Prof. Dr. Volker Lüdemann, Christin Sengstacken, LL.M., Kerstin Vogelpohl

Pay as you drive: Datenschutz in der Telematikversicherung

Das Angebot ist verführerisch. Daten gegen Geld. Wer der KfZ-Versicherung Einblick in sein Fahrverhalten gibt, kann bei vorsichtigem Fahrstil die Prämie senken. Seit Anfang des Jahres ist dies auch in Deutschland möglich. Kunden müssen dafür nur eine Box im Auto installieren, die Daten über das Fahrverhalten speichert und an den Versicherer übermittelt. In der Automobil- und Versicherungsbranche sind maßgeschneiderte Tarife schon seit langer Zeit ein Thema. Bislang stehen neben Datenschutzbedenken vor allem die hohen Infrastrukturkosten dem breiten Einsatz entgegen. Die Einführung des gesetzlich verpflichtenden eCalls ab Herbst 2015 ändert die Situation grundlegend. Mit dem Einbau der hierfür erforderlichen Technik ist künftig jedes Auto telematikfähig. Das Argument der hohen Infrastrukturkosten ist dann hinfällig. Versicherungsexperten gehen davon aus, dass pay-as-you-drive-Tarife bereits in wenigen Jahren eine feste Größe im Kfz-Versicherungsmarkt darstellen. Aus Sicht des Datenschutzes spricht nichts gegen Telematiktarife, wenn die Kunden einwilligen und die Datenschutzgrundsätze eingehalten werden. Risiken entstehen jedoch abseits des eigentlichen Tarifmodells. Diesen versteckten datenschutzrechtlichen Gefahren geht der Beitrag nach.

I. Einleitung

Die Kfz-Versicherung befindet sich im Umbruch. Im Zuge intelligenter und vernetzter Automobile hält die Telematikversicherung Einzug in den Haftpflichtversicherungsmarkt. Nicht zuletzt die Car2Car Kommunikation und der automatische Notruf eCall[1] verändern das Fahrverhalten auf deutschen Straßen, auch Versicherungen bemühen sich um das Auto der Zukunft. Als erster deutscher Versicherer bietet die „Sparkassen Direkt Versicherung“ (S-Direkt) seit Beginn des Jahres ein Tarifmodell an, dessen Versicherungsprämie in Abhängigkeit des Fahrverhaltens bemessen wird. Dieses Versicherungsmodell ist bisher einmalig auf dem deutschen Markt. Neu ist es hingegen nicht, amerikanische und britische Agenturen bieten bereits seit Jahren erfolgreich fahrbezogene Telematikversicherungen an[2].

Das Tarifmodell erfordert eine detaillierte und dauerhafte Datenverwendung, um die fahrbezogene Versicherungsprämie bestimmen zu können[3]. Datenschützer befürchten dadurch eine Überwachung des Autofahrers, die ungewollte und ausufernde Datenverwendungen nach sich ziehen könnten[4]. Denn bereits erhobene Daten wecken Begehrlichkeiten auf Seiten weiterer Wirtschaftsteilnehmer abseits des Versicherungsmarktes. Durch die Möglichkeit, mithilfe der Daten Bewegungs-, Nutzungs- und Kommunikationsprofile zu erstellen[5], erlangen die Fahrdaten einen Wert, dessen wirtschaftliche Bedeutung vom Fahrzeugnutzer nicht abschätzbar ist. Kritische Auseinandersetzungen müssen jedoch berücksichtigen, dass es sich bei diesem Versicherungsmodell nicht um eine zwingende Datenpreisgabe handelt. Die Telematikversicherung ist lediglich ein neues Tarifangebot an den Versicherungskunden. Die datenschutzrechtliche Risikobewertung muss sich daher an der vertraglichen Gestaltung der vorhandenen Versicherungsbedingungen orientieren. Die Art und Weise der Datenverwendung sollte dem Kunden größtmöglichen Schutz bieten, wenn er sich für das Angebot entscheidet. Dafür müssen die gesetzlichen Datenschutzmaßnahmen ausreichend berücksichtigt und eingehalten werden. Es steht daher nicht zur Debatte, ob Telematikversicherungen aus Datenschutzsicht grundsätzlich zulässig sind, sondern ob ihre jeweilige Umsetzung datenschutzkonform ist.

Der vorliegende Beitrag bietet zunächst eine Übersicht des neuen Versicherungsmodells (II.) und bewertet dieses vor ausgewählten datenschutzrechtlichen Gesichtspunkten (III.), abschließend wird das Versicherungsmodell einer kritischen Würdigung unterzogen (IV.).

II. Darstellung des Versicherungsmodells am Beispiel S-Drive[6]

Die Telematikversicherung ist auf dem deutschen Versicherungsmarkt ein Novum. Das Verständnis ihres Ablaufs bedingt die Erklärung anhand existierender Vertragsregelungen. Da die „Sparkassen Direkt Versicherung“ bisher einziger Anbieter des Versicherungsmodells ist, sollen hier stellvertretend deren Vertragsbestimmungen zur Beschreibung der Funktionsweise herangezogen werden.

Der Versicherungsnehmer erhält nach Abschluss des Vertrags eine Messbox, die in seinem Fahrzeug installiert wird. Die Box zeichnet auf, wann, wo und wie schnell gefahren wurde. Ebenfalls registriert sie starke Beschleunigungen und abrupte Bremsvorgänge. Der Kunde erhält einen kennwortgeschützten Zugang zu einem Webportal und einer Smartphone-App, wodurch er jede einzelne Fahrt nachträglich betrachten und nachvollziehen kann. Gleichzeitig beinhaltet der Service eine Fahrzeugortungs-Funktion und einen automatischen Notruf. Bei Diebstahl des Pkws können Versicherungsnehmer oder Versicherungsgeber eine Ortung durchführen. Zudem registrieren Crash-Sensoren

1 Zum Datenschutz beim automatischen Notruf siehe auch Lüdemann/Sengstacken, Lebensretter eCall: Türöffner für neue Telematikdienstleistungen, RDV 2014, 177; Rohwetter, Geheimfunk im Notruf, Die Zeit 29/2014, S. 25.

2 Die Versicherungsmodelle besitzen eine große Popularität auf dem Markt der Fahranfänger bspw. mit dem Versicherungspaket „drive like a girl“, abrufbar unter: http://www.drivelikeagirl.com/.

3 Roßnagel, Datenschutz in der künftigen Verkehrstelematik, NZV 2006, 281.

4 So unter anderem der ehemalige Bundesdatenschutzbeauftragte Schaar, abrufbar unter: http://www.autohaus.de/telematik-telefonica-vernetzt-auto-und-versicherung-1237602.html.

5 Weichert, Datenschutz im Auto – Teil 2, SVR 2014, 241.

6 Die folgenden Darstellungen sind den Vereinbarungen zum Telematik-Sicherheits-Service (S-Drive-Service) der Sparkassen-Direkt-Versicherung entnommen, abrufbar unter: https://www.sparkassen-direkt.de/fileadmin/pdf/telematik/Endkundenvertrag.A2.2.pdf. Zudem bietet nun die Signal-IDuna Tochter Sijox eine pay as you drive-Versicherung an, siehe www.aap-drive.de.

eine Kollision anhand von Beschleunigungskräften. Das System übermittelt den exakten Unfallort, die Stärke der Beschleunigungskräfte, Uhrzeit und Fahrtrichtung an eine Notrufstelle.

Die Datenverarbeitung findet in zwei voneinander getrennten Datenkreisen statt. Die von der Box gemessenen Werte werden in Form von Rohdaten alle 20 Sekunden an einen Kooperationspartner gesendet[7]. Dort werden sie im Auftrag gegen eine Kunden-ID erhoben und verarbeitet. Persönliche Daten, die Rückschlüsse auf eine bestimmte Person zulassen, besitzt nur der Versicherungsgeber. Der Kooperationspartner und von ihm beauftragte Subunternehmen ermitteln auf Grundlage der Datensätze Score-Werte. Nach der Bearbeitung erhält die Versicherung monatlich insgesamt fünf Score-Werte. Vier Score-Werte ergeben sich für Geschwindigkeit, Fahrweise, Nachtfahrten und Stadtfahrten, aus ihnen wird ein Gesamtscore durch Gewichtung der Einzelscores ermittelt. Dem Versicherungsgeber ist es nicht möglich, dem Versicherungsnehmer einzelne Fahrten zuordnen. Diese Möglichkeit besitzt lediglich der Kunde, indem der Kooperationspartner die aufbereiteten Daten auf dem Webportal bzw. der App zur Verfügung stellt.

Auf Grundlage der Score-Werte ermittelt der Versicherungsgeber die zu zahlende Versicherungsprämie. Erreicht der Kunde einen guten Jahres-Gesamtpunktwert, erhält er einen Rabatt von 5% auf seine nächste Jahres-Beitragsrechnung. Liegt der Score unter dem festgelegten Zielwert, wird kein zusätzlicher Beitrag fällig, es bleibt bei der zum Vertragsabschluss vereinbarten Versicherungsprämie. Zusätzlich werden dem Kunden jährlich 71,40 EUR für die Bereitstellung der Telematikbox in Rechnung gestellt.

III. Datenschutzrechtliche Beurteilung

Die Telematikversicherung im Kfz-Bereich ist grundsätzlich rechtskonform[8]. Die datenschutzrechtliche Legitimation ergibt sich aus dem Versicherungsvertrag und umfasst gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG jene Datennutzung, die für die Erfüllung des Vertragszwecks erforderlich ist. Da die freiwillige Entscheidung des Versicherungsnehmers die Datenverwendung bestimmt und auslöst, handelt es sich um ein in den Grenzen des Bundesdatenschutzrechts frei zu gestaltendes Vertragsverhältnis. Die proklamierten Risiken der Fahrerüberwachung und der Erstellung von Bewegungsprofilen werden durch die vorhandene Vertragsgestaltung nicht erfüllt.

Denn obgleich die installierte Messbox personenbezogene Daten erhebt, werden diese zur weiteren Verarbeitung an den Kooperationspartner sowie dessen beauftragte Subunternehmer pseudonymisiert übermittelt. Die Erhebung unter Nutzung der Kunden-ID verhindert den Rückschluss auf den Versicherungsnehmer. Eine Herstellung des Personenbezugs ist an dieser Stelle nur mit einer entsprechenden Referenzliste möglich[9]. Der Versicherungsgeber selbst erhält lediglich aggregierte Datensätze als Scorewerte. Diese können dem Versicherungsnehmer zwar zugeordnet werden, besitzen jedoch nicht die erforderliche Informationstiefe, um eine Erstellung von Bewegungsprofilen zu ermöglichen. Der Versicherungsgeber erhält keine detaillierten Datensätze, damit er keine fahrtgenaue Überwachung betreiben kann. Das System zweier getrennt gestalteter Datenverwendungskreise ermöglicht hinsichtlich der Fahrtüberwachung durch die Versicherung einen ausreichenden Datenschutz.

Darüber hinaus eröffnen sich jedoch Risikopotentiale, die in der bisherigen Kritik kaum Beachtung gefunden haben. Diese betreffen insbesondere die Fahrzeugnutzung durch Dritte, die automatische Bemessung der Versicherungsprämie sowie Datenverwendungsmöglichkeiten über den Versicherungsgeber hinaus.

1. Überwachungsrisiko durch den Versicherungsnehmer

Ein Überwachungsrisiko ergibt sich nicht durch den Versicherungsgeber, sondern in Person des Versicherungsnehmers. Eine vertragliche Regelung und damit eine datenschutzrechtliche Erlaubnis existiert nur zwischen der Versicherung und ihrem Kunden. Mittels Kennwortzugang zum Webportal bzw. zur App erhält ausschließlich der Versicherungsnehmer Einsicht in die Fahrtdaten des Pkw. Dadurch besitzt er die uneingeschränkte Möglichkeit, das betroffene Fahrzeug und dessen Nutzung ständig überwachen zu können. Weichen Fahrzeugnutzer und Versicherungsnehmer voneinander ab, können die Fahrdaten von Letzterem uneingeschränkt eingesehen werden. Der Versicherungsgeber bestimmt in den Vertragsbedingungen, dass der Versicherungsnehmer jeden anderen Nutzer des Fahrzeugs darauf hinzuweisen hat, dass eine Erfassung der Fahrtdaten erfolgt und diese von ihm eingesehen werden können[10].

Bei der privaten Pkw-Nutzung mag dieses Risiko gering erscheinen, da im familiären Bereich eine Überwachung der Fahrdaten und des Aufenthaltsortes nur private Konsequenzen nach sich zieht[11]. Gleichwohl ist das Recht auf informationelle Selbstbestimmung eines dritten Fahrers gefährdet, wenn die Datenerhebung nicht offensichtlich ist. Denn sein Recht kann er nur wahrnehmen, wenn er weiß, ob und wie Daten über ihn erhoben werden. Die Transparenz der Datenverarbeitung müsste an dieser Stelle den Datenschutz gewährleisten[12]. Kommt der Versicherungsnehmer seiner Hinweispflicht zur Datenverarbeitung nicht nach, müsste die technische Gestaltung der Messbox die Transparenz der Datenverarbeitung gewährleisten. Der Vorgang der Datenerhebung sollte dem Fahrer stets im Pkw angezeigt werden, so dass er sich des Eingriffs in sein Recht auf informationelle Selbstbestimmung bewusst ist. Gleichwohl müsste ihm die Möglichkeit zugestanden werden, die Datenverarbeitung unterbrechen zu können. Dies ist nicht möglich, da ein Ausbau oder eine Stilllegung des Geräts ohne vorheriges Einverständnis des Versicherungsgebers nicht erlaubt ist[13]. Diese technisch bedingte Wahlbehinderung müsste

7 Im Rahmen des S-Drive-Service werden die Daten an den Téléfonica Digital Instance Server im Hosting Center der TeleCityGroup nach London gesendet und dort von der Firma Masternaut verarbeitet.

8 So auch der Landesdatenschutzbeauftragte Schleswig-Holsteins Weichert, abrufbar unter: http://www.heise.de/newsticker/meldung/Datenschuetzer-warnt-vor-Versicherungstarif-mit-Wanze-im-Auto-2074881.html.

9 Gola, in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 3a Rn. 10.

10 § 7 der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

11 Ebenfalls möglich ist ein Anwendungsausschluss des BDSG gem. § 1 II Nr. 3 BDSG, da die Datenerhebung ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt; a. M. Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl., § 1 Rn. 10, welcher den Ausschluss nur begründet, wenn die Datenverarbeitung nicht automatisiert erfolgt; ebenso restriktive Auslegung lt. Dix, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl. 2011, § 1 Rn. 148 m. w. N.

12 In diese Richtung auch Roßnagel, 281 (Fn. 3).

13 § 5c der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

zumindest für anderweitige Nutzer offensichtlich gemacht werden, indem die Transparenz der Datenerhebung durch Signale oder Icons im Fahrzeug hergestellt würde[14].

Problematischer erweist sich das Überwachungsrisiko bei dienstlicher Fahrzeugnutzung, etwa bei Außendienstmitarbeitern. Der Abschluss einer Telematikversicherung für Dienstfahrzeuge ermöglicht dem Arbeitgeber die Überwachung des Arbeitnehmers auf unkomplizierte Weise. Für den Arbeitgeber ist es lohnenswert zu wissen, ob sich der Außendienstmitarbeiter auf dem schnellsten Weg zum Kunden begibt, ob er während der Fahrt an anderen Orten verweilt und wie lange er sich tatsächlich beim Kunden aufhält. Der Vorgang der telematikbasierten Standortnutzung ist vergleichbar mit der Ortungsmöglichkeit eines Betriebsmobiltelefons[15]. Dabei besteht eine vertragliche Vereinbarung ebenfalls nur zwischen dem Telekommunikationsdienstleister und dem Arbeitgeber als Vertragskunde. Der Arbeitgeber ist gem. § 98 Abs. 1S. 2 TKG verpflichtet, weitere Nutzer über die erteilte Einwilligung in die Handyortung zu informieren. Unterlässt er dies, besteht die Gefahr der heimlichen Überwachung des Arbeitnehmers. Eine Rechtfertigung für den Einsatz dieser Überwachungsmöglichkeit könnte gem. § 32 Abs. 1 S. 1 BDSG durch das arbeitsvertragliche Kontrollinteresse des Arbeitgebers gegeben sein[16]. In diesem Zusammenhang dürfen personenbezogene Daten des Beschäftigten verarbeitet werden, wenn dies für die Durchführung des Beschäftigtenverhältnisses erforderlich ist. Erlaubt ist eine Datennutzung etwa für die Optimierung des Fuhrparkeinsatzes oder das Aufspüren gestohlener Fahrzeuge[17]. Eine vollständige Kontrolle des Arbeitnehmers am externen Arbeitsplatz würde jedoch einen unzulässigen Eingriff in das Persönlichkeitsrecht darstellen, insbesondere wenn der Pkw auch der zusätzlichen privaten Nutzung unterliegt[18]. Diese Grundsätze müssten auch für die Überwachung des Arbeitnehmers durch die Standortbestimmung mittels Telematikversicherung gelten. Denn es könnte ein zusätzlicher Druck auf den Arbeitnehmer entstehen, indem sein Fahrverhalten der ständigen Kontrolle unterliegt. Eine Konfliktsituation zwischen Fahrüberwachung und termingerechter Wahrnehmung von Außendiensstterminen wäre die Folge.

Ebenso stellt sich bei der Mehrfachnutzung des Fahrzeugs die Frage, wem die erzeugten Versicherungsscores zuzurechnen sind. Die Scores werden ausschließlich auf Grundlage der Fahrleistung ermittelt, eine Autorisierung des Fahrers erfolgt nicht. Sie werden grundsätzlich dem Versicherungsnehmer zugeordnet. Eine nachträgliche Berichtigung der Fahrtdaten erscheint ausgeschlossen. Dies folgt allein schon aus den Versicherungsbedingungen, die gleichfalls einen nachträglichen Korrekturanspruch von Fehlmessungen durch das Messsystem ausschließen[19].

2. Risiko der automatisierten Einzelentscheidung

Bedenklich erscheint vor dem Hintergrund des Verbots der automatisierten Einzelentscheidung die Berechnung der telematikbasierten Versicherungsprämie. Denn eine Bewertung, die den Betroffenen auf ein bloßes Objekt eines automatisierten Entscheidungsverfahrens reduziert, unterliegt dem Verbot des § 6a BDSG. Der Gesetzgeber beabsichtigt, vor automatisierten, beeinträchtigenden Entscheidungen zu schützen, die ausschließlich aufgrund der Bewertung von Persönlichkeitsprofilen ergehen, ohne dass der Betroffene die Möglichkeit der Einflussnahme oder der Nachvollziehbarkeit hat[20].

Die durch Telebox erhobenen personenbezogenen Daten bilden die ausschließliche Datenbasis, auf welcher mithilfe des Scoreverfahrens eine unmittelbare Entscheidung über den Versicherungsnehmer getroffen wird[21]. Grundlage der automatisierten Einzelentscheidung bildet die Bewertung von Persönlichkeitsmerkmalen, welche laut Art. 15 Abs. 1 EU-DatSchRl auch Verhalten und Zuverlässigkeit von Personen umfassen. Persönlichkeitsmerkmale setzten somit eine gewisse Komplexität voraus[22]. Der Versicherungsgeber erhält Score-Werte über Geschwindigkeit, Fahrweise sowie Nacht- und Stadtfahrten. Der Score Geschwindigkeit erfasst die Einhaltung von Geschwindigkeitsbegrenzungen und verschlechtert sich bei Überschreitungen. Mithilfe des Scorewertes kann daher ein Rückschluss auf Verhalten und Zuverlässigkeit des Versicherten erfolgen. Ein weiterer Rückschluss auf das Verhalten ist durch die Score-Werte Stadtfahrt und Nachfahrt möglich. Sie veranschaulichen, zu welcher Tageszeit und auf welche Art der Versicherte sein Fahrzeug nutzt. Zusätzlich wird die Fahrweise bewertet. Diese vier Score-Werte stellen Aspekte der Persönlichkeit des Versicherungsnehmers dar; werden sie miteinander verknüpft, kann die Persönlichkeit des Versicherungsnehmers abgelesen und bewertet werden.

Die Ausschließlichkeit der automatisierten Entscheidung liegt vor, wenn keine inhaltliche Bewertung und eine darauf gestützte Entscheidung durch eine natürliche Person stattfindet. Eine Umgehung des Verbots soll insbesondere verhindert werden, indem lediglich eine mehr oder minder formale Bearbeitung durch einen Menschen erfolgt, der keine Befugnis oder ausreichende Datengrundlage besitzt, um von der automatisierten Entscheidung abweichen zu können[23]. Der Entscheidung muss daher ein menschliches Ermessen zugrunde liegen. Die profane Übernahme einer vorbereiteten automatisierten Entscheidung ist dabei nicht angebracht, der menschliche Entscheidungsträger muss einen Spielraum für abweichende Entscheidungen besitzen. Für die Ermittlung der Versicherungsprämie ist ausschließlich die Gesamtsumme der Score-Werte entscheidend, weitere Faktoren oder gar eine Überprüfung der ermittelten Datensätze findet nicht statt[24].

Auch weitere Gesichtspunkte zur Ermittlung der Versicherungsprämie fließen nicht in die Entscheidung ein. Vielmehr wird nicht einmal die auftretende Fehlerquote von falsch gemessenen Daten der Telebox berücksichtigt[25]. Bisher besteht auch keine Möglichkeit der Korrektur[26]. Durch menschliche

14 So auch für andere Bereiche in der Kfz-Telematik gefordert von Weichert, Datenschutz im Auto – Teil 2, SVR 2014, 241.

15 Gola, Datenschutz bei der Kontrolle „mobiler" Arbeitnehmer, NZA 2007, 1139.

16 Hallaschka/Jandt, Standortbezogene Dienste im Unternehmen, MMR 2006, 436.

17 Wedde, in: BDSG, § 32 Rn. 104 (Fn. 11).

18 Gola, 1139 (Fn. 15); so auch die permanente Ortung verneinend Wedde, in: BDSG, § 32 Rn. 108 (Fn. 11).

19 § 1e der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

20 Klug, in: Gola/Schomerus, BDSG § 6a Rn. 1 (Fn. 9).

21 Vgl. Scholz, in: Simitis (Hrsg.), BDSG, § 6a Rn. 5 (Fn. 11).

22 Klug, in: Gola/Schomerus, BDSG, § 6a Rn. 7 und 9 (Fn. 9).

23 So die Begründung zur Novellierung des § 6a I BDSG und der Einführung des Satz 2 im Jahr 2009, siehe BT-Drs. 16/10529 S. 13; Abel, Die neuen BDSG-Regelungen, RDV 2009, 147.

24 § 9e der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

25 § 1d der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

26 § 1e der Vereinbarungen zum Telematik-Sicherheits-Service (Fn. 6).

Überprüfung könnte jedoch ein höheres Vertrauenspotenzial in das Versicherungsmodell generiert werden.

Die rechtliche Folge der automatisierten Entscheidung beeinträchtigt den Betroffenen in erheblichem Maße, denn mit ihr gehen relevante negative Folgen für den Betroffenen einher[27]. Ungeachtet der Folge einer möglichen höheren Versicherungsprämie kommt grundsätzlich eine erhebliche Beeinträchtigung des Versicherungsnehmers in seinem Persönlichkeitsrecht in Betracht. Denn der Zweck des BDSG ist es gemäß § 1 Abs. 1 BDSG, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird[28]. Es soll gewährleisten, dass der Einzelne selbst bestimmt, wann welche Informationen über ihn preisgegeben werden, um ein selbständiges Gesellschaftsmitglied zu sein[29]. Andernfalls würde der Einzelne zum Adressat von „optimierten" Verhaltenserwartungen degradiert werden[30]. Es stellt sich die Frage, inwiefern der Versicherungsnehmer sich bei dieser Entscheidungsgrundlage eigenständig verhalten kann. Zwar erteilt er seine Erlaubnis, dass seine personenbezogenen Daten erhoben und verarbeitet werden, allerdings wird ihm die Möglichkeit entzogen, deren Auswertung inhaltlich zu kontrollieren. Dadurch wird er gezwungen, sein Verhalten anzupassen, um in den Genuss eines Rabatts zu gelangen.

Darüber hinaus liegt eine erhebliche Beeinträchtigung vor, wenn der Betroffene durch die Entscheidung in seiner wirtschaftlichen oder persönlichen Entfaltung nachhaltig gestört wird[31]. Wenn anzunehmen ist, dass sich telematikbasierte Versicherungsmodelle auf dem Versicherungsmarkt durchsetzen, wird sich auch die Kostenstruktur alternativer Versicherungsmodelle verändern. Daraus würde folgen, dass durch einen hohen Zuspruch der Versicherungsnehmer die Preise für alternative Angebote steigen. Versicherungsnehmer könnten gezwungen sein, telematikbasierte Angebote annehmen zu müssen. Sie wären damit in ihrer Wahlfreiheit eingeschränkt und müssten ihre Daten unfreiwillig zur Verfügung stellen, obgleich sie dies nicht wünschen. Ein derartiger Zwang würde gleichfalls eine Beeinträchtigung der informationellen Selbstbestimmung bedeuten, da ein datenschützendes Verhalten nur noch unter unverhältnismäßigem Aufwand möglich wäre.

3. Risiko weiterer Datenverwendungen

Werden Daten für einen bestimmten Zweck erhoben, bergen sie grundsätzlich die Gefahr der Begehrlichkeit weiterer Wirtschaftsteilnehmer zu unterliegen. Datenverwendungsmöglichkeiten eröffnen sich dabei nicht nur im privatwirtschaftlichen Umfeld, sondern auch im Bereich der Unfallaufklärung bis hin zur Verfolgung von Straftaten. Mittels Telematikversicherung erhobene Daten könnten insbesondere genutzt werden, um die Aufklärung von Verkehrsdelikten zu beschleunigen und zu vereinfachen[32]. Ihre Nutzung durch Strafverfolgungsbehörden ist dabei eine naheliegende Verwendungsmöglichkeit, die unter dem Deckmantel der Unfallaufklärung begründet werden könnte.

Rückblickend betrachtet, hat sich das Strafverfolgungsinteresse auch auf neue technische Entwicklungen und moderne Kommunikationsmöglichkeiten ausgeweitet. Mithilfe von modernen Kommunikationsmedien erhobene Daten müssen gem. § 100a ff StPO unter Umständen den Strafverfolgungsbehörden zur Verfügung gestellt werden[33]. Dieses Interesse könnte auch auf mittels Telematikversicherung erhobene Daten ausgeweitet werden, dafür bedürfte es jedoch einer gesetzlichen Erlaubnis. Eine Parallele ergibt sich zur strafrechtlichen Verwertung von Autobahnmautdaten, sog. „TollCollect Daten". Das LG Magdeburg hatte zu entscheiden, ob eine Herausgabe dieser Daten an die Strafverfolgungsbehörden im Diebstahlsfall gemäß § 100 g f. StPO rechtmäßig ist[34]. Dieses wurde mit der Begründung verneint, dass die Erhebung der Daten unter strenger gesetzlicher Zweckbestimmung des Autobahnmautgesetzes erfolgte. Eine darüber hinausgehende Datenverwendung würde eine Zweckänderung mit sich bringen, die der Gesetzgeber ausdrücklich verweigert[35]. Eine derartige gesetzliche Zweckbestimmung existiert für Daten aus Telematikversicherungen nicht. Ihre Verwendung wird lediglich durch zugrundeliegende Vertragsbedingungen bestimmt. Eine Ausweitung auf andere Zwecke erscheint daher möglich. Mit dieser Maßnahme könnten Verkehrsunfälle effektiver aufgeklärt werden, dies gilt auch für leichte Verkehrsverstöße z.B. Geschwindigkeitsübertretungen. Denn die Daten liegen erhoben vor und werden, obgleich für einen anderen Zweck, zunächst gespeichert. Zu beachten ist dabei, dass eine Verwendung für andere Zwecke vor dem Hintergrund des § 28 II BDSG zu beurteilen ist. Demzufolge ist eine Übermittlung von Daten für einen Zweck zulässig, der der Verfolgung von Straftaten dient, und wenn kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. An der Interessenabwägung lässt sich bereits eine restriktive Auslegung des Ausnahmetatbestandes erkennen, nicht zuletzt muss sich auch die ursprüngliche Datenerhebung der verantwortlichen Stelle auf die Erfüllung eigener Geschäftszwecke beschränken. Als Beispiel sei genannt, dass auch der Arbeitgeber die Fahrtdaten seiner Dienstwagenflotte nur bei schwerwiegenden Verkehrsverstößen an die Polizei herausgeben wird[36].

Eine weitere Ähnlichkeit lässt sich zum Einsatz von Unfalldatenspeichern erkennen. Auch diese erfassen die Fahrdaten und können bei Unfällen zur Aufklärung der Sachlage dienen. Entscheidender Unterschied bei der Datenerfassung ist, dass die Daten im Unfalldatenspeicher im Abstand von 45 Sekunden überschrieben werden und der Fahrzeugführer die Möglichkeit hat, mittels Knopfdruck gespeicherte Daten zu löschen[37]. Diese Möglichkeit bleibt dem Versicherungsnehmer bei Telematikdaten verwehrt. Diese Tatsache fällt besonders ins Gewicht, wenn der Fahrzeugführer sich durch die erfassten Daten selbst belas-

27 Scholz, in: Simitis (Hrsg.), BDSG, § 6a Rn. 28 (Fn. 11).

28 Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl., § 1 Rn. 1.

29 Gola, in: Gola/Schomerus, BDSG, § 1 Rn. 7 (Fn. 9); Roßnagel, 281, 282 (Fn 3).

30 Simitis, in: Simitis (Hrsg.), BDSG, § 1 Rn. 36 (Fn. 11).

31 Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Aufl. 2008, S. 159.

32 Roßnagel, 281, 281 (Fn. 3).

33 Roßnagel, 281, 285 (Fn. 3); zu dieser Problematik auch Mielchen, Daniela, Verrat duch den eigenen PKW – wie kann ich mich schützen, SVR 3/2014, 81.

34 LG Magdeburg, NStZ 2006, 34.

35 Vgl. LG Magdeburg, Beschluss vom 03.02.2006 – 25 Qs 7/06; ebenso das Bundesamt für Datenschutz und Informationssicherheit, abrufbar unter http://www.bfdi.bund.de/DE/Themen/WirtschaftUndFinanzen/Verkehr/Artikel/MautdatenFuerVerbrechensbekaempfung.html?nn=409802.

36 Gola, in: Gola/Schomerus, BDSG, § 28 Rn. 38 (Fn. 9).

37 Informationen zum Kienzle UDS, abrufbar unter http://www.rgvs.de/Angebote/UDS/uds.html.

ten könnte. Denn einen tatsächlichen Zugriff auf die gespeicherten Daten hat lediglich der Versicherungsgeber durch Anfrage beim datenverarbeitenden Subunternehmen. Nur dort kann eine Löschung veranlasst werden. Fraglich ist, ob der Versicherungsgeber bei Anfrage der Verfolgungsbehörde die Daten tatsächlich bereitstellt. Diese Praxis ist wahrscheinlich, da Versicherungen bereits jetzt Auskunft erteilen über Angaben, die im Rahmen von Schadensanzeigen getätigt werden. Es ist zwar möglich, diesen Eingriff in das Grundrecht auf informationelle Selbstbestimmung des Einzelnen zu rechtfertigen, wenn es dem überwiegenden Interesse der Allgemeinheit dient. Ein derartiger Eingriff wird in der Regel jedoch nicht bei geringfügigen Unfallschäden gerechtfertigt sein[38].

Derartige Datenauskünfte könnten gegen den nemo-tenetur-Grundsatz verstoßen[39]. Diesem Grundsatz zufolge ist niemand verpflichtet, sich selbst anzuklagen bzw. sich selbst zu belasten[40]. Bei der Verwendung von Telematikdaten, die ursprünglich freiwillig und mittels Einwilligung des Versicherungsnehmers für die Bemessung der Versicherungsprämie erhoben wurden, würde durch die Beschlagnahmung der Daten der nemo-tenetur-Grundsatz vollständig ausgehöhlt[41]. Um diesen Umstand zu umgehen, müsste der Versicherungsnehmer als erstes einen Zugriff auf die erhobenen Daten haben. Dies könnte durch eine Autorisierung der Rohdaten zur weiteren Verarbeitung erfolgen oder eine nachträgliche Löschungsmöglichkeit. Diese Maßnahme würde jedoch dem Versicherungsprinzip zuwider laufen, da der Versicherungsgeber nicht mehr zwingend alle relevanten Daten erhalten würde. Zudem erschwert sich die Lage, wenn nicht der Versicherungsnehmer sondern ein Dritter gefahren ist. Sodann wäre der Versicherungsgeber in der Lage, die Daten an die Verfolgungsbehörden herauszugeben. Dabei könnte es sich jedoch um Daten handeln, deren Erhebung nicht durch den Dritten autorisiert wurde, da kein Vertragsverhältnis zwischen ihm und der Versicherung besteht. Eine Übermittlung wäre in diesem Fall unzulässig.

Vor dem Hintergrund der Datenverwendungsmöglichkeiten ist es daher unzureichend, dass der Versicherungsnehmer derzeit keinen Einfluss auf die Weitergabe oder ihre Löschung hat.

IV. Fazit

Die Telematikversicherung kann grundsätzlich die Datenschutzregelungen erfüllen. Individuelle vertragliche Vereinbarungen verhindern es nicht, dass der Versicherungsnehmer einen ausreichenden Schutz seiner Datenverwendungen erwarten darf. Dieser Schutz steht allerdings in Abhängigkeit des Vertragspartners und darf nicht zu Lasten ausufernder Versicherungsbedingungen in den Hintergrund gedrängt werden.

Die Betrachtung des derzeitigen Versicherungsmodells zeigt ungeklärte Sachverhalte auf, die sich rechtlich in einer Grauzone bewegen. So könnte ein Verbot der automatisierten Einzelfallentscheidung vorliegen, indem die Prämienbemessung vollständig ohne menschliches Ermessen erfolgt. Dieser Vorgang wird nicht allen Fahrtsituation gerecht, da es oftmals auf die spontane Reaktion des Fahrers im Einzelfall ankommt. Eine pauschalierte Delegierung an eine automatische Entscheidungseinheit verkennt diesen menschlichen Aspekt. Ebenso ist es fraglich, die Informationspflicht über die Datenverwendung bei der Pkw-Nutzung durch Dritte an den Versicherungsnehmer zu delegieren. Eine Datenverwendung durch den Versicherungsgeber als verantwortliche Stelle beinhaltet auch die Informationspflicht des Betroffenen. Insbesondere im Bereich der Arbeitnehmerüberwachung ergibt sich eine gefährliche Korrelation zum Arbeitnehmerschutz.

Grundsätzlich gilt es zu beachten, dass im hart umkämpften Versicherungsmarkt der Datenschutz nicht auf Kosten des Versicherungsnehmers ausgehöhlt wird und zu einer Randbedingung degradiert wird. Obgleich bisher nur ein einziger Anbieter von Telematikversicherungen auf dem deutschen Markt existiert, könnten weitere Versicherungsgesellschaften nachziehen. Das verführerische Versprechen des Anbieters, durch zusätzliche Datenpreisgabe die Versicherungskosten zu senken, darf das Datenschutzbewusstsein der Versicherungsnehmer nicht verdrängen. Nahezu unausweichlich wird die restriktive Datenpreisgabe für den risikobewussten Verbraucher jedoch dann, wenn das Versicherungsmodell sich durchsetzt und alternative Angebote zur Ausnahme werden. An dieser Stelle wäre der Gesetzgeber gefordert, zu Beginn kritischer Auseinandersetzungen rechtliche Klarheiten zu schaffen. Dies gilt nicht zuletzt mit Hinblick auf mögliche Datenverwendungen durch die Strafverfolgungsbehörden, sondern auch auf jene im privatwirtschaftlichen Bereich. Ansonsten droht dem Autofahrer eine dauerhafte Überwachung durch das eigene Fahrzeug.

Prof. Dr. Lüdemann
ist seit 2009 Professor für Wirtschafts- und Wettbewerbsrecht an der Hochschule Osnabrück. Zuvor war er u.a. Syndikusanwalt und Geschäftsführer im Volkswagen Konzern. Volker Lüdemann forscht und lehrt im Bereich des Datenschutzes und verfügt über umfangreiche Erfahrungen als externer Datenschutzbeauftragter für öffentliche und nicht-öffentliche Stellen.

Christin Sengstacken, LL.M.
ist Referentin für Datenschutz und Compliance bei der Amprion GmbH in Dortmund. Zuvor war sie wissenschaftliche Mitarbeiterin und Projektleiterin am Forschungszentrum Energiewirtschaft und Energierecht (fee) der Hochschule Osnabrück und beschäftigte sich schwerpunktmäßig mit aktuellen datenschutzrechtlichen Fragestellungen.

Kerstin Vogelpohl
studiert an der Hochschule Osnabrück Wirtschaftsrecht LL.B. Neben ihrem Studium ist sie als studentische Hilfskraft am Forschungszentrum für Energiewirtschaft und Energierecht (fee) der Hochschule Osnabrück im Bereich Datenschutzrecht tätig.

38 Mielchen, 81, 85 (Fn. 33).

39 Vgl. § 136 I S. 2 StPO.

40 Pfeiffer, in: Pfeiffer, Strafprozessordnung Kommentar, 5. Aufl. 2005, § 136 StPO Rn. 4.

41 Mielchen, 81, 85 (Fn. 33).