

■ Big Data im Fahrzeug

Rechtliche Überlegungen zur Kfz-Datenweitergabe

von Dr. Daniela Mielchen*

Grundsätzlich ist die für 2015 geplante serienmäßige Ausstattung von Neuwagen mit E-Call-Einrichtungen zu begrüßen – zumindest soweit sie eine Notruf-Funktion erfüllen. Skeptisch sollte jedoch den zunehmend realisierbaren Mehrwertdiensten entgegen getreten werden. Insb. bei unzureichender Aufklärung über die Tragweite der Datenweitergabe droht nicht nur eine Verletzung der informationellen Selbstbestimmung. Ebenso ist der verfassungsrechtlich garantierte „nemo tenetur“-Grundsatz in Gefahr, sollten z.B. die Strafverfolgungsbehörden Zugriff auf die vom eigenen Fahrzeug gespeicherten Daten haben. Ferner kann es bei Feststellung eines unangepassten Verkehrsverhaltens zu Nachteilen mit Versicherungen kommen.

1. Ausgangssituation

Fahrzeughersteller unternehmen derzeit alles, um ihre Produkte zu fahrenden Smartphones umzurüsten. Neben Informationstechnologien werden zukünftig auch die bis zu 70 datensammelnden Steuerungsgeräte im Fahrzeug und die ab 2015 in jedem Neuwagen zu verbauende E-Call-Einrichtung, welche bei einem Unfall einen Notruf absetzen soll, den Fahrer gläsern machen. So ist es ohne weiteres denkbar und in moderatem Maße jetzt schon Realität, dass die Polizei Daten des Fahrzeugs auswertet, um den Fahrer einer Ordnungswidrigkeit oder Straftat zu überführen.

2. Staatlicher Datenzugriff

Darf der Staat auf alle Daten zugreifen, die er bekommen kann oder gibt es Grenzen? So ist auf das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1, Art. 1 Abs. 1 GG zu verweisen, wonach die Befugnis des Einzelnen gewährleistet sein soll, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Ist dieses Recht nicht erheblich eingeschränkt, wenn der Staat den Verkehrsteilnehmern eine verbindliche Pflicht auferlegt, das nicht ausschaltbare E-Call-System mit der Folge zu nutzen, dass Daten über ihn oder das Fahrzeug gesendet und gespeichert werden? Ebenso werden strafrechtliche Schutzrechte ausgehöhlt, wenn der Staat Zugriff auf all die über seine Bürger durch deren Fahrzeuge erhobenen Daten hat. Ein Aussageverweigerungsrecht läuft faktisch leer, wenn die Verfolgungsbehörden problemlos an die über den jeweiligen Fahrzeugführer erhobenen Daten gelangen.

Zwar werden seit jeher Zwangsmaßnahmen zur Erlangung und Sicherung von Beweisen in Form von Sicherstellung und Beschlagnahme gem. §§ 94 ff. StPO durchgeführt, doch darf dies nur unter bestimmten Voraussetzungen geschehen. Denn die Sicherstellung/Beschlagnahme stellt immer einen Eingriff in Grundrechte des Betroffenen dar.

Die Anordnung hat daher, wie alle Zwangsmaßnahmen im Strafverfahren, dem Grundsatz der Verhältnismäßigkeit zu genügen. Dieser Grundsatz verlangt, dass die Maßnahme zur Erreichung des angestrebten Ziels geeignet und erforderlich sein muss und dass der mit ihr verbundene Eingriff nicht außer Verhältnis zur Bedeutung der Sache und zur Stärke des bestehenden Tatverdachts stehen darf. Darüber hinaus muss er für die Ermittlungen notwendig sein. Letztlich ist erforderlich, dass der Tatverdacht eine Tatsachengrundlage hat, aus der sich die Möglichkeit der Tatbegehung durch den Beschuldigten ergibt. Eine bloße Vermutung reicht grundsätzlich nicht aus. So wird in der Praxis bei einem Anfangsverdacht auf die Begehung erheblicher Straftaten der Eingriff in die Grundrechte des Beschuldigten durchaus als verhältnismäßig angesehen, so dass eine Beschlagnahme und Verwertung von Daten grundsätzlich stattfinden darf. Anders sollte es jedoch aussehen, wenn lediglich leichte Vergehen oder Ordnungswidrigkeiten im Raum stehen.

Bedenkt man, dass zum einen demnächst durch E-Call, Telematiksysteme etc. eine Vielzahl an leicht abrufbaren Daten verfügbar sein wird und dass zum anderen bei jedem Unfall ein gewisser Anfangsverdacht besteht (zumindest einer der Beteiligten dürfte den Unfall verschuldet haben) ist zu befürchten, dass ein Datenabruf durch Sicherstellung/Beschlagnahme zukünftig möglicherweise routinemäßig und flächendeckend bei jedem Unfall durchgeführt wird. Verschärfend kommt hinzu, dass mehrheitlich nicht einmal ein Durchsuchungsbeschluss notwendig sein wird. Denn während der entsprechende Richtervorbehalt hier dem Schutz der Grundrechte dienen soll, ist dieser entbehrlich, wenn die eingreifenden Beamten von Gefahr im Verzug ausgehen dürfen. Diese Annahme wird bei den vielfach flüchtigen, semifesten oder löschbaren Daten regelmäßig berechtigt vorliegen, so dass die Entscheidung über die Verhältnismäßigkeit des Eingriffs überproportional häufig bei den Polizeibeamten liegen wird. Dies gilt besonders dort, wo kein richterlicher Notdienst erreichbar ist. Der Aufwand, der zur Erlangung der Daten investiert werden müsste, wäre zudem deutlich geringer als bei bisherigen Ermittlungsmethoden, wenn es zentrale Anlaufstellen gibt, an denen die Daten verfügbar sind, was diese Ermittlungsmöglichkeit für die Verfolgungsbehörden zusätzlich attraktiv macht.

3. Datenzugriff durch Private

Doch nicht nur bei staatlichen Eingriffen, sondern auch im privatrechtlichen Bereich (z.B. Versicherer/Versicherter, Hersteller/Käufer, Leasinggeber/Leasingnehmer) sind negative datenschutzrechtliche Fiktionen denkbar.

* RAin, FAin VerkehrsR Dr. Daniela Mielchen, Hamburg.

4. Ausblick

Nicht ohne weiteres sind schon jetzt Forderungen an Datensicherheit formulierbar, da die IT-Entwicklung und Vernetzung rasant voranschreitet. Allerdings fällt es

leicht, sich den Forderungen des diesjährigen Verkehrsgerichtstags in Goslar anzuschließen, der weitreichende Aufklärung und Grenzziehung anmahnt.