durch.html.

9 Diskussionspapier BVDW, Connected Cars – Chancen und Risiken für die künftigen Anbieter im Automobilmarkt, Januar 2016.

insassen und andere Verkehrsteilnehmer zu.[10] Wer Zugriff auf diese Daten hat, wird in Zukunft noch heute ungeahnte Möglichkeiten haben, mit diesen Daten neue Wertschöpfungsprozesse anzustrengen.

[Rz 6] Dass der bloße Zugriff auf Daten aber natürlich noch keine Datenrechte begründet, illustrierte der Vortrag von Dominik Herrmann von der Universität Siegen, der Sicherheitsrisiken beim Betrieb kritischer Infrastrukturen erläuterte und sie beispielhaft an einigen Pilotprojekten für den testweisen Einsatz autonomer Fahrzeuge konkretisierte. Er skizzierte den Risikomanagementkreislauf zur Einschätzung möglicher Sicherheitsrisiken bei kritischen Infrastrukturen.

[Rz 7] Danach muss zunächst das Risiko identifiziert, bewertet, gesteuert und schließlich überwacht werden. Zur Identifikation von Risiken könne die Historie bereits eingetretener Risiken dienen, die Entwicklung eines Fehlerbaumes und die Analyse möglicher Bedrohungen nach dem STRIDE-Katalog. Allerdings würde angesichts der Komplexität kritischer Infrastrukturen eine beliebig lange Kette möglicher Angreifer entstehen, die Eingang in das Risikomanagement finden müssten.

[Rz 8] Wer ein Datenrecht hat, sollte Datensicherheitsaspekte beachten – so eine These seines Vortrages. Er setzte sich mit Methoden der Verschlüsselung auseinander und verdeutlichte, dass Verschlüsselung etwa allein des Nutzernamens im Falle eines Differenzangriffs die Identifizierung der dahinter stehenden Person nicht verhindere. Vielmehr seien Möglichkeiten des Verrauschens von Datenvolumina ergänzend hinzuziehen. Vollkommene Anonymität sei in Zeiten von Big Data angesichts des stetig steigenden Zusatzwissens zunehmend schwieriger zu erreichen.

2. Welche Daten entstehen überhaupt beim Betrieb von Fahrzeugen?

[Rz 9] Jörg Arnold vom forensischen Institut Zürich referierte zu Datenrechten aus Sicht der Beweissicherung bzw. erläuterte zunächst einmal die digitalen Spuren, die bei der Nutzung smarter Fahrzeuge entstehen. So wird neben anderen personenbezogenen Daten (Standortdaten, Dashcam-Daten, Navigationsdaten) auch die sog. Vehicle Identification Number (VIN) erhoben, die eine fahrzeugscharfe Nutzung ermöglicht. Am Beispiel des Event Data Recorders (EDR) zeigte Arnold die Nutzungsmöglichkeiten solcher Daten auf – die aus seiner Sicht etwa bei Verdacht auf Begehung einer Straftat von den Strafverfolgungsbehörden gesichert werden dürfen, unabhängig davon, wer daran Rechte geltend macht. Dass Autodaten in einem Rechtsstreit den Beteiligten zur Verfügung stehen müssen, illustrierte er anhand der Verurteilung von General Motors (GM) in den USA zur Veröffentlichung bzw. Zugänglichmachung der Daten aus dem EDR im Zusammenhang mit Unfällen. Gleichzeitig wies er auf die Möglichkeit für GM hin, mittels der EDR-Daten einen Nachweis im Rahmen der Produkthaftung führen zu können.

[Rz 10] Abschließend verwies er auf die Tatsache, dass etwa das Fahrzeugmodell Corvette seit 2015 in der EU bereits vollständig mit einem Performance Data Recorder ausgestattet werde, womit die Möglichkeit für eine umfassende Datenerhebung aus dem Auto nun theoretisch verfügbar ist, jedoch praktisch auch noch durchgesetzt werden muss – unabhängig von der normativen

10 Daniela Mielchen, Verrat durch den eigenen PKW – wie kann man sich schützen?, SVR 2014, 81 (83); Hornung/Goeble (Fn. 1), 265; Max von Schönfeld, Ein fahrbarer Datensatz – Datenschutzrechtliche Probleme im modernen Auto, DAR 2015, 617 (618).

Zuordnung eines Datenrechts. Seine Beispiele führen vor Augen, welche Begehrlichkeiten und welches Interesse an mittels Fahrzeugen generierten Daten bestehen können.

3. Zulassung von Roboterautos und Änderung des Straßenverkehrsrechts

[Rz 11] Digitalisierung des Strassenverkehrs bedeutet vor allem auch den Einsatz von automatisierten Fahrzeugen: Mit Blick auf die Zulassung von Roboterfahrzeugen fokussierte Stefan Huonder vom ASTRA, angesichts der erwarteten Entwicklung, dass in den kommenden 20 Jahren mit dem Einsatz von Roboterautos sicher gerechnet werden kann[11], auf das Jahr 2040. Er legte dar, dass eine Steigerung der Autonomie der Fahrzeuge mit einer zunehmenden Pflichtbefreiung des Fahrers einhergehen müsse. Doch nach den heute geltenden Gesetzen, insbesondere dem ECE-Reglement bleibe der Fahrzeugführer auch im Falle autonomer Mobilität weiterhin verantwortlich.

[Rz 12] Insbesondere im Hinblick auf die Sicherheit im Straßenverkehr müsse auch der Nachweis der von autonomen Fahrzeugen erwarteten gesteigerten Sicherheit erst noch geführt werden. Denkbar seien dafür Simulationen. Am Beispiel der TESLA-Nutzungsbedingungen warf er die Frage auf, ob der Nachweis über die erforderliche Sicherheit künftig möglicherweise auch über Feldversuche oder Kilometerleistung erbracht werden könnte. Letztlich müsste aber vor allem gefragt werden, welches Sicherheitsniveau als ausreichend anzusehen sei und ob die Gesellschaft gegenüber Menschen fehlertoleranter sei als gegenüber der Technik.

[Rz 13] Zurzeit bestünden noch keine ausreichenden Nachweise, daher empfahl Huonder in dem bis Ende 2017 zu erwartenden Gesetzentwurf für ein neues Straßenverkehrsgesetz in der Schweiz Regelungen zu einer Pflichtbefreiung sowie für Feldversuche zu bewilligen.

III. Wem gehören Daten in der Wertschöpfungskette?

[Rz 14] Wem gehören Daten in einer Wertschöpfungskette? Wer darf über sie (alleine) verfügen? Dürfen andere auf diesen Daten basierende Geschäftsmodelle aufbauen? Die Brisanz dieser Frage zeigt sich besonders deutlich, wenn Daten – etwa im Rahmen eines WebObservatory – visualisiert und für Entscheidungsgrundlagen sowie Geschäftsprozesse anschaulich dargestellt werden.

1. Analyse von Geschäftsmodellen anhand von Visualisierungen

[Rz 15] Alexander Gröfflin von der Universität Basel stellte ein solches WebObservatory-Projekt vor, das nachvollziehbar macht, wie car-sharing-Angebote in Basel genutzt werden. Unter der Domain webobservatory.io/dmi.unibas.ch wird die Nutzung unter verschiedenen Gesichtspunkten (Standort, Tankfüllung etc.) einzelner car-sharing-Angebote visualisiert. Dafür werden grundsätzlich allgemein zugängliche Daten wie Verfügbarkeit von Autos an bestimmten Orten, Preise und Tarife, aber auch Suchmaschinenranking, öffentlicher Verkehr und Preise mittels eines Da-

11 http://www.pwc.de/de/pressemitteilungen/2015/pwc-prognose_autonomes-fahren-setzt-sich-zwischen-2025-und-2030-durch.html.

tentools erfasst, gespeichert und auf Muster untersucht. Auf diese Weise lassen sich beispielsweise häufige Start- und Endpunkte, aber auch individuelle Nutzerprofile erstellen.

[Rz 16] Basierend auf diesen Erkenntnissen lassen sich Geschäftsmodelle entwickeln – nicht nur durch denjenigen, der die Daten ursprünglich generiert hat (hier: das car sharing-Unternehmen), sondern auch durch andere, denen diese Daten – bei erstem intuitiven Beurteilen – nicht gehören, wie beispielsweise Konkurrenten. Fraglich ist, ob ein solches «zwangsweises Teilen» von Kunden- und anderen Daten eine valide Grundlage für Geschäftsmodelle werden sollte. Hier könnten sich nicht nur datenschutzrechtliche Risiken für die Betroffenen, sondern auch Konflikte im Wettbewerb der Firmen untereinander entwickeln, die Auswirkungen für den Markt, für Anbieter und Konsumenten haben könnten.

[Rz 17] Es erscheint verfrüht hier bereits endgültige Aussagen über Datenrechte zu machen, Auch hier zeigt der Strassenverkehr paradigmatisch Probleme auf, etwa durch den Umstand, dass im vernetzten Verkehr selten ein Datum Aussagen nur über eine Person trifft. Vielmehr sind häufig zugleich mehrere Personen betroffen, die im Auto sitzen oder als andere Fahrzeugführer am Verkehr teilnehmen. Vor dem Hintergrund dieser Mehrrelationalität wird ein Ausschließlichkeitsrecht an Daten kritisch hinterfragt.[12]

[Rz 18] Müssten vor diesem Hintergrund Regulierungsbehörden vielmehr Datensparsamkeit verpflichtend vorgeben, um diesen und weitere Konflikte zu entschärfen?

[Rz 19] Auf europäischer Ebene ist der Grundsatz der Datensparsamkeit bereits in Art. 8 der Charta der Grundrechte der Europäischen Unionstatuiert. Danach sind nur so viele personenbezogene Daten zu erheben, wie wirklich erforderlich ist oder anders gesagt: Es sind so wenig personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen, wie irgend möglich[13], worauf auch der kantonale Datenschutzbeauftragte Basel-Stadt Beat Rudin einen Schwerpunkt in seinem Vortrag legte. Datensparsamkeit kann natürlich auch bedeuten, dass weniger Daten zur Verfügung stehen, die den Fahrer be- oder entlasten. Hier könnte oder müsste man also vielmehr überlegen, inwieweit die Zulassung von Roboterautos an eine Pflichtbefreiung des Fahrers gekoppelt wird.

2. Gehören die Daten dem, der für sie verantwortlich ist?

[Rz 20] Phillip Brunst vom Cyber Crime Research Institute Köln fasste wesentliche IT- und auch datenschutzrechtliche Prinzipien im Zusammenhang mit intelligentem Verkehr zusammen: Vertraulichkeit, Verfügbarkeit und Integrität gehören zu den Pfeilern der Informationstechnik.

[Rz 21] Unter diesem Blickwinkel beurteilte er den Umgang mit Daten aus autonomen Fahrzeugen.

[Rz 22] Fahrzeugdaten, Fahrerdaten, Standortdaten und Mobilfunkdaten würden maßgeblich vom Prinzip der Vertraulichkeit betroffen. Würden diese abhandenkommen, sei die Vertraulichkeit verletzt. Auch das Prinzip der Verfügbarkeit betreffe das Fahrzeug insgesamt. Betroffen sei es beispielsweise in dem Fall, wenn ein PKW-Hersteller den PKW bei ausbleibender Ratenzahlung abschalte.

12 Specht/Rohmer (Fn. 1), 127 (130).

13 von Schönfeld (Fn. 10), 617 (620).

[Rz 23] Integrität betreffe dagegen beispielsweise die Frage eines möglichen Versicherungsbetruges durch Veränderung der Daten/Fahrzeugparameter. Aus Datenschutzperspektive sei dem Grundsatz der Transparenz und Datensparsamkeit großes Gewicht beizumessen. Nur mit ausreichender Transparenz sei Selbstdatenschutz der Nutzer letztlich wirksam zu ermöglichen.

[Rz 24] Hierzu gehöre ein Protokoll der abgerufenen Daten und eine Spezifizierung der Meldepflichten. Hinsichtlich des Datenschutzprinzips der Datensparsamkeit warf Brunst die Frage auf, ob Daten wirklich immer online verfügbar sein müssen oder ob nicht eine lokale Speicherung reiche. Schließlich betonte Brunst die Vorteile, die spezifische Freischaltmöglichkeiten durch Nutzer böten. Im Zusammenhang mit dem Strafrahmen bewertete Brunst Datenmissbrauch als reines Datenschutzproblem.

3. Dateneigentum aus zivilrechtlicher Perspektive

[Rz 25] Im Zentrum der jüngeren Diskussion[14] stehen unterschiedliche Überlegungen zu Eigentumsrechten an Daten aus zivilrechtlicher Perspektive.

[Rz 26] Herbert Zech von der Universität Basel stellte in Frage, ob es für Daten überhaupt ein Recht geben könne, das dem Eigentumsrecht nachempfunden wird, oder anders formuliert: Ob in Bezug auf Daten rechtliche Exklusivität erforderlich sei. Zur Beantwortung der Fragen nutzte er die ökonomische Analyse des Rechts. Er differenzierte zwischen privaten und öffentlichen Gütern. Entscheidende Kriterien für eine eigentumsrechtliche Klassifizierung von Gütern sind die Rivalität und Ausschließbarkeit. Ein öffentliches Gut ist durch drei Kriterien gekennzeichnet: Es ist nicht-ausschließbar, nicht-rival und es ist einer Abnutzung nicht zugänglich. Unter Rivalität ist die Verhinderung des Konsums eines Gutes durch einen Nutzer zulasten anderer zu verstehen. Ausschließbarkeit bedeutet, dass den Nutzern der Konsum eines Gutes vorenthalten bzw. an bestimmte Bedingungen (z.B. Bezahlung) geknüpft werden kann. Sachenrechtliche Regelungen, die analog für Daten herangezogen werden könnten, implizierten mindestens im Punkt «nicht-Rivalität» eine gegenteilige Eigenschaft der Sache als bei einem öffentlichen Gut. Während ein öffentliches Gut zur gleichen Zeit von verschiedenen Individuen konsumiert werden kann, kann eine Sache, an der das Eigentum zugeordnet wurde, nur von dem Eigentümer oder von einer Person, die von ihm abgeleiteten Rechte innehält, genutzt werden.

[Rz 27] Ausgehend von seinem vorläufigen Befund – es gebe kein Eigentumsrecht an Daten – zog er weiter bereits bestehende Regelungen wie den Datenschutz, den Geheimnis- und den Investitionsschutz heran, um zu prüfen, inwieweit sich aus diesen Regelungen eventuelle neue Rechte an Daten herleiten ließen. Er kam zu dem Schluss, dass diese Regularien durchaus Rechte gewährten, diese sich aber nicht mit einem «Eigentum an Daten» vergleichen ließen. So gewährt Datenschutz einen Persönlichkeitsschutz, der nicht verfügbar ist im Sinne eines Eigentumsschutzes. Auch biete das Strafrecht Möglichkeiten, sich einer Löschung zu verwehren. Ein Zugangsrecht im Sinne eines «Dateneigentums» sei daraus aber nicht ableitbar. Abzuwarten blieben Entwicklungen auf europäischer Ebene etwa in Bezug auf ein etwaiges Datenerzeugerrecht.

---

14 Grützmacher (Fn. 1), 485 ff.; Specht/Rohmer (Fn. 1), 127 ff.; Dorner (Fn. 1), 617 ff.; Hornung/Goeble (Fn. 1), 265 ff.; Heun/Assion (Fn. 1), 812; OLG Dresden, NJW-RR 2013, 27; Schefzig (Fn. 1), 3 ff.; Schwartmann/Hentsch (Fn. 1), 117 ff.

IV. Wer darf die Daten vor Gericht nutzen?

[Rz 28] Die Frage nach einem Dateneigentum wird auch gestellt, um zu klären, wer Daten etwa vor Gericht benutzen darf. Wer darf vor Gericht verlangen, dass sie benutzt werden und wer darf mit ihnen Beweis führen?

1. Beweislastfragen im Zivilprozess

[Rz 29] Diese Frage war zentral für den Vortrag von Ruth Janal von der Freien Universität Berlin. Sie befasste sich insbesondere mit der Beweislast im deutschen Zivilprozess und skizzierte die unterschiedlichen Interessenkonstellationen im Zusammenhang mit autonomen Fahrzeugen. Als Interessenten kommen Betreiber, Eigentümer, Halter, Führer, Versicherung, Hersteller, Werkstatt, Händler, mithin eine große Anzahl möglicher Beteiligter in Betracht.

[Rz 30] Kern ihres Vortrags war die Untersuchung der Frage, ob Fahrzeug- und Fahrzeugführerdaten im Zivilprozess verwertet werden können.

[Rz 31] Am Beispiel von eCall, dem für alle neu zugelassenen Fahrzeuge ab 2018 verpflichtenden Notrufsystem, speichert das Notrufsystem Unfalldaten und es besteht eine ausdrückliche Auslesemöglichkeit für Dritte. Jedoch ist damit noch nicht die Frage geklärt, wie ein Unfallbeteiligter an die Daten kommen kann. In der Vergangenheit sei vielfach eine Verweigerungshaltung seitens der Hersteller festzustellen gewesen, Daten auszulesen.

[Rz 32] Auch nach dem Benutzerhandbuch von Tesla werden Daten nur bei einem entsprechenden Gerichtsbeschluss weitergegeben. Gleichzeitig behält sich Tesla vor, die Daten gerade bei Reparaturen im Rahmen eines Garantiefalles vorzubehalten und nicht offenzulegen. Diese Nutzungsbedingungen von Tesla zeigen aus Sicht der Referentin die Problematik, wie schwierig es für Unfallbeteiligte ist, einen Gerichtsbeschluss auf Herausgabe von Daten zu erwirken und dafür eine entsprechende materiell-rechtliche Grundlage zu finden.

[Rz 33] Ein Herausgabeanspruch aus Eigentum scheide aus, da der Unfallgegner weder Eigentümer des Fahrzeugs, noch des Datenträgers ist.

[Rz 34] Ein Anspruch aus § 34 Bundesdatenschutzgesetz (BDSG) scheide ebenfalls aus, da berechtigte Interessen Dritter und/oder Geschäftsgeheimnisse entgegenstünden.

[Rz 35] Eine Pfändung nach § 809 deutsche Zivilprozessordnung (ZPO) würde nur zu einer Inaugenscheinnahme des Fahrzeugs führen.

[Rz 36] Ob ein Herausgabeanspruch aus § 242 Bürgerliches Gesetzbuch (BGB) hergeleitet werden könne, wurde anschliessend an das Referat unter den Teilnehmern kontrovers diskutiert. So stehe bereits in Frage, ob eine Sonderrechtsbeziehung bestehe, ob der Fahrzeugführer Schuldner eines Hauptanspruchs sei und schließlich ob die Herausgabe der Daten zumutbar sei.

[Rz 37] Letztlich problematisierte Ruth Janal vor allem die Frage nach einem Recht auf Anordnung zur Vorlage eines Gegenstands nach § 144 ZPO. Problematisch sei zwar schon, dass Daten nicht, wie normalerweise Gegenstände, körperlich fassbar seien. Bei vorhandener Verfügungsgewalt über den Datenträger oder Zugriff auf Passwörter und Auslesewerkzeuge könne jedoch darauf zugegriffen werden. Fraglich sei aber darüber hinaus, wem gegenüber die Anordnung zur Vorlage eines Gegenstands ausgesprochen werden könne. Kommen Dritte, wie etwa der Pkw- oder Softwarehersteller in Betracht, denen unter Umständen Zeugnisverweigerungsrechte oder berufliche Verschwiegenheitspflichten zustehen, die einer Herausgabe entgegenstünden? Schließlich

könne eine Anordnung gegenüber einer gegnerischen Partei an der fehlenden Durchsetzbarkeit unter dem Aspekt der Vermögensgefährdung des Herstellers und Wahrung der Geschäftsgeheimnisse scheitern.

[Rz 38] Letztlich bleibe einem Gericht wohl nur der Weg über eine Kenntnisnahme der Daten im Wege freier Beweiswürdigung. Diese Lösung setze aber einen substantiierten Parteivortrag voraus, für den wiederum erforderlich ist, zu wissen, was tatsächlich passiert ist. Bei Unkenntnis über das konkrete Unfallgeschehen bzw. die nahe liegende Unfallursache sei auch dieser Weg für Unfallbeteiligte in der Regel nicht gangbar, um Kenntnis der Daten zu erhalten.

[Rz 39] Wenn ein Smart Key vorhanden ist, auf dem die erzeugten Daten gespeichert werden, könne unter Umständen auf die Daten auch im Zivilprozess leichter zugegriffen werden. Zwar müsse auch hier nach der Verwertbarkeit gefragt werden. Jedoch bestünden keine Anhaltspunkte für ein Beweisverwertungsverbot.

[Rz 40] Letztlich müsse man sich auch bei der Datenauswertung nach einem Unfall der Frage stellen, ob das Recht auf Wahrheitsfindung das Recht auf informationelle Selbstbestimmung überwiegt. Im Rahmen der Abwägung müssen die unterschiedlichen Interessen Beachtung finden. Maßgeblich für die Abwägung sei insbesondere das Gewicht des Eingriffs, ob es sich um Innenraumüberwachung handele, inwiefern Umweltdaten, also Daten von Unbeteiligten betroffen seien etc.

[Rz 41] Schließlich müsse zudem noch immer die Qualität der Daten kritisch hinterfragt werden, etwa im Hinblick auf Manipulierbarkeit durch den Hersteller, hinsichtlich ihrer Formate, hinsichtlich ihrer Standardisierung und auch im Hinblick auf etwaige nicht ausreichende Sicherheit.

[Rz 42] De lege ferenda schlägt die Referentin vor, die Vermutungsregeln bei Produktfehlern der Hersteller anzupassen.

[Rz 43] Darüber hinaus empfahl sie beim Einsatz von Unfalldatenspeichern eine klare Regelung hinsichtlich der Zugriffsrechte für alle Unfallbeteiligten zu schaffen, für eine Harmonisierung der Daten und Programmformate zu sorgen und eine unabhängige Stelle zur Prüfung von Software zu schaffen.

2. Beschlagnahmemöglichkeiten der Staatsanwaltschaft

[Rz 44] Die für das zivilrechtliche Verfahren erörterten Fragen stellen sich in ähnlicher Weise auch im Strafprozess.

[Rz 45] Alberto Fabbri, der Erste Staatsanwalt der kantonalen Staatsanwaltschaft Basel-Stadt skizzierte aus Perspektive der Ermittlungsbehörden die Herausforderung einer Digitalisierung des Individualverkehrs und zählte beispielhaft Normen der schweizerischen Strafprozessordnung (StPO) auf, die im Zusammenhang mit intelligentem Verkehr Relevanz erlangen können.

[Rz 46] Nach Art. 6 StPO ist die Staatsanwaltschaft kraft Amtes zur Ermittlung aller belastenden wie entlastenden Umstände einer mutmasslichen Straftat verpflichtet.

[Rz 47] Bereits Art. 179 StPO kann im Zusammenhang mit smarten Fahrzeugen Schwierigkeiten bereiten. Danach dürfen nicht beschuldigte Personen nicht in die Ermittlungen einbezogen werden.

[Rz 48] Auch Art. 246 StPO, der die Datenträgerdurchsuchung behandelt, kann im Zusammenhang mit autonomen Fahrzeugen Relevanz erlangen, wonach Aufzeichnungen, Datenträger sowie

Anlagen zur Verarbeitung und Speicherung von Informationen durchsucht werden können, wenn zu vermuten ist, dass sich darin Informationen befinden, die der Beschlagnahme unterliegen.

[Rz 49] Schließlich ging Alberto Fabbri auf die Erhebung von Daten als gerichtsverwertbare Beweismittel und die Schnittstelle zwischen polizeilichen und staatsanwaltschaftlichen Ermittlungen ein: Fällt die Datenerhebung nach einem Verkehrsunfall in die der Polizeizuständigkeit unterliegende Spurensicherung? Da die Staatsanwaltschaft das Verfahren führt und nur diese nach Art. 308 und 309 StPO Zwangsmittel einsetzen könne, sei diese Frage entgegen des vermeintlich eindeutigen Wortlauts des Art. 306 nicht ohne Weiteres zu beantworten. Der Zugriff gestalte sich bei Datenspeicherung im Fahrzeug vergleichbar mit dem Datenzugriff bei einer Bank. Dieser könne nur mithilfe der Bank, vergleichbar also beim Fahrzeug mithilfe des Herstellers, erfolgen. Gleichzeitig müssten aber in diesem Zusammenhang immer auch die Zulässigkeitsvoraussetzungen der Fernmeldeüberwachung beachtet werden. Auch stelle sich überhaupt die Frage, gegen wen sich der Tatverdacht zu richten habe: Gegen den Hersteller, den Entwickler, Programmierer, Provider, Vertreiber? In diesem Kontext müsste insbesondere die Problematik einer transnationalen Datenerhebung und vor allem -speicherung geklärt werden. Die internationale Zusammenarbeit gewinne hier erheblich an Bedeutung.

[Rz 50] Fabbri stellte zum Abschluss seiner Ausführungen zur Debatte, ob der Mensch durch die Autonomisierung von Fahrzeugen und Geräten zunehmend an Subjekteigenschaft verliere und die Gefahr bestünde, im Strafverfahren zum Objekt zu werden? Rundumüberwachung führe zu einer überragenden Techniklastigkeit, sodass in Zukunft Befragungen möglicherweise unnötig würden? Außerdem stellte er in diesem Zusammenhang die Frage nach der Durchsetzbarkeit des nemo-tenetur-Grundsatzes im Strafverfahren. Die Fragen wurden vom Teilnehmerkreis in einer lebhaften Diskussion aufgegriffen.

[Rz 51] Aus der Perspektive des Fahrers oder Fahrzeugeigentümers als natürlicher Person erscheint es naheliegend, die bereits skizzierten Fragen mit dem vorhandenen Datenschutzrecht zu beantworten. Kann der Betroffene aber wirklich mit den Daten im Sinne eines «Meine Daten gehören mir» umgehen?

V. Datenschutz

[Rz 52] Den Abschluss der Tagung bildete ein Vortrag des kantonalen Datenschutzbeauftragten Basel-Stadt Beat Rudin. Er skizzierte die bevorstehenden Gesetzesanpassungen in der Schweiz parallel zur Entwicklung der EU-DSGVO und der Europaratskonvention 108. Datenschutz sei Verkehrsrecht, wobei nach wie vor dieselben Prinzipien gelten würden.

[Rz 53] Viele Anwendungen im Zusammenhang mit intelligentem Verkehr können Big Data-Charakter erlangen, also beispielsweise auf der Basis vieler Fahrzeug- und Verkehrsteilnehmerdaten für Optimierung der Verkehrsflüsse für mehr Sicherheit oder sonstige erwartete Nutzen sorgen. Hier sei aber unbedingt zu beachten, dass durch die Steigerung von Zusatzwissen Möglichkeiten zur nachhaltigen Anonymisierung ursprünglich personenbezogener Daten gemindert würden, sodass Datenschutzaspekte zunehmend auch im intelligenten Verkehr Relevanz erlangten.

[Rz 54] Zwar sei nach wie vor das Grundprinzip zu beachten, dass Betroffene in die Datenverarbeitung einwilligen können müssten. Allerdings sei vor diesem Hintergrund, insbesondere im Zusammenhang mit Big Data-Anwendungen die Anforderungen an Form und Inhalt einer be-

wussten und freiwilligen Einwilligung immer schwerer umsetzbar. Theoretisch sei zwar durchaus die Anwendung skalierbarer Einwilligungen mit verschiedenen Optionsmöglichkeiten für Betroffene denkbar. Jedoch liege gerade in dem Gegensatz zwischen dem Wert personenbezogener Daten für den Betroffenen und dem wirtschaftlichen Vorteil von Big Data-Anwendungen für Unternehmen eine strukturelle Schwäche des Persönlichkeitsschutzes.

[Rz 55] Denkbar wäre hier als gesetzgeberischen Vorschlag zu prüfen, ob die Beweislastregeln zu Gunsten der Nutzer entwickelt werden sollten. Jedoch würde eine solche Regelung insofern kritisch zu hinterfragen sein, dass die Datenerhebung durch den Anbieter/Betreiber dann als Entlastungsverpflichtung zum Schutz des Nutzers gerechtfertigt werden würde.

[Rz 56] Abschließend stellte Beat Rudin verschiedene parlamentarische Initiativen einzelner Abgeordneter vor. Diese betreffen ein Recht auf Kopie der Daten sowie die Forderung nach einer verstärkten Kontrolle der Daten durch die Betroffenen und wurden als Einzelinitiativen ins Parlament eingebracht.

VI. Fazit

[Rz 57] Die Tagung bot einen guten 360° Blick auf das Thema «Dateneigentum». Gemeinsam war allen Vorträgen das Ergebnis: Datenschutz muss in einem digitalisierten Verkehr immer mitgedacht werden. Datenschutzrecht stellt als Querschnittsmaterie eine Grundordnung für den Umgang mit personenbezogenen Daten auf.[15] Jedoch darf nicht außer Acht gelassen werden, dass (zumindest das deutsche) Datenschutzrecht auf der Grundlage einer selbstbestimmungsorientierten Konzeption entwickelt worden ist.[16] Die sich daraus ergebenden Verfügungs- und Kontrollrechte sollen der individuellen Selbstentfaltung als Funktionsbedingung für einen demokratischen Prozess dienen und wurden vom Bundesverfassungsgericht eng mit der Menschenwürde verknüpft. Menschenwürde und demokratischer Prozess sind aber keine handelbaren Güter.[17] Zwar legt das Datenschutzrecht, das als Verbot mit Erlaubnisvorbehalt konstruiert ist, die Möglichkeit nahe, von «eigenen» Daten zu sprechen[18], in deren zulässige Verarbeitung der Betroffene ausdrücklich einwilligen oder eine sonstige Rechtsgrundlage vorliegen muss. Allerdings darf in diesem Kontext nicht außer Betracht gelassen werden, dass der durch Einwilligung oder Vertragsschluss vorliegende «Handel» mit Daten mangels Transparenz der Datenverarbeitung im derzeitigen Stadium gerade nicht auf Augenhöhe erfolgt, sondern vielmehr von einer enormen Asymmetrie in der Verhandlungsmacht geprägt ist.[19] Ein Ansatzpunkt für eine Regelung von Dateneigentum kann vor diesem Hintergrund kaum ohne Weiteres dem Datenschutzrecht entnommen werden, da dieses selbstbestimmungsorientiert konzeptioniert, aber nicht auf einen «Alleingebrauch» gerichtet ist.

---

15 Hornung/Goeble (Fn. 1), 265 (269).

16 BVerfGE vom 15. Dezember 1983 «Volkszählungsurteil»; zum Charakter des Allgemeinen Persönlichkeitsrechts vgl. auch: Herbert Zech, «Industrie 4.0» – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1154).

17 Hornung/Goeble (Fn. 1), 265 (269); Zech (Fn. 1), 137 (141); Specht/Rohmer (Fn. 1), 127 (132).

18 Hornung/Goeble (Fn. 1), 265 (270); Specht/Rohmer (Fn. 1), 127 (129).

19 Hornung/Goeble (Fn. 1), 265 (270); Dorner (Fn. 1), 617 (624).

[Rz 58] Auch die gesetzlichen Wertungen im Bereich des geltenden Immaterialgüter- und Geheimnisschutzes eröffnen auf den ersten Blick keine Möglichkeit der Anerkennung eines zivilrechtlichen Dateneigentums im Wege richterlicher Rechtsfortbildung.[20]

[Rz 59] Die Interessenkonflikte, die im digitalisierten Strassenverkehr und bei Einsatz (hoch)automatisierter Fahrzeuge beispielhaft auftreten, illustrieren jedoch das Bedürfnis nach einer Rechtsreform. Insbesondere die strukturelle Machtasymmetrie in der Verhandlungssituation zwischen den Datensubjekten und den mit dem Datenhandel befassten Unternehmen spricht für das Bedürfnis, Regelungen für ein Dateneigentum de lege ferenda zu entwickeln.[21]

[Rz 60] Und wem gehören jetzt die Daten, die künftig im Intelligenten Verkehr generiert werden? Das ist noch offen und muss in den kommenden Jahren durch Experten aus unterschiedlichen Gebieten im Austausch mit der Zivilgesellschaft eruiert und mit Hilfe neuer Rechtskonzepte herausgearbeitet werden. Wesentlich dafür sollte, wie durch die unterschiedlichen Referenten der Tagung bereits angedeutet, der nötige Interessenausgleich zwischen Persönlichkeits- und Wertschöpfungsinteressen sein.

RAin Christine Möhrke-Sobolewski ist als Syndikusanwältin tätig und berät im Konzerndatenschutz der Deutschen Bahn AG zu telemedien-, telekommunikations- und allgemein datenschutzrechtlichen Fragestellungen der Konzernleitung. Seit November 2016 ist sie Doktorandin an der Universität Basel bei Prof. Dr. Sabine Gless.

20 Dorner (Fn. 1), 617 (625); Zech (Fn. 1), 137 (141); Specht/Rohmer (Fn. 1), 127 (132); Schwartmann/Hentsch (Fn. 1), 117 (126).

21 Dorner (Fn. 1), 617 (626).