Editorial - Grußwort des Forschungsprojektleiters »BayWiDI« Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur nun schon neunten Ausgabe des BayWiDI-Newsletters.

Am 11. und 12. April 2018 fand das 13. For..Net Symposium in Passau statt. Unter dem Motto »Wertschöpfung durch Digitalisierung – Innovation. Ethik. Sicherheit.« wurde vor den Augen zahlreicher Zuhörer ein ertragreicher Diskurs über Fragen, Probleme, Lösungen und Chancen der Digitalisierung geführt. In diesem Rahmen wurde der 5. For..Net-Award, ein Preis für Innovationen zu Datenschutz und IT-Sicherheit, an Christian Bennefeld verliehen, der mit seinem Unternehmen den eBlocker vertreibt, eine Hardwarelösung, die einmal an das Heimnetzwerk angeschlossen das Online-Verhalten anonymisiert und dem Nutzer die Kontrolle über seine Daten ermöglicht. Weitere Informationen zum Ablauf, dem Inhalt und den Highlights der Veranstaltung können Sie dem folgenden Tagungsbericht entnehmen, der Ihnen einen prägnanten Überblick hierüber liefert.

Die Digitalisierung erfasst mittlerweile alle Lebensbereiche und führt zu teils drastischen Veränderungen. Themen, die hierbei regelmäßig für umfangreiche und kontroverse Diskussionen sorgen, sind das automatisierte und das autonome Fahren. Die mediale Aufmerksamkeit war immens, als am 18. März 2018 ein selbstfahrendes Fahrzeug der Firma Uber einen Fahrradfahrer tödlich erfasste. Der Technologie-Website »The Information« zufolge handelte es sich um einen Softwarefehler; der Computer habe Daten des Sensors, der Hindernisse auf den Straßen erfassen sollte, als fehlerhaft beurteilt und darum ignoriert. Doch wer soll im Falle von automatisierten Fahrzeugen für derartige Unfälle haften? Wie wird die Haftung bei autonom fahrenden Fahrzeugen, also solchen bei denen kein Fahrer mehr beteiligt ist, geregelt werden? Die Auseinandersetzung mit dem Rechtsrahmen für solche Innovationen stellt einen essentiellen Teil des Fortschritts dar. Deshalb finden Sie in diesem Newsletter einen Beitrag, der sich mit Haftungsfragen nach straßenverkehrsrechtlichen Normen befasst.

Nach Informationen von Süddeutscher Zeitung, WDR und NDR ist der „Staatstrojaner“ nun aktuell im Einsatz. Die Kritik daran ist groß, es wird von ungerechtfertigten Grundrechtseingriffen gesprochen. Eine Auskunft darüber, in welchen und wie vielen Fällen der Einsatz bereits erfolgte, wurde unter Berufung auf ermittlungstaktische Gründe vom BKA bislang nicht erteilt. Ermöglicht wird der Einsatz dieser Software neben der Änderung der StPO auch durch das neue Polizeiaufgabengesetz (PAG) des Freistaates Bayern. Ein folgender Beitrag wird das Dilemma zwischen „Sicherheit durch Verschlüsselung“ und „Sicherheit trotz Verschlüsselung“ beleuchten und einen Überblick über die damit verbundenen Risiken, sei es durch Missbrauch des Trojaners selbst oder durch das Ausnutzen von Sicherheitslücken durch Dritte, liefern.

Nach diesem kurzen Überblick wünsche ich Ihnen nun viel Spaß bei der Lektüre des Newsletters!

Ihr Prof. Dr. Dirk Heckmann,
Leiter des Forschungsprojekts »BayWiDI«

Inhalt

Tagungsbericht zum 13. Internationalen For..Net Symposium »Wertschöpfung durch Digitalisierung - Innovation. Ethik. Sicherheit.« am 11. und 12. April 2018

Das zum 13. Mal in Passau ausgerichtete For..Net Symposium stand unter dem Leitthema „Wertschöpfung durch Digitalisierung – Innovation. Ethik. Sicherheit." und verzeichnete über 140 Anmeldungen. Umfassend beleuchtet wurden dabei die durch die Digitalisierung hervorgebrachten Innovationen unter Heranziehung aktueller Anwendungsbeispiele, etwa aus den Bereichen Open Data, Industrie 4.0 sowie Social Media.

Unter der wissenschaftlichen Leitung von Prof. Dr. Dirk Heckmann, Leiter der Forschungsstelle For..Net, sowie der Schirmherrschaft der Staatsministerin für Digitalisierung Dorothee Bär fanden sich am 11. und 12. April 2018 zahlreiche Vertreter aus Wissenschaft, Praxis und Politik in der Redoute in Passau ein, um sich mit den vorgenannten Themen zu beschäftigen und den geschaffenen Raum für angeregte Diskussionen zu nutzen.

Den Auftakt des diesjährigen Symposiums bildeten die Grußworte von Prof. Dr. Carola Jungwirth, Präsidentin der Universität Passau, von Dorothee Bär, die per Videobotschaft zugeschaltet wurde, sowie von Prof. Dr. Dirk Heckmann. Anschließend sprach Prof. Dr. Wilfried Bernhardt die Keynote „Wertschöpfung durch Open Data in Verwaltung, Justiz und Gesetzgebung", wobei er insbesondere unter dem Aspekt des Open by Default and Design-Prinzips einen Informationsanspruch der Bürger auf ein Maximum an Datenveröffentlichung skizzierte. Prof. Dr. Wilfried Bernhardt übte eingehend Kritik an der gegenwärtigen Gesetzeslage, welche Bürgern keinen einklagbaren Anspruch auf Datenveröffentlichung gewähre. Ebenso bewertete der Referent das Open-Data-Gesetz der Bundesregierung. Zwar sei diese Initiative an sich begrüßenswert, jedoch fehle es bislang insgesamt an einer konkreten Umstellung der Datenpolitik hin zu einem proaktiv datenöffnenden Staat.

Prof. Dr. Dirk Heckmann befasste sich mit der Rolle des Rechts im Kontext digitaler Vernetzung. Unter der These „Keine Wertschöpfung ohne Wertschätzung" ging er auf die Wichtigkeit des Erhalts errungener Verfassungswerte ein. Hierbei beleuchtete der Leiter der Forschungsstelle ausgewählte juristische Probleme anhand zweier konkreter Anwendungsbeispiele digitalisierter Lebensbereiche: einerseits das autonome Fahren, andererseits die sozialen Medien. Im Ergebnis könne – so der Referent – effektiver Rechtsschutz nur durch die Kombination aus Technikgestaltung und Technikwissen erzielt werden.

Es folgte der Vortrag von Prof. Dr. Christoph Lütge von der TUM mit dem Titel „Ethik und Innovation in Industrie 4.0". Dieser widmete sich primär cyberphysischen Systemen, wie etwa 3D-Druckern, durch welche moderne Produktionsprozesse signifikant verändert würden. Hierbei verdeutlichte der Referent, dass zugleich mit positiven Entscheidungen für die Industrie 4.0 spezifische, auf einer breiten gesellschaftlichen Diskussion fußende, ethische Regeln geschaffen werden müssten. Ohnehin dürfe technologischer Fortschritt nicht nur rechtlich gesteuert werden, sondern müsse gleichermaßen durch die Bevölkerung aktiv gestaltet werden.

Die Gründerin und Geschäftsführerin der newsgreen GmbH, Diana Kinnert, referierte zu „Fortschritt und Bewahrung: Plädoyer für eine Kultur des Digitalen". Sie porträtierte die durch die Digitalisierung hervorgebrachten, neuartigen Erscheinungsformen von Machtstrukturen, Abhängigkeiten und Grundprinzipien. Diese führten zur Notwendigkeit eines neuen Gesellschaftsvertrags, wodurch die „neue Kultur des Digitalen" als Chance für die Demokratie zu begreifen sei. Geschaffen werden müsse vor allem eine breite Diskussionsplattform, worüber zentrale Themen der Digitalisierung debattierbar wären.

Den Abschluss des ersten Veranstaltungstages bildete eine Podiumsdiskussion zum Thema „Wertschöpfung und Werteerhaltung: Wo endet die Innovationsspirale?". Im Zentrum standen dabei die Auswirkungen technischer

Seitlicher Blick auf die Bühne und ins Plenum (© Robert Geisler)

Entwicklungen auf das derzeitige Meinungsbild. Konkret gefragt wurde danach, ob es innerhalb der Gesellschaft eine tatsächliche Haltung zu diesen Themen gibt oder ob die Adressaten vielmehr nur noch Getriebene dieser Entwicklung sind. Die Teilnehmenden kamen überein, dass zumindest eine Tendenz zu letztgenannter Gefahr bestünde, nachdem die Digitalkultur national häufig nur als Expertenthema deklariert werde. Einigkeit herrschte zudem dahingehend, dass es hierzulande an einer Kultur des Scheiterns fehle, was insbesondere mögliche Innovationen enorm behindere.

for..net
Forschungsstelle für IT-Recht und Netzpolitik

Bestens geeignet zur Vernetzung unter den Teilnehmenden war wieder der traditionelle Galaabend auf der Veste Oberhaus, in dessen Rahmen der For..Net Award 2018 für datenschutzkonforme IT-Innovationen an die eBlocker GmbH verliehen wurde. Deren Gründer und geschäftsführender Gesellschafter, Christian Bennefeld, eröffnete den zweiten Tag des Symposiums mit seinem Vortrag „To track or not to track – rechtskonformer Einsatz von Website-Tracking“. Er beschrieb anschaulich, wie interessenbasierte Online-Werbung mittels intimer Persönlichkeitsprofile realisiert wird, die ihrerseits mithilfe verschiedenster Tracking-Methoden erstellt werden. Dabei stellte der Referent eine Auswahl solcher Methoden vor, etwa sichtbare und versteckte Tracking-Pixels, Cookies, Tags und Fingerprinting. Insgesamt seien nach Christian Bennefeld das Tracking sowie das Sammeln und Auswerten von Daten bislang (noch) lukrativer als das „Geschäftsmodell Datenschutz“.

Im Anschluss sprach Prof. Dr. Dirk Heckmann über das BSI Forschungsprojekt 356 zur IT-Sicherheitsregulierung. Ohne IT-Sicherheit sei die Digitalisierung im Gesamten nichts wert, denn Digitalunsicherheit drohe gravierende Folgen nach sich zu ziehen. Nach Prof. Dr. Dirk Heckmann sei eine große Schwachstelle der IT-Sicherheit auch insbesondere der Nutzer. Besprochen wurden ferner die Hauptziele und zentralen Fragestellungen des aktuellen Forschungsprojekts an der Universität Passau.

Im Rahmen des Vortrags „Datenschutzrechtliche Verantwortung in komplexen IT-Systemen“, setzte sich Dr. Paulina Jo Pesch (KIT) vertieft mit Blockchain-Systemen auseinander. Nachdem diese keinen zentralen Anbieter haben, die Nutzer mithin alles selbst verwalten, liege nach Ansicht der Referentin die eigentliche Innovation darin, dass Teilnehmer, die sich mitunter nicht einmal gegenseitig vertrauen, eine gemeinsame Blockchain ohne zentrale Stelle einrichten können. Allerdings wies Dr. Paulina Jo Pesch ebenso auf die hohe Gefahr von Datengefährdungen im Zusammenhang mit der Blockchain hin, aufgrund derer sie sich für die Vermeidung derartiger Systeme aussprach, sofern datenschutzfreundlichere Alternativen verfügbar sind.

Unter dem Titel „Datenschutz durch Technikgestaltung: Das Zusammenspiel technischer und rechtlicher Innovation am Beispiel von Gesundheitsdaten“ zeigte Ninja Marnau, Senior Researcher am CISPA – Helmholtz-Zentrum i. G., zunächst auf, dass und inwieweit Art. 25 Abs. 1 DS-GVO IT-Innovationen vorantreibe. Diesbezüglich präsentierte die Referentin eine neue Methode der Datenanonymisierung mittels „Verrauschung“ namens Differential Privacy, die vor allem verbesserte Schutzgarantien für den Einzelnen mit sich bringe. Zwar sei die Blockchain-Technologie grundsätzlich für den Einsatz im Zusammenhang mit Gesundheitsdaten prädestiniert, allerdings stünde deren Ewigkeitsgarantie im Widerspruch zum Datenschutzrecht, etwa mit Blick auf das Recht auf Löschung bzw. Berichtigung. Eine denkbare Lösung bestünde jedoch beispielsweise im Konzept veränderbarer Blöcke.

Im Anschluss folgte eine Podiumsdiskussion mit den Referentinnen und Referenten unter der Moderation von Prof. Dr. Dirk Heckmann. Dabei wurde übereinstimmend betont, dass es grundsätzlich wichtig sei, neuartige Entwicklungen anzunehmen, um die Weiterentwicklung nicht zu blockieren. Insgesamt müsse Deutschland weiter zukunftsfähig gemacht werden – ein Ziel, dass durch „neues Denken“ zu erreichen sei, mithin vor allem durch Abkehr von tradierter Bürokratie.

Die Aufzeichnungen der Vorträge des Symposiums können über die Webseite von For..Net

https://www.for-net.info/symposien/symposium-2018/programm-videos/

abgerufen werden. Das 14. Internationale For..Net Symposium wird unter dem Thema „Digitale Bildung, digitale Haltung“ am 25. und 26. April 2019 in Passau stattfinden.

Kitur/Leeb/Lorenz

Haftung nach dem Straßenverkehrsrecht im Rahmen von automatisiertem Fahren

Roboterstaubsauger, smarte Rasenmäher und andere selbstständige informationstechnische Systeme haben längst Eingang in die Gesellschaft gefunden. Diese „Automatisierung“ macht auch vor dem Straßenverkehr nicht Halt und zeigt sich bereits an bereichsspezifischen Assistenzsystemen wie dem Anti-Blockier-System (ABS), dem Tempomat oder automatischen Einparkhilfen.[1] Das Phänomen „automatisiertes Fahren“ hatte vor dem 8. StVG-ÄndG vom 16.06.2017[2] noch keinen Niederschlag in den straßenverkehrsrechtlichen Haftungsvorschriften gefunden. Fragen ergeben sich im Haftungsbereich insbesondere im Zusammenhang mit der Eigenschaft als Fahrzeugführer und Fahrzeughalter. Dieser Beitrag soll sich der Einordnung von Fahrassistenzsystemen und autonomen Fahrzeugen in das straßenverkehrsrechtliche Haftungsregime widmen.

Entwicklung der Rechtslage

Die grundlegenden Haftungstatbestände finden sich in § 7 StVG (Halterhaftung) und in § 18 StVG (Fahrzeugführerhaftung). Damit knüpfen die Normen maßgeblich daran an, ob der Anspruchsgegner diese bezeichneten Eigenschaften aufweist.

Fahrzeughalter ist die Person, die das Fahrzeug für eigene Rechnung in Gebrauch hat und die Verfügungsgewalt über das Fahrzeug ausübt.[3] Verfügungsgewalt meint dabei die Befugnis, über den Einsatz und die Ziele des Fahrzeuges zu entscheiden.[4] Fahrzeugführer ist demgegenüber, wer zum Zeitpunkt eines verkehrsrelevanten Ereignisses die tatsächliche Gewalt über das Fahrzeug ausübt, es lenkt.[5] Da es bei der Haltereigenschaft vordergründig weder auf die Eigentumslage noch darauf ankommt, auf wen das Fahrzeug zugelassen ist,[6] lässt sich bei der Bestimmung von Fahrzeughalter und Fahrzeugführer feststellen, dass diese sich jedenfalls den gemeinsamen Nenner der Verfügungsgewalt teilen, wenngleich in verschiedenen Ausprägungen.

Den völkerrechtlichen Rahmen des Straßenverkehrsrechts setzt das Wiener Übereinkommen über den Straßenverkehr vom 8. November 1968 (Wiener Übereinkommen), dessen Einhaltung gem. Art. 3 Abs. 3 Wiener Übereinkommen Voraussetzung für die Zulassung zum internationalen Verkehr ist.[7] Art. 8 Abs. 1 Wiener Übereinkommen schreibt vor, dass jedes Fahrzeug einen Führer haben muss; auch Art. 13 Abs. 1 Wiener Übereinkommen bestimmt die Notwendigkeit der tatsächlichen Herrschaftsgewalt des Fahrzeugführers über das Fahrzeug. Um der technologischen Entwicklung gerecht zu werden, sieht nunmehr seit dem 23.03.2016 Art. 8 Abs. 5bis Wiener Übereinkommen vor, dass Fahrzeuge mit selbigem vereinbar sind, soweit sie in ihrer Bauweise und technischen Ausrüstung den internationalen Zulassungsvorgaben entsprechen und außerdem die automatisierte Führung jederzeit vom Fahrer wieder unterbrochen bzw. deaktiviert werden kann. Damit sind automatisierte Fahrzeuge nicht mehr als grundsätzlich völkerrechtswidrig einzustufen.

Diese Wertung hat sich auch in dem 8. StVG-ÄndG niedergeschlagen. So sieht der neue § 1a Abs. 1 StVG die Zulässigkeit eines Kfz mit hoch- oder vollautomatisiertem Fahrsystem vor, sofern ein bestimmungsgemäßer Gebrauch vorliegt. Die technischen Anforderungen finden sich in § 1a Abs. 2 und Abs. 3 StVG. Hoch- und vollautomatisiertes Fahren meint dabei Konstellationen, in denen das Fahrzeug die wesentlichen Quer- und Längssteuerungen und damit die Gesamtleitung der Fahrt nahezu

1 *Lutz*, NZV 2014, 67.

2 S. BGBl. 2017, 1648.

3 *Jänich/Schrader/Reck*, NVZ 2015, 313, 315 m.w.N.

4 *König*, in: Hentschel/König/Dauer Straßenverkehrsrecht Kommentar, 44. Aufl. 2017, § 7 StVG Rn. 14.

5 *Heß*, in: Burmann/Heß/u.a. Straßenverkehrsrecht Kommentar, 25. Aufl. 2018, § 18 StVG Rn. 3.

6 *Burmann*, in: Burmann/Heß/u.a. Straßenverkehrsrecht Kommentar, 25. Aufl. 2018, § 7 StVG Rn. 5.

7 Das Wiener Übereinkommen mit Stand 19.09.2016 ist abrufbar unter https://www.admin.ch/opc/de/classified-compilation/19680244/201609190000/0.741.10.pdf, abgerufen am 06.06.2018.

selbstständig übernimmt.[8] Demgegenüber sind teilautomatisierte Fahrzeuge lediglich mit einzelnen, bereichsspezifischen intelligenten Assistenzsystemen ausgestattet.[9]

Vom automatisierten Fahren zu unterscheiden ist jedoch das autonome Fahren, bei dem das Fahrzeug völlig selbstständig fährt und die Insassen somit nur noch als Passagiere zu qualifizieren sind.[10] Dieser Anwendungsfall ist derzeit weder von nationalem noch von internationalem Recht vorgesehen.

Insbesondere: Fahrzeughalter- und Fahrzeugführerhaftung

1. Fahrzeugführerhaftung gem. § 18 StVG

§ 1a Abs. 4 StVG legt ausdrücklich fest, dass auch diejenigen Personen Fahrzeugführer sind, die einen hoch- oder vollautomatisierten Fahrmechanismus in Gang gesetzt haben und sich in dem betreffenden Fahrzeug befinden; und zwar auch dann, wenn eine eigenhändige Lenkung des Fahrzeugs zum relevanten Zeitpunkt nicht stattfindet. Damit ist der Anwendungsbereich des § 18 StVG auch für den Fall des hoch- oder vollautomatisierten Fahrens eröffnet. Bei diesem Tatbestand handelt es sich um eine verschuldensabhängige Haftung, vgl. § 18 Abs. 1 S. 2 StVG, bei der das Verschulden des Fahrzeugführers vermutet wird.[11] Der Kern einer jeden verschuldensabhängigen Haftung liegt in der Verletzung einer Pflicht bzw. eines Rechtsguts.[12] Als solche Pflichten kommen neben den fortbestehenden Pflichten, die sich für den Führer eines Fahrzeugs im Straßenverkehr ergeben, nunmehr die besonderen Pflichten gem. § 1b StVG für diejenigen Fahrzeugführer, die sich eines hoch- oder vollautomatisierten Fahrzeugs bedienen. Dazu gehört insbesondere die Pflicht des Fahrzeugführers zum Wiederaufgreifen der Steuerung in den Fällen des § 1b Abs. 2 StVG, sowie seine „Wahrnehmungsbereitschaft" gem. § 1b Abs. 1 StVG. Mit § 1a Abs. 4 StVG wurde nun Rechtssicherheit hinsichtlich der Frage geschaffen, inwieweit „Führer" eines hoch- oder vollautomatisierten Fahrzeugs dem ursprünglich in der StVG vorgesehenen Fahrzeugführer entsprechen. Der Gesetzgeber hat sich in der Hinsicht für eine umfängliche Gleichstellung mit dem herkömmlichen Fahrzeugführer entschieden. Der Gesetzesbegründung ist diesbezüglich vor allem das Streben nach Rechtssicherheit und Verkehrsunfallopferschutz zu entnehmen.[13] Konkret bedeutet dies, dass auch im Falle des aktivierten Fahrsystems derjenige Insasse gem. § 18 StVG haftet, der auf dieser Fahrt für das In-Gang-Setzen des Systems verantwortlich ist. Gleichzeitig wird im Falle von derart selbstständigen informationstechnischen Systemen oftmals von Robotern oder „intelligenten" Assistenzsystemen gesprochen, wodurch eine Verbindung zu grundlegend menschlichen Eigenschaften geschaffen wird.[14] Die Position, die sich für die Schaffung einer eigenen Rechtspersönlichkeit von Robotern ausspricht,[15] hat sich diesbezüglich zwar noch nicht in der Gesetzgebung durchsetzen können. Allerdings ist die der Begrifflichkeit zugrunde liegende Wertung zu beachten: „intelligenten" Assistenzsystemen wird bereits durch diese Wortwahl eine nicht unbeachtliche Selbstständigkeit zugesprochen. Zum Vergleich sei auf den Fall hingewiesen, in dem ein Unfall sich während einer Fahrstunde ereignet: hier wurde der Fahrlehrer, nicht hingegen der Fahrschüler als Fahrzeugführer i.S.d. § 18 StVG qualifiziert, weil diesem ein hoher Anteil an Verantwortung zukam.[16] Daraus kann jedenfalls geschlossen werden, dass die Verantwortlichkeit während der konkret in Frage stehenden Fahrt für die Bestimmung der Führereigenschaft eine wesentliche Rolle spielt. Diese Selbstständigkeit führt dazu, dass bei der Gleichstellung von herkömmlichen Fahrzeugführern mit solchen, die ein hoch- oder vollautomatisiertes Fahrzeug in Betrieb nehmen, in der Praxis viele Zweifelsfälle zu erwarten sind. Daher bleibt bislang offen, ob die anvisierte Rechtssicherheit durch die Schaffung des § 1a Abs. 4 StVG erreicht werden kann. Auch ist zu bedenken, dass die Beweislast der Exkulpation bei dem Fahrzeugführer liegt.[17] Dies dürfte in einigen Konstellationen, in denen der Unfall

8 *Jahnke*, in: Burmann/Heß/u.a. Straßenverkehrsrecht Kommentar, 25. Aufl. 2018, § 1a StVG Rn. 4.

9 Vgl. zur Übersicht der Automatisierungsstufen: Redaktion der Wirtschaftswoche (WiWo) vom 24.01.2018, abrufbar unter https://www.wiwo.de/technologie/mobilitaet/teilautomatisiertes-fahren-die-technik-muss-besser-werden/20880248.html, abgerufen am: 06.06.2018.

10 *Jahnke*, in: Burmann/Heß/u.a. Straßenverkehrsrecht Kommentar, 25. Aufl. 2018, § 1a StVG Rn. 5.

11 *Engel*, in: MüKo Straßenverkehrsrecht Band 2, 1. Aufl. 2017, § 18 StVG Rn. 2.

12 *Grundmann*, in: MüKo BGB, 7. Aufl. 2016, § 276 Rn. 6 m. w. Nw., Rn. 52.

13 BT-Drs. 69/17, S. 7 f.

14 *Keßler*, MMR 2017, 589.

15 Aufgeworfen in der Entschließung des EU-Parlaments vom 16.02.2017 P8_TA-PROV(2017)0051, Zivilrechtliche Regelungen im Bereich Robotik, Entschließung des Europäischen Parlaments v. 16.2.2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik, abrufbar unter http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//DE, abgerufen am 28.05.2018.

16 OLG Koblenz, Urt. v. 01.12.2003 – 12 U 772/02 – NZV 2004, 401; zustimmend *Engel*, in: MüKo Straßenverkehrsrecht Band 2, 1. Aufl. 2017, § 18 StVG Rn. 3.

17 *Engel*, in: MüKo Straßenverkehrsrecht Band 2, 1. Aufl. 2017, § 18 StVG Rn. 4.

während einer automatisierten Fahrtzeit geschieht, schwer fallen, weswegen ein differenzierender Haftungsmechanismus bei aktivierten Assistenzsystemen sachgerechter erscheint.[18]

2. Fahrzeughalterhaftung gem. § 7 Abs. 1 StVG

Bei dem Haftungstatbestand gem. § 7 Abs. 1 StVG handelt es sich demgegenüber um einen verschuldensunabhängigen Tatbestand. Bei solchen verschuldensunabhängigen Haftungsmechanismen liegt der Geltungsgrund maßgeblich in der Schaffung einer Gefahrenquelle durch sozialadäquates Verhalten.[19] Der Norm kommt somit kein Strafcharakter, sondern vielmehr eine Zuweisung der Verantwortlichkeiten in Konstellationen von gesellschaftlich anerkannten Tätigkeiten zu.[20] Auch hier knüpft die Haftung an einer Eigenschaft an, nämlich die des Fahrzeughalters. Dabei kommt es, wie eingangs bereits erwähnt, jedoch nicht auf Eigentumsverhältnisse, sondern maßgeblich auf die Verfügungsgewalt an. Vor diesem Hintergrund könnte – ebenso wie im Rahmen der Fahrzeugführerhaftung – der fehlende Einfluss des Verantwortlichen im Falle von automatisierten Fahrsystemen problematisiert werden.[21] Diese kritische Betrachtung findet ihren Ursprung in der dem Straßenverkehrsrecht zugrunde liegenden Prämisse, dass für die Gefahrenquelle „Kfz" derjenige heranzuziehen ist, der aufgrund seiner tatsächlichen Position in der Lage ist, etwaige Schäden zu vermeiden.[22] Bei genauer Betrachtung liegt allerdings die Eröffnung der Gefahrenquelle in der Entscheidung, ein Fahrzeug überhaupt im öffentlichen Straßenverkehr zu nutzen, also anknüpfend an die Entscheidung des „ob".[23] Demgegenüber normiert § 18 StVG einen verschuldensabhängigen Tatbestand, der daran anknüpft, wie das Fahrzeug geführt wurde. Die Entscheidung, ein Kfz in Betrieb zu nehmen, ist hingegen unabhängig von der Fahrweise, sodass die Halterhaftung nicht im elementaren Widerspruch zu automatisierten Fahrten steht. Abgrenzungsprobleme sind hingegen denkbar, wenn ein Fahrzeug sich mittels Assistenzsystem selbst in Betrieb setzt und sodann einen Unfall verursacht.

Ausblick

Mit dem 8. StVG ÄndG sowie der zuvor in Kraft getretenen Reform des Wiener Übereinkommens haben automatisierte Fahrzeuge endgültig Eingang in das Rechtssystem gefunden. Damit wird der grundsätzlichen Aufgeschlossenheit der Gesellschaft gegenüber automatisiertem Fahren Rechnung getragen. Die Mobilität jüngerer und älterer Bevölkerungsgruppen ist dabei nur ein Teil der positiv zu wertenden Aspekte, auch hinsichtlich der Effektivität und der Nachhaltigkeit des Nutzungsverhaltens bestehen neue Chancen.[24]

In der Praxis können dennoch viele Fragen im Bereich der Haftung auftreten. Hinsichtlich des neuen § 1b StVG bleibt abzuwarten, wie sich insbesondere das Merkmal „wahrnehmungsbereit" aus § 1b Abs. 1 StVG sowie die Voraussetzungen des § 1b Abs. 2 Nr. 2 StVG in der Praxis konkretisieren werden. Im Rahmen der völkerrechtlichen Zulassungsvorschriften setzen jedoch die Regelungen der Wirtschaftskommission der Vereinten Nationen über die Annahme harmonisierter technischer Regelungen für Radfahrzeuge, […] und die gegenseitige Anerkennung von Genehmigungen, die nach diesen Regelungen erteilt wurden (UNECE-Regelungen) der Praktikabilität automatisierter Fahrzeuge noch Grenzen. Nach Regelung Nr. 79[25] ist nämlich derzeit eine automatisierte Lenkung nur bis zu einer Geschwindigkeit von 10 km/h zulässig. Eine Anpassung auf hoch- und vollautomatisierte Fahrzeuge ist jedoch in Bearbeitung.[26]

Vom nationalen, europäischen und völkerrechtlichem Rechtsrahmen ausgenommen ist bisher allerdings noch das autonome Fahren, bei dem vollständig auf einen Fahrzeugführer verzichtet wird (s. oben zur Abgrenzung zum automatisierten Fahren). In dieser Konstellation scheint ein unveränderter Rückgriff auf die Dogmatik der Gefährderhaftung im Straßenverkehr ausgenommen. Im Zusammenhang mit autonomen und automatisiertem Fahren wird jedoch immer mehr der Haftung von anderen Beteiligten, wie etwa den Softwarelieferanten, Relevanz zugemessen.[27]

Auch andere Rechtsgebiete werden von der Automatisierung von Fahrzeugen betroffen sein. Zu nennen seien etwa die – ebenfalls als Gefährderhaftung konzipierte – Produkthaftung gem. § 1 Abs. 1 S. 1 ProdHaftG oder die strafrechtlichen Normen wie § 142 StGB oder §§ 315b f. StGB, denen bislang ebenso die Prämisse menschlichen Verhaltens zugrunde liegt.

Der gesellschaftliche Wandel zeigt eine grundlegende Akzeptanz des automatisierten Fahrens, welche sich unter anderem in der konstanten Konzeptentwicklung niederschlägt. Wie in jedem anderen Bereich der Digitalisierung sollte die Rechtsentwicklung auch hier möglichst parallel zur technischen Dynamik laufen. Die Novelle des StVG stellt dabei lediglich den Anfang einer notwendigen rechtlichen Entwicklung dar.

Nawrocki

18 In diese Richtung auch die Empfehlung des 53. Deutschen Verkehrsgerichtstag Goslar, S. 2, https://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/empfehlungen_53_vgt.pdf, abgerufen am 06.06.2018.

19 *Engel*, in: MüKo Straßenverkehrsrecht Band 2, 1. Aufl. 2017, § 7 StVG Rn. 5 ff.

20 *Engel*, in: MüKo Straßenverkehrsrecht Band 2, 1. Aufl. 2017, § 7 StVG Rn. 5 f.

21 In diese Richtung *Albrecht*, SVR 2005 Heft 10, 373, 375.

22 *Albrecht*, SVR 2005 Heft 10, 373, 374.

23 *Burmann*, in: Burmann/Heß/u.a. Straßenverkehrsrecht Kommentar, 25. Aufl. 2018, § 7 StVG Rn. 5.

24 Einen Überblick über die Vorteile liefert Lange, NZV 2017, 345, 346 f.

25 Regelung Nr. 79 der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE) – Einheitliche Bedingungen für die Genehmigung der Fahrzeuge hinsichtlich der Lenkanlage, Revision 2, Abl. L 137 vom 27.5.2008, S. 25; BMVI, UNECE-Regelungen, abrufbar unter https://www.bmvi.de/SharedDocs/DE/Artikel/LA/un-ece-regelungen.html, abgerufen am 28.05.2018 (nichtamtliche deutsche Fassung).

26 *Lange*, NZV 2017, 345, 348.

27 S. dazu Beitrag auf https://www.haufe.de/recht/weitere-rechtsgebiete/verkehrsrecht/stvg-reform-als-vorbereitung-auf-selbstfahrende-autos_212_401418.html, abgerufen am 06.06.2018.

Staatstrojaner im Einsatz

Die Industrie 4.0 schlägt sich nicht nur in der rasanten Entwicklung technischer Innovationen nieder, sondern auch in der Tatsache, dass digitale Instrumente nahezu für jedes alltägliche Ereignis verwendet werden. Auch die Ausübung einer beruflichen Tätigkeit geht meist mit der Verwendung elektronischer Geräte einher. So verwundert es nicht, dass auch im Rahmen der Staatstätigkeit eine erhöhte Verwendung informationstechnischer Systeme (IT-Systeme) und digitalisierter Vorgehensweisen aufkommen. Letztere sollen insbesondere im Gefahrenabwehr- und im Strafverfolgungsrecht zu einer Effektivitätssteigerung führen. Auf diesen Gedanken beruhen auch diejenigen Befugnisse der Strafverfolgungs- und Gefahrenabwehrbehörden, die sich nunmehr elektronisch gestalten und in dieser Form eine steigende Relevanz in der Rechtsordnung und -anwendung erfahren haben. Zu nennen sind etwa die Möglichkeit der Durchsuchung verdächtiger IT-Systeme (Online-Durchsuchung) und die Erhebung noch unverschlüsselter Daten (Quellentelekommunikationsüberwachung). Der Zugriff auf IT-Systeme kann weitreichende Sicherheitsrisiken mit sich bringen, insbesondere, wenn dadurch Zugriffe von unbefugten Dritten ermöglicht werden. Dieser Beitrag zeichnet schematisch die staatlichen Eingriffsmöglichkeiten nach dem derzeitigen Stand von Recht und Technik sowie die daraus entstehenden Risiken ab.

Rechtlicher Rahmen

Bei der Online-Durchsuchung wird auf dem zu überprüfenden IT-System eine Software installiert. Diese Infiltration ermöglicht den Zugriff auf sämtliche auf dem Zielrechner befindlichen Daten. In jüngerer Zeit hat sich daneben die Maßnahme der sog. Quellentelekommunikationsüberwachung (Quellen-TKÜ)

etabliert.[1] Dabei handelt es sich gewissermaßen um einen Sonderfall der Online-Durchsuchung, denn auch hier wird mit Hilfe einer Software der Zugang zu einem zu überprüfenden IT-System geschaffen.[2] Im Rahmen der Quellen-TKÜ werden Kommunikationsdaten vor der Verschlüsselung erhoben, um deren Überprüfung zu ermöglichen.[3] Sie ist im Gegensatz zur Online-Durchsuchung als heimliche Maßnahme konzipiert, wenngleich letztere in der Praxis auch meist heimlich erfolgen wird.[4]

In den vergangenen Jahren haben sich beide Maßnahmen sowohl im Gefahrenabwehrrecht als auch im Strafverfolgungsrecht etabliert. So finden sich in den Polizeigesetzen der Länder Ermächtigungsgrundlagen für die Online-Durchsuchung und für die Quellen-TKÜ. Für die Strafverfolgungsbehörden ermöglichen dies bundesweit §§ 100a, 100b StPO. Nach dem neuen bayerischen Polizeigesetz (PAG) ist die Online-Durchsuchung sogar bereits bei „drohender Gefahr für ein bedeutendes Rechtsgut“ möglich, vgl. Art 45 Abs. 1 S. 1 Nr. 1 PAG. An dieser Entwicklung ist zu erkennen, dass Ermittlungsmaßnahmen und Gefahrenabwehrmaßnahmen fortlaufend dem technischen Fortschritt angepasst werden. Obwohl das Bundesverfassungsgericht dafür zum Teil strenge Anforderungen festlegt,[5] liegt die Tendenz in der wachsenden Bedeutung „digitaler stattlichen Befugnisse“.

Technische Grundlage

Die für die Online-Durchsuchung und Quellen-TKÜ erforderliche Infiltration wird mit Hilfe des sog. Staatstrojaners durchgeführt, der als fremde Software

1 Z. Bsp. mit der Normierung in § 100a Abs. 1 S. 2 StPO durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.08.2017, BGBl. I 2017, 3202.

2 *Mansdörfer*, GSZ 2/2018, 445, 47.

3 *Beuckelmann*, NJW-Spezial 2017, 440.

4 *Freiling/Safferling/Rückert*, JR 2018, 9, 16; *Mansdörfer*, GSZ 2/2018, 45, 47.

5 BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 – NJW 2008, 822 (Online-Durchsuchung); BverfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 – BeckRS 2016, 44821 (BKAG).

auf dem Zielrechner installiert wird; notwendige Bedingung dafür ist das Bestehen einer Sicherheitslücke.[6] Sodann ist der Zugriff auf die Daten möglich.[7] Mit Hilfe der installierten Software können nun zahlreiche Überwachungsmaßnahmen vorgenommen werden. So können nicht nur Bildschirmfotos zum Zwecke des Mitlesens von Nachrichten versendet werden, sondern auch mit Hilfe von Keyloggern Tastatureingaben nachvollzogen oder durch Zugriff auf GPS-Daten ein Bewegungsprofil erstellt werden.[8] Nicht zu verkennen ist zudem, dass neben „klassischen" Kommunikationsgeräten wie Smartphones oder Laptops, auch sämtliche „smarte" Geräte wie Sprachassistenten, intelligente Kaffeemaschinen oder vernetzte Autos als Zielrechner in Betracht kommen. Bei der Quellen-TKÜ kann ein Kommunikationsereignis – zum Beispiel ein Skype-Gespräch oder eine in einem Messenger-Dienst verfasste Nachricht – noch vor seiner Verschlüsselung abgehört bzw. mitgelesen werden.[9] Mit dem ersten Staatstrojaner des Unternehmens DigiTask war allerdings auch eine Vergrößerung des Zugriffsspektrums möglich, sodass die Quellen-TKÜ auf eine umfassende Online-Durchsuchung erweitert werden konnte.[10] Die Kritik an dieser ersten Form des Staatstrojaners bestand unter anderem darin, dass die Software abseits derjenigen staatlichen Behörden entwickelt wurde, die sie dann einsetzen sollten und somit wenig Platz für staatliche Überprüfung der Technik bestand.[11] Dies hat sich mit der Einführung eines neuen, staatlich entwickelten Trojaners nun erledigt.[12]

IT-Sicherheit

Problematisch ist in erster Linie natürlich, dass – wie oben gesehen – die

Infiltrierung des IT-Systems eine Sicherheitslücke erfordert. Damit besteht für Ermittlungsbehörden stets ein potenzielles Interesse an dem Erhalt von bestehenden Lücken. Im Mai 2017 hat sich genau dieses Dilemma in der sog. WannaCry-Attacke realisiert.[13] Bei derartigen Angriffen werden Sicherheitslücken zum Zugriff von unbefugten Dritten ausgenutzt und zahlreiche Rechner zum Zwecke weitreichender Erpressung infiltriert; häufig werden dabei Rechner von bedeutenden Einrichtungen wie etwa Krankenhäusern anvisiert.[14] Der Schaden durch Cyberangriffe in Deutschland liegt derzeit im zweistelligen Milliardenbereich.[15] Hinzu kommt, dass Sicherheitslücken stets in der Software zu finden sind, sodass von ihnen nicht nur das konkret zu überwachende System betroffen ist, sondern auch alle Geräte, die mit der gleichen Software ausgestattet sind.[16] Häufig werden zur Infiltrierung mittels Staatstrojaner Schwachstellen in weit verbreiteter Software wie etwa Java, Microsoft oder Antivirenprogrammen genutzt,[17] was die Risikosphäre deutlich erweitert. Wie kann also dem Bestreben nach IT-Sicherheit durch die Entwicklung neuer Verschlüsselungstechniken genüge getan werden, wenn dies zur Gefahrenabwehr und Strafverfolgung gleichzeitig eine Umgehung durch staatliche Behörden erfordert?

Staatliche Eingriffsmöglichkeiten

- Online-Durchsuchungen
- Quellentelekommunikationsüberwachung

Entsprechende Überwachungsmöglichkeiten

- Anfertigen von Bildschirmfotos
- Verfolgen von Tastatureingaben
- Erstellen von Bewegungsprofilen
- Ablesen von Chat-Nachrichten

Betroffene Geräte

- Smartphones
- Laptops
- Sprachassistenten
- vernetzte Autos
- alle sonstigen »smarten« Geräte

Während der staatliche Konflikt zwischen dem Nutzen und dem Schädigungspotenzial von Sicherheitslücken den Kern des Dilemmas darstellt, sind indes auch zahlreiche Folgeprobleme zu verzeichnen. Eines davon ist etwa die Entstehung eines „Schwarzmarkts" für Sicherheitslücken. Unternehmen spezialisieren sich auf die Ermittlung von Sicherheitslücken durch sog. „Bug

6 S. zur technischen Durchführung Blechschmitt, StraFo 2017, 361, 362 f.

7 *Kruse/Grzesiek*, KritV 04/2017, 331, 337 f.

8 *Kruse/Grzesiek*, KritV 04/2017, 331, 334 f. mit weiteren Beispielen.

9 *Kipker*, ZRP 2016, 88, 88.

10 *Kipker*, ZRP 2016, 88, 88.

11 *Kipker*, ZRP 2016, 88, 88.

12 *Roggan*, GSZ 2/2018, 52, 52; BT-Drs. 18/2352, 23 f.; *Kipker*, ZRP 2016, 88, 88.

13 S. dazu Beitrag auf https://www.zeit.de/thema/wannacry, abgerufen am 06.06.2018.

14 Beitrag vom 14.05.2018 auf http://www.faz.net/aktuell/politik/inland/verfassungsschutz-warnt-vor-cyberattacken-auf-infrastruktur-15588804.html, abgerufen am 06.06.2018.

15 *Pohlmann/Riedel*, DuD 2018, 37, 37 m.w.N.

16 *Roggan*, StV 2017, 821, 828.

17 *Pohlmann/Riedel*, DuD 2018, 37, 40.

Bounty"-Programme.[18] Erleichtert wird dies natürlich besonders dann, wenn Sicherheitslücken bewusst offen gehalten werden.[19] Eine weitere Folgeerscheinung ist der sog. „Greymarket", bei welchem Schwachstellen zu „guten Zwecken" wie der (auch ausländischen) Strafverfolgung vermarktet werden.[20] Zuletzt bleibt auf die Möglichkeit der gezielten Schädigung von Personen durch Kontrollübernahme von IT-Systemen hinzuweisen, man denke etwa an die Fremdsteuerung des Assistenzsystems eines Fahrzeugs.[21]

Ausblick

Insgesamt mag die Infiltrierung zur Gefahrenabwehr und zur Strafverfolgung legitime Zwecke verfolgen.[22] Angesichts der obigen Ausführungen stellt sich allerdings die Frage, ob nicht ein Richtungswechsel in der Gesetzgebung erforderlich ist. Dementsprechend haben sich verschiedene Stimmen kritisch zu der StPO-Novelle im letzten Jahr geäußert.[23] Alternativ wird etwa vorgeschlagen, die TKÜ nicht an den unverschlüsselten Daten vorzunehmen, sondern die zunächst verschlüsselten Daten abzugreifen und vom Hersteller erforderlichenfalls einen Schlüssel zur Dekryptierung zu erhalten.[24] Wie sich diese Problematik in der Praxis weiterentwickeln und wie ihr begegnet werden wird, bleibt abzuwarten. Sicher ist jedoch, dass dies ein Zusammenwirken der zahlreichen betroffenen Kreise verlangt.

Nawrocki/Metzl

18 *Pohlmann/Riedel*, DuD 2018, 37, 38.

19 S. z. zeitlichen Ablauf der Sicherheitslücke nach ihrer Entdeckung Abb. 1 bei *Pohlmann/Riedel*, DuD 2018, 37, 38.

20 *Pohlmann/Riedel*, DuD 2018, 37, 43.

21 S. dazu Beitrag vom 18.10.2017 auf http://www.handelsblatt.com/unternehmen/dienstleister/cyberangriffe-autos-werden-zum-ziel-von-hackern/20470674.html?ticket=ST-624799-Ctr36ttlloNIntqgdWQx-ap3, abgerufen am 06.06.2018.

22 So auch *Pohlmann/Riedel*, DuD 2018, 37, 44; nicht grds. ablehnend ggü. der Schaffung einer entsprechenden Ermächtigungsgrundlage: Stellungnahme von Sinn vom 30.05.2017, abrufbar unter https://www.bundestag.de/blob/509050/6f72dd42df72be6f2da6a024475b3f8a/sinn-data.pdf, abgerufen am 06.06.2018.

23 S. Stellungnahme Nr. 44/2017 des Deutschen Anwaltvereins (Ausschuss Strafrecht), Juni 2017, abrufbar unter https://anwaltverein.de/de/newsroom?newscategories=3&category=&startDate=21.06.2017&endDate=23.06.2017&searchKeywords=, abgerufen am 06.06.2018; Beschlussempfehlung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages vom 31.05.2017, insb. S. 3, abrufbar unter http://dip21.bundestag.de/dip21/btd/18/126/1812600.pdf (BT Drs. 18/12600), abgerufen am 06.06.2018.

24 *Freiling/Safferling/Rückert*, JR 2018, 9, 18.

Designed by Tobias Springer und Marie Nawrocki

Der nächste Newsletter erscheint am 15. September 2018.

Sie finden den Newsletter und die Möglichkeit, sich an- bzw. abzumelden auch unter https://www.baywidi.de/

Hinweise, Anregungen, Lob und Kritik sind herzlich willkommen. Schreiben Sie uns einfach unter: baywidi@uni-passau.de

Impressum

Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Organisation
Gemäß Art. 11 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung:
Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.