RA Andreas Jaspers/Dr. iur. Lorenz Franck

Connected Car und Beschäftigtendatenschutz

Hinter den schillernden Begriffen "Connected Car" oder "Car-to-X" verbergen sich unüberschaubar viele Funktionalitäten und Konnektivitäten. Der „gläserne Autofahrer" avanciert dadurch zum Schreckgespenst. Die zunehmende Vernetzung und Automatisierung im Fahrzeug macht natürlich auch vor dem betrieblichen Flottenmanagement nicht Halt. Der folgende Beitrag erörtert die arbeitsrechtlichen Implikationen dieses Industrietrends.

I. Überblick

Die einstige Vorstellung von einer datenfreien Fahrt[1] ist überholt. Heute wirken bis zu achtzig Steuergeräte in einem modernen Kraftfahrzeug zusammen, die ihre Daten zum Teil dauerhaft in integrierten Speichern ablegen. Hinzu kommen zahlreiche Protokolle zur Kommunikation mit der Außenwelt[2]. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen[3]. Mancherorts wird sogar vom „Verrat durch den eigenen Pkw" gesprochen[4].

Der Einsatz dieser Technologien wirft an sich schon datenschutzrechtliche Fragen auf. Der Beschäftigtendatenschutz als bereichsspezifische Spezialmaterie gilt dabei im Allgemeinen als strengeres Datenschutzrecht[5]. Sollen also Car-to-X-Verbindungen im Unternehmensfuhrpark Verwendung finden, ist genau zu prüfen, welche Daten anfallen und was mit ihnen geschieht. Die an dieser Stelle häufig gestellte Frage, wem die Daten aus dem Fahrzeug „gehören"[6], führt für hiesige Zwecke allerdings nicht weiter. Das Datenschutzrecht greift immer dann, wenn die Daten einen Personenbezug aufweisen.

II. Datenkategorien

1. Positionsdaten

Positionsdaten fallen in diversen Fahrzeugsystemen an. Zu nennen ist zunächst das Navigationssystem, welches kontinuierlich Positionsdaten verarbeitet. Die eingegebenen Zielorte und letzten Routen bleiben in aller Regel im Gerät gespeichert. Eine Außenkonnektivität ist jedoch hierbei für gewöhnlich nicht vorgesehen[7].

Das Notrufsystem eCall überträgt dagegen die Position eines verunfallten Fahrzeuges automatisch an eine Leitstelle. Das System ist „schlafend" konzipiert, sendet also erst im Ernstfall[8].

Intelligente Kennzeichen ermöglichen es, Ein- und Ausfahrten in Parkhäusern und auf Werksgeländen zu protokollieren[9]. Zumindest mittelbar ergeben sich gefahrene Routen auch aus aggregierten Informationen öffentlicher Ladestationen für Elektroautos[10]. Hier werden die jeweilige Kunden-ID und der Standort der Ladesäule zu Abrechnungszwecken erhoben.

Im Logistikbereich kann die Verfolgung ständig aktueller Positionsdaten eine Rolle spielen, ebenso wenn Fahrzeuge einer Rufbereitschaft unterliegen. Die jeweiligen Disponenten müssen ggf. Routen, Reichweiten und etwaige Verspätungen in Echtzeit verfolgen können. Infrastrukturdienste wie Stau-[11] oder Eiswarnungen[12] sind ebenfalls auf Positionsdaten angewiesen.

Elektronische Fahrtenbücher sind schließlich ein Mittel, steuerliche Vergünstigungen für privat genutzte Dienstfahrzeuge geltend zu machen. Die zurückgelegten Strecken werden automatisch aufgezeichnet und sodann vom Mitarbeiter als dienstlich oder privat veranlasst gekennzeichnet[13].

2. Telekommunikationsdaten

Die im fahrzeugeigenen Infotainmentsystem integrierte Freisprechanlage ist unter Umständen in der Lage, Kontakt- und Verbindungsdaten zu speichern. Das Notrufsystem eCall bringt zugleich ab Werk ein Mobilfunkmodul mit und eröffnet damit den Weg zu weiteren kommunikationsgestützten Zusatzdiensten[14].

1 Vgl. Hassemer, NZV 1995, 169, 171 zum 33. Verkehrsgerichtstag 1995 in Goslar.

2 Übersicht bei Asaj, DuD 2011, 558, 559. Zu nennen sind bspw. OBD (II), GSM/UMTS, WLAN, Bluetooth, NFC, GPS u.v.m.

3 Entschließung der 88. DSK am 8./9.10.2014 („Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert"), online unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_DatenschutzImKfz.pdf.

4 Mielchen, SVR 2014, 81 ff.

5 Dies gilt, obwohl es bislang nicht zu einem eigenständigen Beschäftigtendatenschutzgesetz gekommen ist. Zu § 32g des einstigen Entwurfs Reiter/Methner, DSRITB 2014, 371, 378.

6 Grundlegend Roßnagel, SVR 2014, 281 ff.; ferner Kraus, DSRITB 2014, 381, 383 ff.; Asaj, DuD 2011, 558.

7 Treffend Rihaczek, DuD 2011, 5.

8 Grundlegend zum eCall-System Lüdemann/Sengstacken, RDV 2014, 177 ff.

9 Lüdemann/Sengstacken/Vogelpohl, ZD 2015, 55, 59.

10 Hierzu eingehend Lüdemann/Jürgens/Ortmann RDV 2014, 3 ff.

11 Asaj, DuD 2011, 558 zu sog. Floating-Car-Daten.

12 Vgl. http://www.golem.de/news/volvo-cloud-autos-warnen-sich-gegenseitig-vor-glatten-strassen-1502-112332.html.

13 Vgl. § 6 Abs. 1 Nr. 4 S. 3 EStG. Grundlegend zu elektronischen Fahrtenbüchern Rammo/Holzgräfe, DSRITB 2014, 355 ff.

14 Lüdemann/Sengstacken, RDV 2014, 177, 179.

3. Fahrverhalten

Unfalldatenspeicher führen bestimmte Sensordaten zusammen und halten sie für die Unfallauswertung als Daten-Frame in einer Black Box fest[15]. Der Einbau dieser Speicher erfolgt derzeit auf freiwilliger Basis[16].

Für einige Nutzfahrzeuge[17] sind allerdings seit 2006 digitale Tachographen vorgeschrieben, welche die Identität des Fahrers, Lenk-, Ruhe- und Arbeitszeiten, gefahrene Geschwindigkeiten nebst Geschwindigkeitsübertretungen und zurückgelegte Wegstrecken speichern. Ziel der Aufzeichnung ist der Schutz der Fahrer durch die Einhaltung von Ruhepausen und die Steigerung der Verkehrssicherheit durch Verbesserung von Kontrollmöglichkeiten der Polizei und der Gewerbeaufsicht[18].

Sogenannte „Telematiktarife" der Versicherungen gehen noch einen Schritt weiter: Überhöhte Geschwindigkeit, hastiges Bremsen oder Beschleunigen sowie Nacht- und Stadtfahrten werden an den Versicherer ausgeleitet und haben sodann unmittelbar Einfluss auf den Versicherungsbeitrag[19]. Nimmt der Arbeitgeber Zugriff auf diese Daten, wird hierdurch zugleich eine genaue Auswertung des Fahrverhaltens einzelner Mitarbeiter möglich.

4. Bild- und Videodaten

Dashcams sind kleine weitwinklige Kameras auf dem Armaturenbrett, die das Verkehrsgeschehen aufzeichnen. Die Betreiber der Kameras wollen Beweismittel für etwaige Verkehrsunfallsituationen sammeln. Im Unternehmenseinsatz würde auch hier eine Kontrolle der Beschäftigten denkbar. Der Düsseldorfer Kreis[20] und die Rechtsprechung[21] haben der Verwendung von Dashcams allerdings weitgehend eine Absage erteilt[22]. Innenkameras werden demgegenüber häufig in Taxen eingesetzt zum Schutz der Fahrer vor Übergriffen und Beförderungsbetrug. Die aufgezeichneten Daten lassen sich dabei genauso gegen den Fahrzeugführer einsetzen.

5. Fahrzeugdaten

Zu den reinen Fahrzeugdaten zählen jene Informationen, die sich zuvörderst auf die Maschine selbst beziehen. Hierzu gehören Drehzahlen, Temperaturen, Gas- und Flüssigkeitsdrücke, Wartungsintervalle und viele weitere. On-Board-Diagnose-Systeme nutzen diese Daten zur Fehlererkennung und -analyse.

III. Personenbezug

Daten sind personenbezogen im Sinne des § 3 Abs. 1 BDSG, wenn es sich um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person handelt[23]. Bei Telekommunikations-, Fahrverhaltens- oder Bilddaten ist der Personenbezug mit Händen zu greifen. Schwieriger wird es bei Positionsdaten oder reinen Fahrzeugdaten. Ein Ort alleine oder physische Eigenschaften eines Fahrzeuges haben für sich genommen noch keine direkte Beziehung zum Persönlichkeitskern eines Menschen. Der Bezug wird erst hergestellt, wenn der Arbeitgeber zuordnen kann, wer das Fahrzeug zu einem bestimmten Zeitpunkt gefahren hat. Bei hinreichender Kontrolldichte wird die betriebliche Fahrzeugnutzung nahezu lückenlos protokolliert sein. Somit werden die Bewegung im Raum, das Verhalten im Straßenverkehr, der Umgang mit Unternehmenseigentum und andere Persönlichkeitsaspekte ablesbar, und es können ggf. ganze Persönlichkeitsprofile[24] erstellt werden. Mithin muss davon ausgegangen werden, dass sämtliche im Fahrzeug anfallenden Daten auf die eine oder andere Weise Aussagekraft über eine zumindest bestimmbare Person besitzen[25].

IV. Erhebung, Speicherung und Übermittlung

So unterschiedlich die Datenkategorien sind, die in einem Fahrzeug anfallen können, so vielfältig sind auch die mit der Datenverarbeitung verfolgten Zwecke. Neben dem Arbeitgeber kann dadurch eine große Zahl weiterer Empfänger Begehrlichkeiten entwickeln. Fahrzeughersteller, Werkstätten, Behörden oder Versicherungsunternehmen vermögen die gewonnenen Informationen ggf. nutzbringend einzusetzen. Der Beschäftigtendatenschutz endet jedoch nicht an der Betriebspforte. Jede Erhebung und Speicherung durch den Arbeitgeber, jede Weitergabe an einen Dienstleister im Rahmen einer Auftragsdatenverarbeitung und jede Übermittlung an einen Dritten müssen sich gemäß der §§ 3a, 4 Abs. 1 BDSG rechtfertigen lassen. Wie die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zutreffend festgestellt hat, entsteht die besondere Gefährdungs-

15 Hierzu eingehend Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302 ff.; Brenner/Schmidt-Cotta, SVR 2008, 41 ff.

16 Die Frage der datenschutzrechtlichen Zulässigkeit einer Weiterleitung von Unfalldaten an den Haftpflichtversicherer wurde vom OLG Oldenburg, Urteil vom 23.12.2014, Az. 13 U 66/14 (https://openjur.de/u/754111.html) ausdrücklich offengelassen.

17 Lastwagen und Busse mit mehr als neun Plätzen.

18 Zum Ganzen Gola, NZA 2007, 1139, 1142 f.

19 Kinast/Kühnl, NJW 2014, 3057.

20 Beschluss vom 26./27.02.2013, „Videoüberwachung in und an Taxis"; Beschluss vom 25./26.02.2014, „Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)".

21 VG Ansbach, Urteil vom 12.08.2014, Az. AN 4 K 13.01634; AG München Beschluss vom 13.08.2014, Az. 345 C 5551/14; LG Heilbronn, Urteil vom 17.02.2015, Az. I 3 S 19/14.

22 Andere Ansicht: Atzert/Franck, RDV 2014, 136 ff.

23 Auf die Frage, ob bestimmte Fahrassistenzsysteme zur Auswertung der Augenbewegungen oder des Atemalkoholgehalts ggf. besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG verarbeiten, soll hier nicht eingegangen werden; hierzu Kremer, RDV 2014, 240, 241.

24 Asaj, DuD 2011, 558, 560; Lüdemann/Jürgens/Ortmann, RDV 2014, 3, 4; Weichert, SVR 2014, 241, 241 f. Vgl. auch die Entschließung der 88. DSK (Fn 3).

25 Kinast/Kühnl, NJW 2014, 3057, 3060; wohl auch Kremer, RDV 2014, 240, 244.

lage bereits zum Zeitpunkt des Erfassens und nicht erst mit dem Auslesen oder Übermitteln[26].

V. Datenschutzrechtliche Rechtfertigung

1. § 32 BDSG

In Ermangelung eines eigenständigen Beschäftigtendatenschutzgesetzes bleibt § 32 BDSG die Kernvorschrift für alle Fragen hinsichtlich Arbeitnehmerdaten. Solche dürfen grundsätzlich für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. In Connected Car-Szenarien wird des Öfteren auf § 32 BDSG rekurriert[27]. Die Einführung elektronischer Fahrtenbücher lässt sich dabei ohne größere Schwierigkeiten auf § 32 Abs. 1 S. 1 BDSG stützen[28]. Auch für die unmittelbare Optimierung des Fuhrparkeinsatzes oder (irrig) das Wiederauffinden gestohlener Fahrzeuge wird dies in der Literatur vertreten[29]. Allen Darstellungen ist unterdessen gemein, dass eine vollständige Überwachung oder Kontrolle der Beschäftigten als unzulässig anzusehen ist[30]. Hauptaugenmerk bei der Bewertung liegt insoweit bei der tatbestandlichen Erforderlichkeit. Die Datenverarbeitung ist erforderlich, soweit sie zur Erreichung eines konkret festgelegten Zweckes geboten ist. Die Erforderlichkeit ist weitgehend identisch mit der verfassungsrechtlichen Verhältnismäßigkeitsprüfung, bestehend aus legitimem Zweck, Geeignetheit zur Zweckerfüllung, mildestem gleichgeeignetem Mittel und der Verhältnismäßigkeit im engeren Sinne[31]. Die Zweckbestimmung wird dabei bereits durch § 32 Abs. 1 S. 1 BDSG vorgegeben.

Ergeben sich Anhaltspunkte für eine Straftat im Beschäftigungsverhältnis, die mit oder am Dienstfahrzeug begangen wurden, darf der Arbeitgeber nach Maßgabe des § 32 Abs. 1 S. 2 BDSG Daten des Connected Car erheben und verarbeiten.

2. § 28 BDSG

Ob neben der Spezialnorm des § 32 BDSG noch Teile des § 28 BDSG anwendbar sind, ist bis heute trefflich umstritten. Die herrschende Meinung geht davon aus, dass allein § 28 Abs. 1 S. 1 Nr. 1 BDSG völlig verdrängt werde[32]. Für andere Zwecke, die nicht unmittelbar Zwecke des Beschäftigungsverhältnisses sind, bleibt ein Anwendungsbereich für § 28 Abs. 1 S. 1 Nrn. 2 und 3 BDSG.

Der Abschluss von Telematiktarifen etwa und die Übermittlung der dadurch anfallenden Daten an den jeweiligen Versicherer kann nach § 28 Abs. 1 S. 1 Nr. 2 BDSG gerechtfertigt sein, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Das Gleiche gilt für den Einbau von Unfalldatenspeichern und die Ausleitung fahrzeugspezifischer Daten an Werkstätten.

3. Betriebsvereinbarung

Betriebsvereinbarungen gelten als Rechtsvorschriften im Sinne des § 4 Abs. 1 BDSG i.V.m. § 77 Abs. 4 S. 1 BetrVG und stellen damit vollwertige datenschutzrechtliche Erlaubnistatbestände dar. Auch eventuelle Probleme der AGB-Inhaltskontrolle werden hierdurch abgemildert (§ 310 IV BGB). Die Einführung von Connected Car-Konzepten kann folglich durch eine Betriebsvereinbarung geregelt werden[33]. Um einen datenschutzrechtlichen Freibrief handelt es sich gleichwohl nicht: Das Privatleben ist der Regelungsmacht der Betriebsvereinbarung entzogen. Gemäß § 75 Abs. 2 S. 1 BetrVG haben Arbeitgeber und Betriebsrat zudem die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Der gläserne Autofahrer wird also auch durch eine Betriebsvereinbarung nicht ermöglicht.

4. Einwilligung

Die datenschutzrechtliche Einwilligung bietet in Zweifelsfällen eine elegante Nachweismöglichkeit für die verantwortliche Stelle und lässt Datenverarbeitungen zu, die ansonsten nicht zu rechtfertigen wären. Nach zutreffender Ansicht erfasst sie zugleich Umfang und Reichweite technisch-organisatorischer Maßnahmen[34].

Gemäß § 4a Abs. 1 S. 1-3 BDSG muss die Einwilligung informiert, freiwillig und grds. in schriftlicher Form erfolgen. An der Freiwilligkeit kann es indes in Fällen wirtschaftlicher Abhängigkeit, wie insbesondere in Arbeitsverhältnissen, hapern[35]. Daher ist genau darauf zu achten, ob eine rein einseitige Durchsetzung von Arbeitgeberinteressen be-

26 88. DSK (Fn 3).

27 Kremer, RDV 2014, 240, 251; Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 304; Rammo/Holzgräfe, DSRITB 2014, 355.

28 Rammo/Holzgräfe, DSRITB 2014, 355, 360

29 Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 304. Das Wiederauffinden gestohlener Fahrzeuge dürfte ein Zweck sein, der außerhalb des eigentlichen Beschäftigungsverhältnisses liegt, und insoweit eher § 28 Abs. 1 S. 1 Nr. 2 BDSG unterfallen, so auch Rammo/Holzgräfe, DSRITB 2014, 355, 360.

30 Kinast/Kühnl, NJW 2014, 3057, 3059 f.; Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302, 304; Rammo/Holzgräfe, DSRITB 2014, 355, 359; Wedde, in: http://www.eurotransport.de/news/flottenmanagement-systeme-immer-im-visier-des-chefs-537682.html. Mit identischer Stoßrichtung BGH, Urt. v. 04.06.2013, Az. 1 StR 32/13 (https://openjur.de/u/634193.html) zu GPS-Trackern sowie BAG, Urt. v. 19.02.2015, Az.: 8 AZR 1007/13 (http://dejure.org/2015,2096) zur Observation von Arbeitnehmern.

31 Wolff, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, Syst. A, Rn. 26 f.

32 Riesenhuber, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 32 BDSG Rn. 26 ff.; Gola/Jaspers, RDV 2009, 212 ff. Konkret zu Connected Car-Szenarien ebenso Kremer, RDV 2014, 240, 251; Rammo/Holzgräfe, DSRITB 2014, 355, 360.

33 Wesentliche Regelungsinhalte finden sich bei Gola/Wronka, Handbuch Arbeitnehmerdatenschutz, 6. Aufl. 2013, Rn. 1929.

34 VG Berlin, Urt. v. 24.05.2011, 1 K 133/10 (http://openjur.de/u/284643.html).

35 Weichert, SVR 2014, 241, 243; Simitis, in: Simitis, BDSG, 8. Aufl. 2014, § 4a Rn. 62; Kühling, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 4a Rn. 35.

absichtigt ist[36], und ob dem Arbeitnehmer eine zumutbare Handlungsalternative bleibt.

Im Allgemeinen wird davon ausgegangen, dass eine wirksame Einwilligung in Connected Car-Konzepte durchaus möglich ist[37]. Zweifelhaft ist jedoch, welche praktische Relevanz die Einwilligung für Connected Car-Systeme besitzt, wenn die maßgeblichen Verwendungen bereits durch gesetzliche Erlaubnistatbestände oder Betriebsvereinbarungen gedeckt sind. Die Transparenzpflichten erhalten insofern größeres Gewicht.

VI. Transparenzpflichten

Bereits bei der Datenerhebung hat die verantwortliche Stelle gemäß § 4 Abs. 3 BDSG über den Umfang der Datenverarbeitung zu informieren. Für jene Informationspflicht kommt es darauf an, ob der Arbeitgeber selbst Daten mittels eines Connected Car erhebt. Jedenfalls wird man aus der arbeitgeberseitigen Fürsorgepflicht ableiten können, dass der Dienstwagennutzer bei Übergabe des Fahrzeugs über die Datenerhebung durch Dritte (z.B. Werkstätten oder Versicherer) und die Daten, die bei der Fahrzeugbenutzung anfallen, hinzuweisen ist.

Werden personenbezogene Daten anderweitig erstmals für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist dieser gem. § 33 Abs. 1 S. 1 BDSG zu informieren.

VII. Betriebliche Mitbestimmung

§ 87 BetrVG regelt Mitbestimmungsrechte des Betriebsrates. Hinsichtlich Connected Car-Vorhaben fällt vor allem Abs. 1 Nr. 6 ins Auge, der die Einführung und Anwendung von technischen Einrichtungen erfasst, „die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“. Entgegen dem missverständlichen Wortlaut der Nr. 6 („dazu bestimmt“) greift das Mitbestimmungsrecht bereits dann ein, wenn die Maßnahme lediglich zur Überwachung geeignet ist. Eine gezielte Zweckbestimmung durch den Arbeitgeber ist hingegen nicht erforderlich[38]. Sämtliche im Fahrzeug anfallenden Daten sind schlechthin geeignet, eine Verhaltens- und ggf. auch Leistungskontrolle durchzuführen.

Bestimmungen, die den Umgang mit den Fahrzeugen selbst betreffen, können darüber hinaus Rechte nach § 87 Abs. 1 Nrn. 1 (Ordnung und Verhalten) oder 2 (Arbeitszeiten) BetrVG auslösen. Die Gewährung eines Dienstwagens unterliegt der Mitbestimmung nach § 87 Abs. 1 Nr. 10 BetrVG, gleichwohl handelt es sich hierbei im Kern nicht um eine datenschutzrechtliche Norm.

Verletzt unterdessen der Arbeitgeber die im Gesetz niedergelegten Mitbestimmungsrechte in grober Weise, kann der Betriebsrat ggf. nach § 23 Abs. 3 S. 1 BetrVG die Verwendung von Connected Car-Konzepten arbeitsgerichtlich untersagen lassen.

VIII. Widerspruchsrecht

§ 35 Abs. 5 BDSG gewährt dem Betroffenen ein Widerspruchsrecht gegen die automatisierte Verarbeitung seiner Daten oder Verarbeitung in nicht automatisierten Dateien. Dies gilt jedoch nur, sofern das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt.

Hier fließen Aspekte ein, die der verantwortlichen Stelle im Rahmen der Erforderlichkeitsprüfung des § 32 Abs. 1 S. 1 BDSG oder der Interessenabwägung des § 28 Abs. 1 S. 1 Nr. 2 BDSG noch unbekannt waren. Den Betroffenen trifft insoweit eine Initiativverantwortung, entgegenstehende Gesichtspunkte geltend zu machen. Beispielhaft können dies etwa Fälle sein, in denen der genaue Aufenthaltsort eines Betroffenen aus Sicherheitsgründen geheimzuhalten ist[39]. Eine schematische Lösung, welche Beschäftigteninteressen beim Einsatz von Connected Cars höher zu gewichten sind, als diejenigen des Arbeitgebers, kann an dieser Stelle freilich nicht angeboten werden.

IX. Praxisbeispiel 1: Auswertung von Fahrverhaltensdaten

Sowohl bei rein dienstlicher als auch bei gestatteter Privatnutzung eines Dienstfahrzeuges hat der Arbeitnehmer eine Sorgfaltspflicht beim Umgang mit Unternehmenseigentum zu beachten. Durch die Einführung eines Telematiktarifes oder die Rückmeldung durch die Werkstatt könnte der Arbeitgeber nun in den Besitz von Daten zum Fahrverhalten gelangen. Zeigt sich dabei ein unsachgemäßer Gebrauch des unternehmenseigenen Fahrzeuges, hat der Arbeitgeber ein Interesse daran, diese Daten zur Begründung etwaiger Regressforderungen heranzuziehen.

Bei rein dienstlicher Nutzung lässt sich ein solches Vorhaben ggf. auf § 32 BDSG stützen. Dies gilt jedenfalls dann, wenn die Fahrzeugnutzung eng mit dem übrigen Pflichtenkreis des Arbeitnehmers verknüpft ist, wie dies bei Berufskraftfahrern, Kurieren etc. der Fall ist. Um eine unzulässige Ausforschung des Beschäftigten handelt es sich nicht, da der Arbeitgeber nicht anlasslos handelt.

Nun ist die Überlegung gestattet, inwiefern die Grundsätze der gestuften Arbeitnehmerhaftung[40] bereits auf der Ebene der Tatbestandsermittlung anzuwenden sind. Richtigerweise wird man davon ausgehen müssen, dass es sich hierbei maßgeblich um eine Problemstellung auf Rechtsfol-

36 Kinast/Kühnl, NJW 2014, 3057, 3059 f.

37 Rammo/Holzgräfe, DSRITB 2014, 355, 359; Kinast/Kühnl, NJW 2014, 3057, 3060.

38 Vgl. bereits Franck, RDV 2013, 185, 188 zum Themenfeld BYOD.

39 Brink, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 35 BDSG Rn. 76 zu Gefahren für Leib und Leben.

40 Volle Haftung nur bei Vorsatz oder grober Fahrlässigkeit, ansonsten anteilige bis gar keine Haftung des Arbeitnehmers, vgl. BAG, Beschl. v. 27.09.1994, Az.: GS 1/89 (http://dejure.org/1994,77).

genseite handelt. Die Daten dürfen daher verarbeitet werden, bis geklärt ist, ob das Fahrverhalten tatsächlich auf Vorsatz oder grobe Fahrlässigkeit hindeutet.

Bei gestatteter Privatnutzung verlässt die Datenverarbeitung den Boden des Beschäftigtenverhältnisses. Informationsbeschaffungen über Privatfahrten sind für den Arbeitgeber grundsätzlich unzulässig. Ergeben sich jedoch Anhaltspunkte für eine sorgfaltswidrige Privatnutzung und eine damit einhergehende Beschädigung am Fahrzeug, wird der Arbeitgeber anhand eigener oder ihm übermittelter Daten über das Fahrzeug auf Grundlage des Nutzungsvertrages gemäß § 28 Abs. 1 S. 1 Nr. 1 BDSG vertragliche (Regress-)Ansprüche prüfen dürfen.

X. Praxisbeispiel 2: GPS-Tracking

Die Ortung mobiler Beschäftigter kann wegen arbeitsvertraglicher Kontrollrechte oder einer direktionsrechtlichen Ordnungsbefugnis gerechtfertigt sein. Sämtliche Maßnahmen, die der Durchführung des Beschäftigungsverhältnisses dienen, müssen jedoch einer Erforderlichkeitsprüfung im Sinne des § 32 Abs. 1 S. 1 BDSG standhalten. Die Erforderlichkeit ist stets nur dann gegeben, wenn kein milderes, weniger in die Persönlichkeitsrechte eingreifendes Mittel zur Verfügung steht. GPS-Tracking zur reinen Arbeitszeitkontrolle dürfte unverhältnismäßig sein, wenn bspw. die Auswertung reiner Kilometerstände genügt. Die Optimierung des Personaleinsatzes insgesamt, Diebstahlschutz und die persönliche Sicherheit der Mitarbeiter sind hingegen legitime Ziele einer solchen Datenerhebung und -verarbeitung. Vorab zu prüfen bleibt, ob ein vollständiges Tracking aufgezeichnet werden muss, oder ob nur die jeweils letzte Position für die Zweckerreichung genügt. Die Überwachung muss dabei – außer in Fällen konkreten Strafverdachts – transparent gemacht werden[41].

XI. Zusammenfassung

Die Einführung neuer Technik im Fahrzeug stellt den Datenschutz zweifelsohne vor neue Herausforderungen. Neuartig sind jedoch keineswegs die anfallenden Datenkategorien oder die betrieblichen Verarbeitungszwecke, sondern die schiere Masse an gebündelter Information, die durch Connected Car-Systeme zur Verfügung steht. Die geltenden Datenschutzbestimmungen, seien es Befugnisnormen, Betroffenenrechte oder Vorschriften zur betrieblichen Mitbestimmung, werden mit diesen Herausforderungen fertig[42]. Den Unternehmen, die am technischen Segen partizipieren wollen, müssen jedoch die Grundsätze der Datensparsamkeit[43], der Zweckbindung und der Transparenz[44] klar vor Augen stehen. Sowohl die betriebliche Datenschutzkontrolle als auch die Mitarbeitervertretung müssen im Vorhinein wissen, was von Seiten der Autoindustrie auf sie zukommt, um in angemessener Weise die Rechte der Beschäftigten schützen zu können.

RA Andreas Jaspers
RA Andreas Jaspers ist Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. und Mitherausgeber der RDV.

Dr. iur. Lorenz Franck
Dr. iur. Lorenz Franck ist Referent für Beschäftigten-, Sozial- und Gesundheitsdatenschutz bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. sowie Lehrbeauftragter für Datenschutzrecht an der FH Köln.

41 Zum Ganzen Gola, RDV 2012, 285 ff., insbesondere zur Praxis der Aufsichtsbehörden.

42 A.A. Fischer, Flottenmanagement 1/2015, 52 ff.; ferner Weichert, SVR 2014, 241, 247, der jedoch ausdrücklich die Notwendigkeit eines eigenständigen „Autofahrerdatenschutzgesetzes" verneint.

43 Grundlegend Weichert, SVR 2014, 201, 205 f., insbesondere zu „privacy by design".

44 Hierzu Weichert, SVR 2014, 241, 242 f.