DATENSCHUTZ IM AUTO DER ZUKUNFT

ÜBER DAS SPANNUNGSFELD ZWISCHEN AUTONOMEM FAHREN UND DATENAUTONOMIE

Der prognostizierte Wandel der Automobilität hin zu autonomen Fahrzeugen stellt insbesondere den Datenschutz vor neue Herausforderungen. Hierfür müssen im Interesse aller Beteiligten Lösungen gefunden werden.

Vorhersagen über die Zukunft sind stets gewisse Unwägbarkeiten immanent. Nicht anders ist es, wenn man auf die Zukunft der Automobilität zu sprechen kommt. Überraschenderweise scheinen jedoch an einem Punkt kaum Zweifel zu bestehen: Das Auto der Zukunft wird ein autonom fahrendes sein. Wenn von autonomem Fahren gesprochen wird, ist damit im technischen Sinn vollautomatisiertes Fahren gemeint, also ein sich völlig selbstverantwortlich bewegendes Fahrzeug, auf dessen Fortbewegung die Insassen keinen Einfluss mehr nehmen müssen. Während es nach dem antizipierten Fortschreiten der hierfür benötigten Techniken bald schon möglich wäre, solche vollautomatisierten Fahrzeuge auf den Markt zu bringen,[1] hinken die Diskussionen über die hierdurch aufgeworfenen rechtlichen und gesellschaftlichen Fragen dem Stand der Technik hinterher. Ungeklärt sind im Wesentlichen drei Kernbereiche: Cybersecurity, Haftungsrecht und Datenschutz. Während sich für Hacker durch die unverzichtbare Vernetzung solcher Fahrzeuge faszinierende Möglichkeiten der Manipulation von Streckennetzen und Fahrrouten ergeben (Cybersecurity), ist ebenfalls die Frage der Haftung für Unfälle und das Entscheidungsverhalten vollautomatisierter Fahrzeuge (Haftungsrecht) weitgehend ungeklärt. Beides soll nicht Gegenstand dieses Beitrages sein.[2] Vielmehr soll es an dieser Stelle darum gehen, die datenschutzrechtlichen Aspekte des vollautomatisierten Fahrens zu skizzieren. Wie verträgt sich dessen technische Ausgestaltung mit unserem heutigen Verständnis von Datenschutz? Und wem „gehören" eigentlich die im Auto oder durch das Auto produzierten Daten und wer soll hierauf zugreifen dürfen?

Tatsächliche Neuerungen durch das autonome Fahren

Die Vorstellung eines völlig autonom fahrenden Autos sollte zunächst keine Dystopie sein. Das von menschlichem (Fehl-)Verhalten entkoppelte, vollautomatisierte Fahren verspricht zum einen eine deutliche Reduzierung von Verkehrsunfällen.[3] Zum anderen bringt es Bequemlichkeit, uneingeschränkte Mobilität auch für fahruntüchtige Personen (Blinde, Kinder, Senioren) sowie einen beachtlichen Zeitgewinn, indem bisherige Lenkzeit zu Freizeit wird. Allerdings entsteht hierbei auch eine riesige Masse an Daten. Im vollautomatisierten Fahrzeug gibt es zwei zu unterscheidende Datenquellen: Durch das Auto selbst gewonnenen Daten, die dadurch entstehen, dass das Fahrzeug in Echtzeit seine Umgebung scannt und über eine Cloud auch mit anderen Fahrzeugen im Austausch steht. Zum anderen die im Auto generierten Daten, die durch die Konsumenten im Auto entstehen, wenn während der Fahrt im Internet gesurft oder auf Infotainment Angebote der Bordelektronik zurückgegriffen wird. Aus der Verarbeitung all dieser Daten hofft die Automobilindustrie, neue Gewinne erzielen zu können. Bisher erfolgt die Gewinngenerierung der Automobilhersteller im Wesentlichen durch das Zusammensetzen von Zuliefererteilen und der Vermarktung. Das Auto ist das eigentliche Produkt. Im vollautomatisierten Auto erfolgt die Wertschöpfung nicht mehr bloß aus dem Auto an sich, sondern aus der Verarbeitung der erhobenen Daten.[4] Das Auto als materieller Wert tritt hinter die immateriellen Daten zurück. Dies ist keine Wunschvorstellung der Autohersteller, sondern marktwirtschaftliche Analyse. Das monetäre Potential, das im Verkauf von Datenprodukten und Datendienstleistungen steckt, ist riesig. Eine konservative Schätzung kommt auf einen Wert von 1,44 Milliarden US-$ pro Tag[5] – vorausgesetzt, jedes Auto auf der Welt fahre autonom und die einstige Lenkzeit würde ausschließlich durch Internetnutzung gefüllt. Die Automobilindustrie ist somit im Begriff, ihre Wertschöpfungsdynamiken massiv umzustellen. Die Wertgenerierung durch die im Auto erhobenen Daten funktioniert hierbei genauso wie bei der Nutzung von Smartphones, Tablets und Computern: Durch Infotainment Angebote und dem Schalten personalisierter Werbung können diese Daten kommerzialisiert werden. Doch auch für die durch das Auto

1 Digitalchef des VW-Konzerns sprach kürzlich gegenüber der ZEIT von drei Jahren bis zur Umsetzung erster Mobilitätsflotten, http://www.zeit.de/mobilitaet/2018-01/johann-jungwirth-volkswagen-digitalchef-autonome-autos (Stand aller Links: 26.02.2018).

2 Weichert, Straßenverkehrsrecht – Zeitschrift für die Praxis des Verkehrsjuristen (SVR) 2014, 241 (244 f.) und Lüdemann, Zeitschrift für Datenschutz (ZD) 2015, 247 (251); Bodungen/Hoffmann, Neue Zeitschrift für Verkehrsrecht (NZV) 2016, 449 ff. und NZV 2016, 503 ff.

3 Lutz, Neue Juristische Wochenschrift (NJW) 2015, 119; Kütük-Markendorf/Essers, MultiMedia und Recht (MMR) 2016, 22 (23).

4 Stürmer/Schinzel, FIfF-Kommunikation 3/ 2017, 26 (26 f).

5 Stürmer/Schinzel, FIfF-Kommunikation 3/2017, 26.

erhobenen Daten finden sich vielfältige Vermarktungsmöglichkeiten: Die Standortdaten können an Staumeldedienste verkauft werden, die Wahrnehmung von Witterungsbedingungen an Wetterdienste. Die Mautzahlung könnte direkt durch das Auto erfolgen, alternative Routen an Navigationsdienste weitergeleitet werden. Die Möglichkeiten sind schier unendlich.[6]

Technische Funktionsweise autonomer Fahrzeuge

Neben dem Aspekt der veränderten Wertschöpfung ist aus datenschutzrechtlicher Sicht insbesondere interessant, wie das vollautomatisierte Fahren rein technisch funktioniert und welche Daten hierzu erhoben werden müssen. Welcher Ausstattung bedarf also ein Auto, um vollautomatisiert fahren zu können? Die Steuerungsfunktionen eines manuell gesteuerten Autos sind recht simpel. Sie beschränken sich auf drei Richtungsvektoren: Gas, Bremse und Lenkung. Die eigentliche „Arbeit", also die Steuerung und Kombination dieser Parameter übernimmt die Fahrer*in. Diese nimmt die Umgebung wahr, analysiert das Fahrverhalten anderer Fahrzeuge und reagiert auf potentielle Gefahrenquellen. Genau diese Aufgabe wird in Zukunft das vollautomatisierte Auto selbständig erledigen müssen, sprich: Es wird lernen müssen, seine Umgebung zu „verstehen" und aus diesem „Verständnis" heraus die richtigen Schlüsse für das Fahrverhalten zu ziehen. Grundvoraussetzung hierfür ist zunächst, dass das Auto seine Umgebung in Echtzeit über Sensoren und Kameras scannt und somit ein digitales Abbild seiner Umgebung erstellt. Es muss dann die für den Verkehr relevanten Muster erkennen (z.B. ein Zone-30-Schild), diese Muster interpretieren (also die Relevanz der Objekte erfassen) und daraus die richtigen Schlüsse ziehen (die Geschwindigkeit anzupassen). Die Interpretationsleistung dieser Autos ist enorm. Damit nicht jedes einzelne Fahrzeug jede einzelne Gefahrenquelle selbst interpretieren muss, werden die „Erfahrungen" eines einzelnen Autos an eine Datencloud übersandt und allen anderen Fahrzeugen in Echtzeit mitgeteilt. Auto A erkennt ein Schlagloch, leitet die Information an die Cloud weiter und in Sekundenbruchteilen soll das sich hinter Auto A befindliche Auto B ebenfalls von dem Schlagloch wissen, ohne es bisher selbst wahrgenommen zu haben. Zur technischen Umsetzung dieses Verfahrens haben die deutschen Autobauer Daimler, Audi und BMW in einer für sie ungewöhnlichen Synergie gemeinsam den Kartendienst Nokia Here gekauft.[7]

Jedes vollautomatisierte Fahrzeug erzeugt also einen Echtzeit-Scan des Verkehrs und seiner Umwelt und speist diese Erfahrungen in eine gemeinsame Cloud ein. Mehr noch, die „Erfahrungen" jedes einzelnen Fahrzeugs werden zur Selbstoptimierung des Kartendienstes mit anderen Fahrzeugen in Echtzeit geteilt, so dass sich die Masse an eingespeisten Daten exponentiell vervielfacht. Die Folgen dieses technischen Verfahrens sind immens, denn: In einer Welt voller autonomer Fahrzeuge wird man sich weder als Verkehrsteilnehmer*in noch als Passant*in einer solchen Erfassung verwehren können. Ein Auspixeln oder Ausschwärzen wie etwa heute bei Google Street View wird nicht mehr möglich sein. Ein „schwarzer Punkt" innerhalb des digitalen Kartennetzes würde einfach übergangen, sprich: überfahren.

Konsequenzen für den Datenschutz

Aus datenschutzrechtlicher Perspektive stellt diese Einsicht einen tiefen Einschnitt in das bisherige Verständnis des Prinzips der Einwilligung und des Prinzips der Datensparsamkeit (§§ 3a, 4a Bundesdatenschutzgesetz) dar. Wenn jedes Auto notwendigerweise seine ganze Umgebung scannt und ein Auspixeln nicht möglich ist, kann es jedenfalls nicht mehr auf die Einwilligung Unbeteiligter ankommen. Und auch das Prinzip der Datensparsamkeit, das im Kern fordert, nur solche Daten zu speichern, die für die Erfüllung des jeweiligen Zwecks erforderlich sind, verliert seine Zielrichtung: Wenn das ständige und umfängliche Erfassen aller sich um das Auto herum befindlichen Objekte zur technischen Notwendigkeit wird, ist eine ubiquitäre Datenerhebung unausweichlich. Wenn also die Erhebung riesiger Datenmengen ohne die Einwilligung aller Betroffenen die Grundvoraussetzung darstellt für das Gelingen dieser Technik, ist datenschutzrechtlich die entscheidende Frage, wie mit den erhobenen Daten umgegangen werden darf. Die Gefahren, die aus einer fehlenden oder einer nur unzureichenden Reglementierung entspringen, sind bekannt. Wenn alle Daten, die beim Autofahren entstehen, auch unbegrenzt genutzt werden dürfen, können von Herstellern, Versicherungen oder Staaten hochdetaillierte Verhaltens-, Bewegungs- und Persönlichkeitsprofile über die Insassen der Fahrzeuge erstellt werden.[8] Aus gesellschaftlicher und datenschutzrechtlicher Perspektive ist deshalb eine Reglementierung unverzichtbar. Indes hat auch die Automobilwirtschaft ein Interesse an möglichst beständigen Regelungen zur Datennutzung: Sie setzt darauf, ihre künftigen Gewinne zu erheblichen Teilen aus den Daten dieser Fahrzeuge erzielen zu können. Der Produktionszyklus eines neuen Autos beträgt circa sieben Jahre. Wenn sich innerhalb dieses Zeitraums die rechtlichen Rahmenbedingungen zur Verwertbarkeit von Daten ändern, ist der gesamte Produktionszyklus

Michael KR/CC-by-sa/4.0

gefährdet. Auch in der Politik ist man dementsprechend sensibilisiert für die Anfälligkeit der Automobilbranche hinsichtlich der Änderungen rechtlicher Rahmenbedingungen.

Schutz von Fahrzeugdaten durch das BDSG

Angela Merkel hat im vergangenen Jahr anlässlich der CEBIT die Frage aufgeworfen, wem denn nun die Daten gehörten, die beim vollautomatisierten Fahren entstünden, den Autoherstellern oder den Software-Unternehmen.[9] Bezeichnenderweise sind bei den Antwortmöglichkeiten die eigentlichen Verursacher*innen dieser Daten nicht einmal erwähnt – die Automobilnutzer*innen. Rechtlich gesehen gibt es kein „Dateneigentum" an generierten Datensätzen. Indes normiert das BDSG ein Selbstbestimmungsrecht für personenbezogene Daten, §§ 3 Abs. 1, 4 Abs. 1 BDSG. Personenbezogenen Daten sind hierbei alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[10] Bisweilen haben Automobilhersteller argumentiert, bei den erhobenen Daten handele es sich um fahrzeugbezogene, nicht um fahrerbezogene Daten. Zielrichtung dieser Argumentation war, das Schutzregime des BDSG auszuschließen, dessen Anwendungsbereich sich auf personenbezogene (und damit fahrerbezogene) Daten beschränkt. So verständlich die argumentative Position der Automobilhersteller ist, so wenig kann sie juristisch überzeugen: Sowohl bei den Sensordaten (also den durch das Auto erhobenen Daten) als auch bei den im Auto erhobenen Daten, handelt es sich um personenbezogene Daten iSd § 3 Abs. 1 BDSG.[11] Den Sensordaten, die das vollautomatisierte Fahren ermöglichen, haften verschiedene Identifikationsmerkmale an, die einen Rückgriff auf die Fahrzeuginsassen ermöglichen. Als nur ein Beispiel sei die Verknüpfung mit dem jeweiligen KfZ-Kennzeichen genannt. Dasselbe gilt für die Daten aus der Bordelektronik, also den im Auto erhobenen Daten: Das Auslesen dieser Daten und eine Re-Identifikation mit den Nutzer*innen (bspw. durch die Kennung der Mobilgeräte) ist recht problemlos möglich.[12] Damit weisen alle Daten vollautomatisierter Fahrzeuge den für das BDSG vorausgesetzten Personenbezug auf. Ein Abruf dieser Daten kann somit nach den §§ 3 Abs. 1, 4 Abs. 1 BDSG nur erfolgen, wenn eine Rechtsvorschrift dies ausdrücklich zulässt oder die Betroffenen einwilligen.

Die Idee eines „Dateneigentums"

Die Frage der Zugriffsberechtigung ist damit zumindest juristisch weitgehend geklärt. Ungeklärt ist die immer wieder aufkeimende Diskussion nach einem „Dateneigentum", auf die ein kurzer Blick durchaus lohnenswert ist. Es gibt viele Ansätze, wie sich ein solches Dateneigentum juristisch begründen ließe.[13] Gleichwohl ist die Diskussion irreführend. Zumindest aus datenschutzrechtlicher Sicht geht es nicht um die Frage einer Eigentumsposition, sondern um einen Datenzugangsanspruch. Interessant ist nicht, wer an etwas Eigentum erwirbt (und dieses ggf. weiterveräußert), sondern vielmehr, wer überhaupt befugt sein darf, auf die erhobenen Daten zuzugreifen. Bezeichnenderweise sind es gerade Versicherungsunternehmen und Autohersteller, die für ein Dateneigentum der Fahrzeughalter*innen plädieren.[14] Die Intention dahinter ist unschwer zu erkennen: Sie erhoffen sich hierdurch einen erleichterten Zugriff auf sensible Fahrzeugdaten. Die Automobilhersteller, um die Datenvermarktung abzusichern, die Versicherungsunternehmen, um – bisweilen auch durch richterlichen Beschluss – Unfälle aufzuklären oder die Tarifhöhe an das Fahrverhalten der Fahrzeughalter*innen anzupassen („pay as you drive").[15] Das Selbstbestimmungsrecht der §§ 3 Abs. 1, 4 Abs. 1 BDSG verbürgt ein Abwehrrecht der Konsument*innen gegen die unreglementierte Datennutzung von personenbezogenen Daten. Ein „Dateneigentum" hingegen würde als Instrument fungieren, um die Wertschöpfungsprozesse aus der Weiterverarbeitung dieser Daten abzusichern, weil eine Weiterveräußerung dieser Daten an die Hersteller sehr naheliegend wäre. Ein restriktiver Datenzugangsanspruch hingegen würde der Kommerzialisierung sensibler Daten effektiver entgegenwirken.

Wie sollte aber nun aus datenschutzrechtlicher Perspektive auf die antizipierten technischen Gegebenheiten reagiert werden? Wie bereits festgestellt, liegt die Entscheidung, ob personenbezogene Daten verwertet werden dürfen, bei den Fahrzeuginsassen. Wenn eine solche Einwilligung jedoch Grundvoraussetzung für das Funktionieren der Technik ist, wird sie für die Nutzung vollautomatisierter Fahrzeuge erteilt werden müssen – aus Sicht der Automobilhersteller dann im Rahmen einer Generaleinwilligung, die für sie alle Daten zugänglich macht.

Generaleinwilligung vs. informierte Zustimmung

Dies wäre sicher die datenschutzunfreundlichste Gestaltung, würde sie doch genau zu der uneingeschränkten Verwertbarkeit führen, die nicht im Interesse der Verbraucher läge und die deren Recht auf informationelle Selbstbestimmung als leere Hülle zurückließe. Wie könnte aber ein ausgewogener Ausgleich zwischen dem Datenschutz der Konsument*innen und den Vermarktungsinteressen der Industrie aussehen? Gerade hierfür ist die Unterscheidung zwischen den durch das Auto und den im Auto generierten Daten wichtig. Die Erhebung von Sensordaten ist unverzichtbar für das vollautomatisierte Fahren. Dies gilt jedoch nicht für das ubiquitäre Abgreifen und Auswerten von Daten aus der Bordelektronik, das lediglich monetären Interessen der Automobilhersteller dient. Insofern scheint eine Lösung bezüglich der durch das Auto erhobenen Daten in einer Anonymisierung nach § 3 Abs. 6 BDSG zu liegen.[16] Die an sich personenbezogenen Daten müssen derart anonymisiert werden, dass eine Re-Identifikation zwischen Datensatz und Person nicht oder nur mit unverhältnismäßig hohem Kostenaufwand möglich ist. Für das vollautomatisierte Fahren sind zwar Sensordaten notwendig, jedoch kein Personenbezug, sie könnten auch anonymisiert in die Datenmasse eingehen. Eine Cloud würde ebenso effektiv arbeiten, wenn sie weiß, wo Auto A und Auto B fahren, ohne dass sie weiß, wer die Insassen beider Fahrzeuge sind. Dasselbe gilt für viele Vermarktungsmöglichkeiten: Wetter- und Stau-

6 Vgl. Stürmer, Freiheit 2.0, Big Data Kolloquien, https://www.youtube.com/watch?v=7xSR665FBGU.

7 Milliarden-Deal: Deutsche Autobauer kaufen Nokias Kartendienst „Here", Tagesspiegel vom 3.8.2015.

8 Vgl. Lüdemann, ZD 2015, 247, 250.

9 Dachwitz, Dateneigentum: Merkel ist noch unsicher, ob unsere Daten Firma A oder Firma B gehören sollen, netzpolitik.org vom 20.03.2017.

10 Art. 4 EU-DSGVO; zum BDSG Lüdemann, ZD 2015, 247 (250) mwN.

11 Weichert SVR 2014, 201 (204); Lüdemann, ZD 2015, 247 (249 f.); Dix, Zeitschrift für Europäisches Privatrecht (ZEuP) 2017, 1 (2 f); EuGH, Urt. v. 19.10.2016 – C-582/14.

12 Vgl. Lüdemann, ZD 2015, 247 (250).

13 Drexl, Neue Zeitschrift für Kartellrecht (NZKart) 2017, 339 (340) mwN.

14 Vgl. Joachim Müller, Autos produzieren immer mehr Daten – mit dem richtigen Rahmen überwiegen die Chancen, Focus vom 14.02.2017.

15 Lüdemann, ZD 2015, 247 (248).

meldungen beispielsweise können auch ohne Personenbezug vermarktet werden. Eine datenschutzfreundliche Ausgestaltung erscheint bei den durch das Auto erhobenen Daten also greifbar. Schwieriger gestaltet sich dies bei den im Auto erhobenen Daten, bei denen sich der Datenschutz der Benutzer*innen und die Vermarktungsinteressen der Hersteller diametral entgegenstehen. Hier geht es gerade um die Nutzung ausschließlich personenbezogener Daten zu Vermarktungszwecken. Auch hier sollte es wieder darum gehen, Generaleinwilligungen zu verhindern und somit einer unkontrollierten Verwertbarkeit der Daten entgegenzuwirken.

Datenverarbeitung unter dem Regime der EU-DSGVO

Zur Erreichung dieses Ziels springt dem deutschen Datenschutzregime das EU-Recht zur Seite. In der seit Mai 2018 geltenden EU-Datenschutzgrundverordnung (EU-DSGVO) ist ein Kopplungsverbot angelegt. Art. 7 Abs. 4 EU-DSGVO normiert etwas schwammig, dass für die Freiwilligkeit einer Einwilligung in eine Datenverwertung berücksichtigt werden muss, ob die Verarbeitung dieser Daten für die Erfüllung des Vertrages erforderlich ist. Konkretisierend normiert der Erwägungsgrund 43 Satz 2 der EU-DSGVO jedoch sehr deutlich, dass die Einwilligung nicht als freiwillig gilt, wenn „die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist." Damit wird verhindert, dass der Vertragsschluss (der Autokauf) davon abhängig gemacht werden darf, dass die Betroffenen eine Generaleinwilligung zur Datenverarbeitung der Autohersteller erteilen müssen für solche Daten, die für die eigentliche Dienstleistung (die Beförderung) nicht notwendig sind. Dieser Gedanke trägt dem asymmetrischen Vertragsverhältnis zwischen Autohersteller und Benutzer*in Rechnung[17] und bannt die Gefahr, dass durch Generaleinwilligungen der Schutz des BDSG umgangen wird. Offen bliebe indes die Möglichkeit der Nutzer*innen, Einzeleinwilligungen zu bestimmten Datennutzungen für bestimmte Zeiträume zu erteilen (privacy by default). Um solche informierten Einzeleinwilligungen erteilen zu können, sind zwei Voraussetzungen zu erfüllen: Zum einen muss vor dem Autokauf eine umfassende Informationspflicht der Verkäufer*innen darüber bestehen, wie, wann und unter welchen Voraussetzungen das Auto Daten aus der Bordelektronik weiterverarbeitet. Zum anderen muss sichergestellt werden, dass durch verbraucherfreundliche Displayanzeigen der/ die Nutzer*in stets zur Kenntnis nehmen kann, für was nun eine Einzeleinwilligung erteilt werden soll.[18] Nur auf Grundlage solcher Informationen wäre es den Nutzer*innen möglich, von ihrem grundrechtlich verbürgten Recht auf informationelle Selbstbestimmung Gebrauch zu machen.

Weiterführende Literatur:

Volker Lüdemann, Connected Cars – Das vernetzte Auto nimmt Fahrt auf – der Datenschutz bleibt zurück, Zeitschrift für Datenschutz 2015, 247 ff.

Christoph Stürmer/Britta Schinzel, Connected Cars, FifF-Kommunikation 3/2017, 26 ff.

Thilo Weichert, Datenschutz im Auto – Teil 1 und 2, Straßenverkehrsrecht – Zeitschrift für die Praxis des Verkehrsjuristen 2014, 201 ff. und 241 ff.

Benjamin Gremmelspacher studiert Jura in Freiburg und engagiert sich bei der Humanistischen Union für bürgerrechtliche Themen, insbesondere für Datenschutz und Informationsfreiheit.

16 Weichert, SVR 2014, 201 (205 f.).

17 Dix, ZEuP 2017, 1 (4).

18 Weichert, SVR 2014, 241 (242 f.); Lüdemann, ZD 2015, 247 (254).

Anzeige