ARTIKEL-29-DATENSCHUTZGRUPPE

17/DE

WP 252

Stellungnahme 03/2017 zur Verarbeitung personenbezogener Daten im Kontext Kooperativer, Intelligenter Verkehrssysteme (C-ITS)

Angenommen am 4. Oktober 2017

Inhaltsverzeichnis

Diese Arbeitsgruppe wurde nach Artikel 29 der Richtlinie 95/46/EG eingesetzt. Die Gruppe ist ein unabhängiges europäisches Beratungsgremium für Datenschutz und den Schutz der Privatsphäre. Ihre Aufgaben werden in Artikel 30 der Richtlinie 95/46/EG und Artikel 15 der Richtlinie 2002/58/EG beschrieben.

Die Sekretariatsgeschäfte werden von der Europäischen Kommission, Generaldirektion Justiz, Direktion C (Grundrechte und Unionsbürgerschaft), 1049 Brüssel, BELGIEN, Büro MO-59 03/075 geführt.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Inhaltsverzeichnis

1 Einleitung 3
2 Das C-ITS-Konzept 3
3 Zusammenfassung der Arbeitsunterlage zum C-ITS 4
3.1 Personenbezogene Daten 4
3.2 Rechtsgrundlagen 5
4. Stellungnahme der Artikel-29-Arbeitsgruppe 6
4.1 Der Rechtsrahmen 6
4.2 Personenbezogene Daten / Identifizierung betroffener Personen 7
4.3 Risiken für die Privatsphäre 9
4.4 Rechtmäßigkeit der Verarbeitung 10
4.5 Sicherheit 14
5 Erforderliche Maßnahmen 16

1 Einleitung

Die von der Arbeitsgruppe für Datenschutz und Schutz der Privatsphäre der Plattform für Kooperative, Intelligente Verkehrssysteme (C-ITS) ausgearbeitete Unterlage „Processing personal data in the context of C-ITS“ über die Verarbeitung personenbezogener Daten im Kontext von C-ITS wurde der Artikel-29-Arbeitsgruppe am 10. Juli 2017 offiziell vorgelegt.

Bei der Plattform C-ITS handelt es sich um eine Initiative der Direktion für Verkehr und Mobilität der Europäischen Kommission, die Ende 2014 ihre Arbeit mit der Einrichtung spezialisierter Arbeitsgruppen aufnahm, wobei sich jede dieser Arbeitsgruppen mit unterschiedlichen Aspekten des Einsatzes von C-ITS, angefangen bei der Sicherheit über technische Normung bis hin zum Datenschutz, befasst.

Der Zweck dieser Unterlage besteht darin, Hintergrundinformationen über die Verarbeitung personenbezogener Daten im Kontext von C-ITS bereitzustellen und die Artikel-29-Arbeitsgruppe um Orientierungshilfen hinsichtlich der Erhöhung des Datenschutzniveaus bei diesen neuen Anwendungsarten zu ersuchen.

Vor der Abgabe der vorliegenden Stellungnahme wurde die Artikel-29-Arbeitsgruppe von der Kommission eingeladen, mit ihren Delegierten an einer Reihe von Vorbereitungstreffen teilzunehmen.

Die Artikel-29-Arbeitsgruppe freut sich, dass sie sich seit den ersten Anfängen dieser neuen technologischen Idee an der Diskussion mit maßgeblichen Interessengruppen beteiligen kann, und wird dementsprechend eine Reihe von Bedenken bezüglich der Datenschutz-Grundverordnung äußern, die dann, wenn die C-ITS-Lösung zum praktischen Einsatz kommt, den Rechtsrahmen bilden wird.

Die Artikel-29-Arbeitsgruppe begrüßt die von der ICDPPC auf ihrer Konferenz in Hongkong am 25.-29. September 2017 verabschiedete Entschließung zum Datenschutz in automatischen, vernetzten Fahrzeugen und bekräftigt die dort aufgeführten Anforderungen.

2 Das C-ITS-Konzept

C-ITS ist eine „Peer-to-Peer“-Lösung (d. h. zwischen gleichrangigen Partnern) für einen ohne Eingreifen eines Netzbetreibers erfolgenden Datenaustausch zwischen Fahrzeugen und anderen Einrichtungen der Verkehrsinfrastruktur (Verkehrszeichen oder anderen sendenden/empfangenden Basisstationen).

Die Grundidee des Systems besteht darin, dass die gleichrangigen Partner einander direkt über ihren eigenen Status informieren (wobei sie die von den Sensoren, mit denen sie ausgestattet sind, erfassten Daten aufbereiten) und im Gegenzug ähnliche Informationen empfangen können, sodass (jeder Partner) die Möglichkeit bekommt, einen Überblick über den Status des Umfeldes um das Fahrzeug oder die Infrastruktureinrichtung zu erstellen. Man erwartet, dass auf der Grundlage dieser Kommunikationen die jeweilige Verkehrslage genauer vorhersagbar wird und die Unfallverhütung verbessert werden kann.

C-ITS basiert auf ununterbrochener Funkübertragung. C-ITS erzeugt ad hoc erfolgende Mitteilungen; die Einrichtung einer ständigen Kommunikation oder der Aufbau von Verbindungen zwischen den Partnern ist nicht erforderlich.

Im Kontext des C-ITS werden zwei Arten von Meldungen ausgetauscht: einmal die sogenannten Cooperative Awareness Messages (CAM), kooperative Aufklärungsmeldungen, die fortlaufend gesendet werden und kinematische Daten sowie die Maße des Fahrzeugs enthalten, und zum zweiten die Decentralised Environmental Notification Messages (DENM) (dezentrale Umfeldbenachrichtigungen), die nur beim Eintritt besonderer Ereignisse (wie Unfällen) zusätzlich zu den CAM-Meldungen bei dringen Notlagen gesendet werden und Ortsangaben zu dem betreffenden Ereignis enthalten.
CAM- und DENM-Meldungen enthalten kryptografische Signaturen, die dem Empfänger garantieren, dass die Meldungen von einem vertrauenswürdigen Absender ausgesandt werden. Die Verteilung der Zertifikate unter den Partnern erfolgt mittels einer Public Key Infrastructure (PKI), einer Architektur öffentlicher Schlüssel. Bei der PKI handelt es sich um eine Leitungs- und Regelungsstruktur, bei der jedes Zertifikat zu einem bestimmten Zeitpunkt nur einem einzigen Fahrzeug zugeordnet ist. Das Zertifikat zeigt, dass es vom System erkannt wird und vertrauenswürdig ist.

Die Europäische Kommission hat in ihrer C-ITS-Strategie bereits eine Reihe von Anwendungsfällen für den erstmaligen Einsatz (Anwendungen für Tag eins) ermittelt. Diese, in der Unterlage der C-ITS Arbeitsgruppe für Datenschutz und Schutz der Privatsphäre im einzelnen dargelegten Anwendungsfälle beziehen sich zum größten Teil auf Informationsfunktionen (wie Warnungen vor Baustellen, Witterungsbedingungen usw.). In diesen Anwendungsfällen behält der Fahrer die volle Kontrolle über das Fahrzeug und haftet für Manöver des Fahrzeugs. Langfristig wird mit zunehmendem Automatisierungsniveau der Einfluss des C-ITS steigen, da das System schrittweise Entscheidungsfunktionen des Fahrers übernehmen könnte.

Die Artikel-29-Arbeitsgruppe wird sich ausschließlich auf diese anfänglichen Einsatzmöglichkeiten von C-ITS-Anwendungen konzentrieren. Werden höhere Ebenen der Automation eingeführt, ergeben sich neue, hoch relevante Fragen bezüglich der Folgen für die Freiheit und die Rechte der EU-Bürgerinnen und -Bürger. Die Artikel-29-Arbeitsgruppe und zu gegebener Zeit auch der europäische Datenschutzausschuss werden diese Fragestellungen zu einem späteren Zeitpunkt prüfen. Die Artikel-29-Arbeitsgruppe ergreift die Gelegenheit, zu einem zeitnahen Dialog zwischen den maßgeblichen Interessgruppen zu ermutigen, in dem die datenschutzrechtlichen Implikationen dieser Entwickelungsszenarien erörtert und darüber hinaus die schwierigen ethischen Fragen erwogen werden sollten, die durch einen solchen neuen, tiefen Eingriff in traditionell von Menschen geführte Handlungen entstehen.

3 Zusammenfassung der Arbeitsunterlage zum C-ITS

3.1 Personenbezogene Daten

Die Arbeitsgruppe für Datenschutz und Schutz der Privatsphäre der kooperativen, intelligenten Verkehrssysteme erkennt an, dass die von den Fahrzeugen ausgetauschten, per Funk gesendeten Meldungen personenbezogene Daten sind. Diese Schlussfolgerung gründet im Wesentlichen auf zwei Beobachtungen: 1) Die Meldungen enthalten von der PKI ausgestellte, eindeutig dem Sender zugeordnete Berechtigungszertifikate; 2) die Meldungen enthalten eine Kopfzeile, einen Zeitstempel, Standortdaten und die Maße des Fahrzeugs.

In der Arbeitsunterlage wird der Mechanismus zum Austausch von CAM- und DENM-Meldungen mit ihren jeweiligen digitalen Zertifikaten als Verarbeitung pseudonymisierter

Daten eingestuft; dabei wird das Argument angeführt, dass zusätzliche Informationen (die Zuordnung zwischen dem Inhaber des Zertifikats und den Fahrzeugdaten) dem Datennutzer nicht zugänglich sind (diese Informationen werden von den Zertifizierungsbehörden aufbewahrt). Nach Artikel 4 Absatz 5 der Datenschutz-Grundverordnung würde man zur Identifizierung der betroffenen Personen (Dateninhaber) folglich zusätzliche Informationen benötigen. Aus diesem Grund wird in der Unterlage ausgesagt, dass Artikel 11 der Datenschutz-Grundverordnung (Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist) gelten müsse. Die Arbeitsunterlage befasst sich jedoch nicht mit der von den Zertifizierungsbehörden durchgeführten Verarbeitung und nennt keine technischen Einzelheiten zur PKI-Infrastruktur mit ihrer kritischen Bedeutung für die Gewährleistung dessen, dass die ausgetauschten Daten praktisch pseudonymisiert sind.

3.2 Rechtsgrundlagen

Die Arbeitsgruppe für Datenschutz und Schutz der Privatsphäre der C-ITS-Plattform gelangt unter Berücksichtigung der zeitlichen Abstimmung und im Hinblick auf den Einsatz der neuen Technologie im Jahr 2019 zu dem Schluss, dass sich die Rechtmäßigkeit der Verarbeitung nicht auf eine einzige, sondern auf eine Kombination aus zwei oder mehr Rechtsgrundlagen stützen könnte. Zusammenfassend ist die C-ITS-Arbeitsgruppe der Auffassung, dass die möglicherweise geeigneten Rechtsgrundlagen oder Kombination dieser Rechtsgrundlagen unter Berücksichtigung der vorgesehenen Anwendungen für „Tag eins“ folgende sein könnten:

- Öffentliche Interessen (Artikel 6 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung)
- Erfüllung eines Vertrags (Artikel 6 Absatz 1 Buchstabe b der Datenschutz-Grundverordnung)
- Einwilligung (Artikel 6 Absatz 1 Buchstabe a der Datenschutz-Grundverordnung)
- Berechtigtes Interesse (Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung)

Die C-ITS-Arbeitsgruppe merkt an, dass für die Geltendmachung eines öffentlichen Interesses als Rechtsgrund die Notwendigkeit dieser Verarbeitung in einem nationalen Gesetz oder einem EU-Gesetz festgeschrieben werden muss. Dies könnte man im Rahmen der Umsetzung der EU-Strategie für Verkehrssicherheit, Verkehrseffizienz und ökologische Nachhaltigkeit vorsehen. Mit der ITS-Richtlinie 2010/40/EU wird die Europäische Kommission ermächtigt, über delegierte Rechtsakte verbindliche Spezifikationen auf diesem Gebiet zu erlassen. Die C-ITS-Arbeitsgruppe betrachtet den zwingend vorgeschriebenen Einsatz von C-ITS als Option, allerdings nicht für den erstmaligen Einsatz im Jahr 2019.

Die C-ITS-Arbeitsgruppe erwog auch die Option der Verarbeitung personenbezogener Daten, wenn dies zur Erfüllung eines Vertrags, bei dem die betroffene Person Vertragspartei ist, erforderlich ist. Nach den Schlussfolgerungen, zu denen die C-ITS-Arbeitsgruppe gelangte, ist diese Rechtsgrundlage unter Umständen nicht allgemein anwendbar. In bestimmten Szenarien, wenn beispielsweise die betroffene Partei tatsächlich einen Vertrag mit einem privaten Straßenbetreiber geschlossen hat, um die betreffende Straße nutzen zu können, könnte man sich auf diesen Rechtsgrund stützen. Die C-ITS-Arbeitsgruppe stellt fest, dass am C-ITS-Rahmen eine Kette von Akteuren beteiligt ist (Kfz-Hersteller, Softwareentwickler, Straßennetzmanager). Sie können gemeinsam Verantwortliche laut Definition in Artikel 26

der Datenschutz-Grundverordnung sein. Um sich auf die Rechtsgrundlage der Notwendigkeit der Erfüllung eines Vertrags stützen zu können, ist eine Beurteilung der Funktionen der verschiedenen Stellen im Hinblick auf die Zwecke und Mittel erforderlich.

Hinsichtlich des Rechtsgrunds der Einwilligung äußert sich die C-ITS-Arbeitsgruppe ausführlich über die technischen Zwänge, die davon ausgehen, dass die Kommunikation durch Funkübertragungseigenschaften gekennzeichnet ist. Im Kontext des C-ITS verfügen die Akteure, die die Funktionen von Datenverantwortlichen erfüllen, eventuell über keine eins-zu-eins-Beziehung zur betroffenen Person. Die betroffene Person kennt nicht alle Empfänger ihrer Meldungen und kann sie in Anbetracht der Art und Weise, wie die Norm gedacht ist, auch nicht kennen.[1] Die C-ITS-Arbeitsgruppe schlägt jedoch die Möglichkeit vor, die gesendeten CAM- und DENM-Meldungen mit Markern zu versehen, in denen Nutzerpräferenzen verschlüsselt werden können.

Die C-ITS-Arbeitsgruppe zog auch die Verarbeitung zum Zweck der vom Verantwortlichen verfolgten, berechtigten Interessen in Betracht. Um sich auf diesen Rechtsgrund stützen zu können, muss der Datenverantwortliche sicherstellen, dass die Verarbeitung nicht den Interessen bzw. Grundrechten und Grundfreiheiten der betroffenen Person zuwiderläuft. Wie in der Unterlage ausdrücklich anerkannt wird, stehen der Anwendbarkeit dieser Rechtsgrundlage zahlreiche Hemmnisse im Wege. In erster Linie betrifft dies das Erfordernis, festzustellen, wessen Interessen in der Verantwortungskette des C-ITS verfolgt werden, sowie die Notwendigkeit, für jeden beteiligten Akteur je nach dessen Funktion getrennte Ausgewogenheitsprüfungen durchzuführen; in zweiter Linie geht es um die Einführung zusätzlicher besonderer Schutzmaßnahmen zur Verhinderung unangemessener Folgen für die betroffenen Personen.

4. Stellungnahme der Artikel-29-Arbeitsgruppe

4.1 Der Rechtsrahmen

Der erstmalige Einsatz der kooperativen, intelligenten Verkehrssysteme ist für 2019 vorgesehen. Der maßgebliche Rechtsrahmen für die Verarbeitung personenbezogener Daten in Bezug auf C-ITS ist folglich die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (Datenschutz-Grundverordnung), die am 25. Mai 2016 in Kraft trat und bis 25. Mai 2018 geltendes Recht sein wird.

Darüber hinaus könnte in Zukunft die neue Verordnung über Privatsphäre und elektronische Kommunikation Relevanz erlangen. Nach dem Vorschlag der Europäischen Kommission (COM(2017)10)[2] sollte die Verordnung auch für Kommunikationsvorgänge zwischen Maschinen gelten.

[1] ETSI EN 302 637-2 „Intelligent Transport Systems“ ITS; Vehicular Communications; Basic Set of Applications; Teil 2: Specification of Cooperative Awareness Basic Service’ und ETSI EN 302 637-3 „Intelligent Transport Systems ITS; Vehicular Communications; Basic Set of Applications; Teil 3: Specifications of Decentralised Environmental Notification Basic Service“.

[2] Gesetzgebungsvorschlag COM(2017)10 der Europäische Kommission über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (Verordnung über Privatsphäre und elektronische Kommunikation), Januar 2017. Siehe auch die Stellungnahme WP247 der Artikel-29-Arbeitsgruppe, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

4.2 Personenbezogene Daten / Identifizierung betroffener Personen

Die C-ITS-Arbeitsgruppe hat ganz richtig festgestellt, dass per C-ITS übermittelte Daten personenbezogene Daten sind, weil sie sich auf identifizierte oder identifizierbare betroffene Personen beziehen. Die betroffenen Personen können auf verschiedene Weise identifiziert werden. Erstens ist dies über die Zertifikate, die ihnen durch die PKI bereitgestellt werden, möglich, denn diese Zertifikate werden in ihrer Gestaltung einmalig sein, damit das Fahrzeug, in denen sie installiert sind, eindeutig wird. Zweitens ist dies über die eigentlichen Standortdaten möglich; die Identifizierungskraft von Standortdaten ist bekannt[3]: es genügen ein paar Punkte auf einem Pfad, um eine Einzelperson in einem Kollektiv mit hoher Präzision zu isolieren, wenn man die meist regelmäßigen Mobilitätsmuster der Menschen berücksichtigt.

Dies trifft insbesondere auf CAM-Meldungen zu. DENM-Meldungen enthalten ebenfalls Berechtigungstickets und die Daten zur Beschreibung eines bestimmten Ereignisses. Je nach der Art und Weise, in der das Ereignis eintritt (beispielsweise selten in Erscheinung tretendes Gebiet, auffällige Tageszeit oder die Dynamik der Ereigniskette) kann die betroffene Person auch aufgrund dieser Meldungen identifizierbar sein.

Zur Anwendbarkeit von Artikel 11 der Datenschutz-Grundverordnung möchte die Artikel-29-Arbeitsgruppe folgende Bedenken äußern. In Artikel 11 wird erklärt, dass es Verarbeitungsvorgänge gibt, für die die Identifizierung der betroffenen Person nicht oder nicht mehr erforderlich ist, und dass der Verantwortliche nicht verpflichtet ist, zur bloßen Einhaltung der Datenschutz-Grundverordnung die betroffene Person zu identifizieren. Dieser Artikel sollte als Methode zur Durchsetzung „echter“ Datenminimierung, bei der jedoch die Ausübung der Rechte der betroffenen Person nicht erschwert wird, ausgelegt werden. Die Ausübung dieser Rechte muss mithilfe zusätzlicher, von der betroffenen Person bereitgestellten Informationen ermöglicht werden. Durch die Berufung auf Artikel 11 der Datenschutz-Grundverordnung ohne genaue Angabe, welche zusätzlichen Informationen zur Ermöglichung der Identifizierung der betroffenen Personen erforderlich sind, wird die Ausübung der Rechte der betroffenen Personen (Zugang, Berichtigung, Portabilität usw.) de facto verhindert. Allerdings sind pseudonymisierte Daten per definitionem personenbezogene Daten (siehe Artikel 4 der Datenschutz-Grundverordnung), da es sich bei ihnen um Daten handelt, die sich auf eine identifizierbare natürliche Personen beziehen (siehe insbesondere Erwägungsgrund 26 der Datenschutz-Grundverordnung).

[3] Artikel-29-Arbeitsgruppe, WP X, Stellungnahme 05/2014 über Anonymisierungstechniken.

Aus diesen Grund fordert die Artikel-29-Arbeitsgruppe die C-ITS-Arbeitsgruppe zu Vorschlägen hinsichtlich des Konzepts der „zusätzlichen Informationen“ auf, die im Zusammenhang mit diesem neuen Dienst übermittelt werden können, damit diese Bestimmung wirksam werden kann; hierbei können beispielsweise spezifische Fahrzeugdaten oder die hohe Identifizierbarkeit von Standortdaten berücksichtigt werden. Die Arbeitsgruppe lehnt jede Auslegung von Artikel 11 ab, die auf eine Minderung der Verantwortung des oder der Datenverantwortlichen für die Einhaltung von Datenschutzverpflichtungen hinausläuft.

Die durch das C-ITS verarbeiteten personenbezogenen Daten können im Zusammenhang mit Signalverstößen (beispielsweise „Signalverstoß/Sicherheit an Kreuzungen“ in der Arbeitsunterlage) auch besondere Datenkategorien, wie sie in Artikel 10 der Datenschutz-Grundverordnung definiert werden, einschließen. Diese besonderen Kategorien von Daten können in C-ITS verarbeitet und an andere Fahrzeuge gesendet werden. In Artikel 10 der Datenschutz-Grundverordnung wird im Einzelnen festgelegt, dass Daten über strafrechtliche Verurteilungen und Straftaten nur verarbeitet werden dürfen, wenn dies unter behördlicher Aufsicht erfolgt oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Daraus folgt, dass die Anwendungen für Tag eins so zu verändern sind, dass die Erfassung und Verwendung von eventuell unter Artikel 10 fallenden Informationen verhindert wird.

Die Arbeitsgruppe sieht mehrere technische Möglichkeiten zur Minimierung der Risiken einer Wiedererkennung.

Erstens kann die Ausgabepolitik für die PKI-Zertifikate verbessert werden. Solange ein Zertifikat gültig ist, kann ein Fahrzeug identifiziert und nachverfolgt werden; Nachverfolgung im Nahbereich ist eine wichtige Gestaltungskomponente von C-ITS. Die Verfolgung im Nahbereich erlaubt die Herstellung eines engen Kausalzusammenhangs zwischen den Straßenverhältnissen und den Kraftfahrzeugen, die sich in dem betreffenden Bereich bewegen; aus diesem Grund wird sie als notwendig erachtet, damit das System aktiviert werden kann und die Anwendungen funktionieren können. Um eine für die Verkehrssicherheit nicht erforderliche Langzeitverfolgung zu verhindern, werden die Berechtigungstickets im Zeitablauf geändert. Die C-ITS-Arbeitsgruppe betont zwar die Notwendigkeit einer niedrigen Tauschfrequenz für die Berechtigungstickets, damit der Verbrauch von Zertifikaten begrenzt und die einfache Identifizierung von Gefahren und Ausgabe von Warnungen bezüglich in der Nähe befindlicher Fahrer nicht zunichtegemacht werden, aber die Artikel-29-Arbeitsgruppe empfiehlt eine sorgfältige Bewertung der Möglichkeiten einer höheren Frequenz, um die Risiken einer Langzeitverfolgung zu begrenzen.

Zweitens muss die Häufigkeit der Sendung von CAM-Meldungen angepasst werden.
Nach den vorgeschlagenen Häufigkeitseinstellungen für CAM-Meldungen wäre die Verfolgung von Fahrzeugen in einem Bereich von wenigen Metern möglich. Dies ist beispielsweise möglich, wenn verschiedene Segmente sehr dichter Abfolgen zeitbezogener Punkte, die sich z. B. auf einer Karte lokalisieren lassen, durch ein bestimmtes Zertifikat unterschiedlich „gefärbt“ werden (in der Annahme, dass jedem Zertifikat visuell eine andere Farbe zugeordnet wird). Die Aussage der C-ITS-Arbeitsgruppe in ihrer Unterlage, nämlich dass eine „unterschiedliche Färbung“ dieser Segmente auf der Karte (d. h. Zuordnung unterschiedlicher Zertifikate zu den Segmenten) einen Beobachter an der Rekonstruktion des gesamten Weges eines Fahrzeugs hindern würde, ist in Frage zu stellen. Mobilitätsdaten hängen schon von ihrer Art her stark miteinander zusammen und wiederholen sich bei den

meisten Fahrern regelmäßig; die Durchführung eines Abgleichs scheinbar unzusammenhängender Segmente auf einem durchgehenden Pfad sollte man bei einem Angreifer mit den erforderlichen Mitteln und der entsprechenden Motivation nicht als abwegig betrachten. Ändert ein Fahrzeug sein Zertifikat, wäre es darüber hinaus immer noch möglich, das alte mit dem neuen Zertifikat in Verbindung zu bringen, denn jedes Fahrzeug in der Nähe des sein Zertifikat wechselnden Fahrzeugs wird in der Lage sein, das Verschwinden des alten und Auftauchen des neuen Zertifikats zu beobachten und somit eine Verbindung zwischen den beiden herzustellen. Die C-ITS-Arbeitsgruppe sollte sich mit diesem Problem befassen, damit derartige Korrelationen verhindert werden.

Drittens hebt die Artikel-29-Arbeitsgruppe die Wichtigkeit des Grundsatzes der Datenminimierung zur Eindämmung von Wiedererkennungsrisiken hervor; hierbei können auch Abhilfemaßnahmen wie Generalisierung oder Rauschinjektion[4] zum Einsatz kommen. Diese Abhilfemaßnahmen können technisch so gestaltet werden, dass das Gesamtbild des Umfeldstatus und die Möglichkeit der Erkennung einer neuen Gefahr nicht beeinträchtigt werden, aber zugleich eine unnötige Exposition oder Langzeitverfolgung des Fahrers begrenzt wird. Besondere Aufmerksamkeit sollte der Generalisierung der statischen Eigenschaften bzw. einer entsprechenden Rauschinjektion gewidmet werden, um das Risiko einer Verfolgung mittels „Abnahme des Fingerabdrucks“ der Fahrzeugeigenschaften möglichst gering zu halten.

4.3 Risiken für die Privatsphäre

Die Artikel-29-Arbeitsgruppe erkennt an, dass die Grundidee des C-ITS den Autofahrern Vorteile erbringen kann, indem es ihnen ein höheres Niveau an Einsatzfähigkeit und Umweltbewusstsein bietet; der Nutzen für die Allgemeinheit besteht in der Erhöhung der Verkehrssicherheit und dem Schutz der Sicherheit anderer Autofahrer sowie Fußgänger. Nichtsdestotrotz weist die Artikel-29-Arbeitrgruppe ausdrücklich darauf hin, dass ein in großem Maßstab erfolgender Einsatz dieser neuen Technologie, der die Erfassung und Verarbeitung nie da gewesener Mengen an Standortdaten natürlicher Personen in Europa mit sich bringen wird, eine neue Bedrohung der Grundrechte darstellt und für den Schutz der personenbezogenen Daten und der Privatsphäre sowohl der Nutzer als auch anderer, möglicherweise betroffener natürlicher Personen neue Herausforderungen mit sich bringt.

In erster Linie können mit C-ITS aufgrund seines Konzept Dinge offengelegt werden, die wir gewöhnlich nicht öffentlich machen, nämlich wohin wir fahren und wie wir fahren. Durch die Übertragungs- und Empfangsmöglichkeiten der Fahrzeuge werden diese ganz privaten Informationen öffentlich an jedes in der Nähe befindliche Fahrzeug gefunkt. Dies ist eine Form der verteilten, permanenten Verhaltensüberwachung, die ein unbehagliches Gefühl der heimlichen Beobachtung auslösen kann.

Mangelnde Transparenz ist ein weiteres erhebliches Risiko für die Privatsphäre. Durch ihre Fahrzeuge werden Nutzer zu ununterbrochen sendenden Funkstationen. Sie müssen sich vollständig über den Umfang der Verarbeitung, die anderen Partner, mit denen sie Daten im C-ITS-Umfeld austauschen (andere Fahrzeuge, Automobilhersteller, Straßennetzmanager, sonstige öffentliche oder private Beteiligte) und die Art und Weise, wie sie diese Daten verarbeiten, im Klaren sein.

[4] Siehe die Beispiele in der Stellungnahme 05/2014 der Artikel-29-Arbeitsgruppe, WP216, über Anonymisierungstechniken.

Die Entscheidung, für die Verbreitung von Meldungen das Funken unter Partnern statt eins-zu-eins-Kommunikationen zu wählen, stellt eine weitere Herausforderung dar, denn dadurch können Meldungen von einer unbegrenzten Zahl an Einrichtungen, deren Absichten und technologischen Einsatzfähigkeiten dem Absender nicht bekannt sind und auch nicht bekannt sein können, empfangen werden. Dies verursacht eine Informationsasymmetrie zwischen den Absendern und den anderen Partnern (Empfängern) des C-ITS. Diese Asymmetrie muss mit einem höheren Niveau der Kontrolle über die personenbezogenen Daten wieder ausgeglichen werden.

Kinematische und standortbezogene Daten werden für eine ganze Reihe interessierter Parteien mit ganz unterschieden Absichten und Zielsetzungen, angefangen bei Werbeagenturen, über Automobilhersteller bis hin zu Versicherungsgesellschaften, von hohem Wert sein. Ein uneingeschränkter, willkürlicher Zugang zu innerhalb des C-ITS weitergegebenen Daten kann zu einer missbräuchlichen Ansammlung individueller Bewegungsprofile, einer „Datifizierung“ von Fahrverhalten, führen, auf deren Grundlage auf die jeweilige Person zugeschnittene Waren und Dienstleistungen gestaltet, beworben und verkauft werden können.

Die gleiche Attraktivität könnten Mobilitätsdaten möglicherweise auch für eine über den Zweck, für den C-ITS-Daten erzeugt und verarbeitet werden, hinausgehende Verfolgung von Straftaten und Verkehrsvergehen entwickeln. Dies gibt Anlass zu Bedenken hinsichtlich der Erforderlichkeit und Verhältnismäßigkeit bei der potenziellen Nutzung der Daten für diese andere Zwecke.

Die schleichende Ausweitung der Zweckbestimmung ist ein weiteres hervorstechendes Risiko von C-ITS. Die der gewählten Senderarchitektur innewohnende Informationsasymmetrie hinsichtlich der Identität der anderen Partner könnte, wenn ihr nicht mit Instrumenten zur Vertrauensbildung entgegengewirkt wird, Abweichungen vom ursprünglichen Anwendungsbereich der Kommunikation hervorrufen und Nutzer an ursprünglich nicht beabsichtigte Zielorte umleiten. Dies kann entweder aufgrund fehlerhafter Vorhersagen zum Zustand des Umfeldes (indem beispielsweise ein Verkehrsstau hervorgerufen wird anstatt die Verkehrsbelastung zu senken) oder sogar aufgrund einer nicht neutralen Interpretation von Umweltdaten eintreten (indem Autofahrer beispielsweise aufgrund wirtschaftlicher Interessen eines der Partner dazu gebracht werden, bestimme Gebiete zu besuchen).

4.4 Rechtmäßigkeit der Verarbeitung

Es ist hervorzuheben, dass die Verordnung (EU) 2016/679 keine Anwendung auf die Verarbeitung personenbezogener Daten im Zuge einer rein persönlichen oder haushaltsbezogenen Tätigkeit findet (Artikel 2 (2)(c)). Diese Ausnahme kann nur gelten, wenn sie strikt auf die innerhalb eines Kraftfahrzeugs stattfindende Verarbeitung beschränkt ist, und auch dann nur, wenn der Autofahrer die volle Kontrolle über die Verarbeitung innerhalb des Endgeräts hat. Sie kann nicht gültig sein, wenn das im Kraftfahrzeug eingebaute Endgerät die Daten an andere, in der Nähe befindliche Fahrzeuge weiterleitet, sei es sofort oder als Ergebnis einer vor Ort erfolgenden Verarbeitung. In derartigen Fällen ist die Verarbeitung nicht auf eine streng persönliche Tätigkeit beschränkt.

Angaben zur Rechtmäßigkeit der Verarbeitung personenbezogener, in die Funktionsweise des C-ITS einbezogener Daten sind in Artikel 6 Absatz 1 der Datenschutz-Grundverordnung zu suchen. Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung

der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben; b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen; c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen; e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

In Anbetracht des Anwendungsbereichs des C-ITS, nämlich der Erhöhung der Verkehrssicherheit, der Förderung der Verkehrseffizienz und dem Voranbringen der ökologischen Nachhaltigkeit unter anderem mittels der Einführung dieses europaweiten, interoperablen Systems, ist die Artikel-29-Arbeitsgruppe der Auffassung, dass der Erlass eines EU-weiten Rechtsaktes die langfristige Rechtsgrundlage für diese Art der Datenverarbeitung bildet (Artikel 6 Absatz 1 Buchstabe c der Datenschutz-Grundverordnung). In Anbetracht der prognostizierten weiten Verbreitung (halb-)autonomer Kraftfahrzeuge ist damit zu rechnen, dass die Einbeziehung dieser Technologie in Fahrzeuge irgendwann zur zwingenden Vorschrift wird, vergleichbar mit der gesetzlichen Verpflichtung für Automobilhersteller, alle neuen Fahrzeuge mit eCall-Funktionalität auszustatten. Eine solche gesetzliche Verpflichtung sollte jedoch keine flächendeckende Erfassung und Verarbeitung personenbezogener Daten ermöglichen. Im Rahmen des durch die anwendbaren Grundrechte gewährten Schutzes ist es geboten, den Umfang gesetzlicher Verpflichtungen umfassend zu bewerten und als verhältnismäßig und in einer demokratischen Gesellschaft unbedingt erforderlich zu bestätigen.

Dieser Bewertungs- und Gesetzgebungsprozess ist von der Kommission so bald wie möglich einzuleiten, um zu verhindern, dass die Verarbeitung von Standortdaten und anderen personenbezogenen Daten von EU-Bürgerinnen und -Bürgern im Rahmen des C-ITS ohne Rechtsgrundlage stattfindet und nicht vollständig durch ein adäquates Niveau an Schutz gedeckt wird.

In der Analyse der anderen Rechtsgrundlagen fehlen einige maßgeblichen Elemente. Bei dieser Aufgabe könnte eine Bewertung der technischen Einsatzmöglichkeiten des C-ITS und seines Anwendungsbereichs hilfreich sein.

Die Verfolgung der Position, Geschwindigkeit und Richtung des Fahrzeugs ist wesentlicher Kern des C-ITS. Je höher die Häufigkeit der ausgetauschten Meldungen, desto schärfer und detailreicher ist der Überblick über die Umgebung der Fahrzeuge und umso besser wird die Fähigkeit des Systems, Gefahren vorherzusehen. Die Artikel-29-Arbeitsgruppe ist sich darüber im Klaren, dass der Umfang, in dem Daten übernommen und beigetragen werden, ein entscheidender Faktor für den Betrieb von C-ITS ist; eine schlechte Datenverteilung oder niedrige Auflösung des von jedem Fahrzeug erfassten Umweltbildes könnte die Validität von C-ITS als Instrument der Verkehrssicherheit beeinträchtigen oder sogar zerstören.

Aber die Auslösung einer Datenübernahme und das Aufzwingen einer allgegenwärtigen Verfolgung sind nicht dasselbe. Die Möglichkeit, vom C-ITS an sich zu profitieren, sollte

Autofahrer zur freien Teilnahme am C-ITS anregen. Tritt dies ein, kann eine kritische Masse an Nutzern erreicht werden, um einen korrekten Betrieb des Systems zu erlauben ohne es aufzuzwingen; gleichzeitig wird den Menschen die Freiheit der Entscheidung erhalten, ob sie an dem System teilnehmen möchten und wenn ja, die Verfolgungsoptionen (Zeitpunkte, Häufigkeit, Standorte) zu wählen, die ihren Vorlieben am besten entsprechen.

Das Niveau der Verfolgungsauflösung wird in den Leistungsindikatoren des Systems[5] gut dargestellt:

„A vehicle will generate a CAM approximately every 4 metres and when the driving direction changes with more than 4°. When a distance between current and past position has been changed more than 4 meters or the speed is changed more than 0.5 m/s compared to the last time a CAM is sent but at least once a second and at the most once 0.1 second under normal conditions." [Ein Fahrzeug erzeugt etwa alle 4 m sowie bei einer Änderung der Fahrtrichtung um mehr als 4 Grad eine CAM. Hat sich die Entfernung zwischen der derzeitigen und der vorhergehenden Position um mehr als 4 Meter verändert oder ändert sich die Geschwindigkeit um mehr als 0,5 m/s gegenüber dem letzten Mal, so wird eine CAM gesendet; unter normalen Umständen wird jedoch mindestens einmal pro Sekunde und höchstens einmal pro 0,1 Sekunde gesendet.]

Diese Verfolgungsoptionen sind die Messbasis. Laut der Unterlage *handelt es sich hierbei um die derzeit festgelegten Spezifikationen, die sich jedoch mit den tatsächlichen Erfordernissen neu hinzukommender Funktionen ändern können.* Aus der Unterlage geht auch hervor, dass diese Einstellungen vom Nutzer nicht geändert werden können. Damit verfälscht die C-ITS-Arbeitsgruppe das Gleichgewicht zwischen dem Erfordernis, die Übernahme des C-ITS zu fördern, und dem Erfordernis, „Schwarzfahrer", die nicht am System teilnehmen, aber seine Vorteile genießen, dadurch zu verhindern, dass die Häufigkeit des Meldungsaustausches (und somit die Granularität der Verfolgung) auf den höchstmöglichen Wert gesetzt wird.

Die C-ITS-Arbeitsgruppe hat noch keine Übereinstimmung über die technische Machbarkeit der Einholung von Einwilligungen erreicht. Die Arbeitsgruppe betont, dass, wie in Artikel 7 der Datenschutz-Grundverordnung sowie Erwägungsgrund 42 umrissen wird, sämtliche Elemente einer gültigen Einwilligung erfüllt sein müssen. Datenverantwortliche müssen sorgfältig auf die Modalitäten für die Einholung spezifischer und freier Einwilligungen nach entsprechender Aufklärung bei den verschiedenen Teilnehmern wie Kraftfahrzeugeigentümern und Kraftfahrzeugnutzern achten. Eine solche Einwilligung muss jeweils separat für bestimmte Zwecke erteilt werden und darf nicht mit dem Kauf- oder Leasingvertrag eines neuen Kraftfahrzeugs gebündelt werden; auch muss die Einwilligung genauso einfach zurückgezogen werden können, wie sie erteilt wird. In Bezug auf Arbeitnehmer ist eine Einwilligung darüber hinaus kein ausreichender Rechtsgrund, denn das Verhältnis zwischen Arbeitgebern und Arbeitnehmern ist durch rechtliche Unterordnung geprägt; Arbeitnehmern steht es nicht frei, ihre Einwilligung zu verweigern.

Da C-ITS auf ununterbrochener Funkübertragung basiert, gibt es keinen Punkt, an dem die Übertragung unterbrochen ist und aufseiten des Nutzers Absichten oder Wünsche signalisiert werden könnten. Darüber hinaus ist die Funkübertragung eine vollkommen nach außen gerichtete Kommunikationsmethode ohne Rückwirkung; damit wird es unmöglich, einen gegenseitigen Erkennungsmechanismus zwischen der betroffenen Person (dem Absender) und dem Verantwortlichen (dem Empfänger) einzurichten. Dieses Fehlen einer gegenseitigen

[5] Processing personal data in the context of C-ITS. Annex I – day one applications, standards & security (A.2.2 CAM).

Erkennung dürfte für sich genommen die Nutzung von Einwilligungen nicht ausschließen, erschwert es aber, nur Daten für bestimmte, genau festgelegte Zwecke von bekannten Datenverantwortlichen verarbeiten zu lassen. Andererseits ist die in der Unterlage vorgebrachte Behauptung, dass eine Einwilligung nicht als tragfähige Rechtsgrundlage betrachtet werden könne, weil der Verantwortliche in diesem Stadium nicht in einem Grad definiert sei, der es der betroffenen Person ermögliche, dessen Identität zu kennen, irreführend, denn die Existenz eines genau definierten Verantwortlichen bzw. mehrerer Verantwortlicher ist eine Vorbedingung für die Verarbeitung an sich und keine Rechtsgrundlage nach Artikel 6 Absatz 1 der Datenschutz-Grundverordnung würde Unbestimmtheiten bei dessen Identifizierung rechtfertigen. Der technische Aufwand, zur Signalisierung von Nutzerpräferenzen Marker in die Struktur der CAM- und DENM-Meldungen aufzunehmen, ist ein guter Ausgangspunkt, aber noch keine Lösung.

Die C-ITS-Arbeitsgruppe spricht auch die Möglichkeit an, sich auf das Erfordernis der Erfüllung eines Vertrags (Artikel 6 Absatz 1 Buchstabe b der Datenschutz-Grundverordnung) zu stützen. Ein spezieller Vertrag zwischen einer betroffenen Person und dem Verantwortlichen, der von anderen Kauf- oder Leasingverträgen für ein Kraftfahrzeug getrennt ist, könnte dem Fahrer im Prinzip die freie Einhaltung des Systems erlauben.

Was die Option der in Artikel 26 der Datenschutz-Grundverordnung vorgesehenen gemeinsamen Verantwortlichkeit für die Verarbeitung angeht, so ist darauf hinzuweisen, dass es sich hier weder um ein Machtspiel zwischen den gemeinsam Verantwortlichen handelt noch beabsichtigt ist, einen Ermessensspielraum für die Gestaltung von Vereinbarungen zu gewähren, damit die Pflichten der Verarbeitungsverantwortung teilweise oder vollständig umgangen werden können. Die gemeinsam für die Verarbeitung Verantwortlichen, die eine feste Beziehung zu Kunden oder natürlichen Personen hergestellt haben, können direkt mit ihnen kommunizieren und müssen die volle Verantwortung für die Information dieses Personenkreises über die Verantwortungskette sowie das Bestehen und die Zwecke der anderen gemeinsam für die Verarbeitung Verantwortlichen übernehmen.

Im Hinblick auf den Fall, dass die Verarbeitung für die Erfüllung eines bestimmten, frei gewählten Vertrags, zu dem die betroffene Person Vertragspartei ist, erforderlich ist, hat die Artikel-29-Arbeitsgruppe wiederholt klargestellt[6], dass diese Bestimmung streng auszulegen ist und dass ein eindeutiger Zusammenhang zwischen der Beurteilung der Erforderlichkeit und der Einhaltung des Grundsatzes der Zweckbindung besteht. Im Kontext des C-ITS sind vor allem zwei Gesichtspunkte von besonderer Bedeutung. Erstens ist es wichtig, vorab die am Vertrag beteiligten Parteien eindeutig zu bestimmen, damit die Verarbeitung auf den begrenzten Umkreis der am Anwendungsbereich des C-ITS beteiligten Akteure beschränkt und eine weitergehende Nutzung durch unbestimmte andere Parteien vermieden werden kann. Das in der Unterlage angeführte Beispiel eines Vertrags zwischen betroffenen Personen und dem Betreiber einer Privatstraße ist unvollständig, weil an der Verarbeitung auch andere – entweder als gemeinsam für die Verarbeitung Verantwortliche nach Artikel 26 der Datenschutz-Grundverordnung handelnde oder im Kontext eines einzelnen, die Funktionen eines voll für die Verarbeitung Verantwortlichen erfüllenden Konsortiums agierende – Parteien (beispielsweise Automobilhersteller und Softwareentwickler) beteiligt sein können, die einen Vertrag mit betroffenen Personen schließen können. Zweitens müssen das Grundprinzip des Vertrags, sein Gehalt und seine Ziele vor der eigentlichen Verarbeitung festgelegt worden sein und der oder die für die Verarbeitung Verantwortliche(n) muss/müssen anhand dieses Grundprinzips und dieser Ziele prüfen, ob die Verarbeitung für die Erfüllung

[6] Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten und Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG.

des mit jedem einzelnen Nutzer geschlossenen Vertrags erforderlich ist; hierbei ist zu berücksichtigen, dass Kraftfahrzeuge von den Eigentümern oder anderen Nutzern gefahren werden können.

Hinsichtlich der möglichen Anwendung der Bedingung, dass die Datenverarbeitung aus einem berechtigten Interesse erforderlich sein muss (Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung), erinnert die Artikel-29-Arbeitsgruppe daran, dass diese Bestimmung nicht als Möglichkeit „der letzten Wahl" für komplexe Fälle, in denen andere Gründe für eine rechtmäßige Verarbeitung nur schwer anwendbar sind, behandelt werden sollte. Das Ergebnis der Ausgewogenheitsprüfung könnte bestimmen, ob man sich auf Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung als Rechtsgrundlage für die Verarbeitung stützen kann. Die Identifizierung der Verantwortlichen und ihrer Interessen ist laut Aussage der Unterlage eine Voraussetzung; es sind aber auch andere maßgebliche Faktoren zu berücksichtigen.[7] Berücksichtigt man insbesondere den Grund, aus dem ein Interesse berechtigt ist (d. h. ob es dem öffentlichen Interesse oder dem geschäftlichen Interesse eines bestimmten Beteiligten entspringt), sowie die Folgen für die betroffenen Personen und ihre Erwartungen bezüglich der Privatsphäre, so können in Anbetracht der potenziellen Sensibilität von Standortdaten die zusätzlichen Schutzmechanismen auch unter technischen Gesichtspunkten unangemessene Folgen für sie begrenzen.

4.5 Sicherheit

C-ITS basiert auf der Funkübertragung von Meldungen. Für die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Kommunikationen, d. h. die Kommunikationssicherheit, sind in diesem Zusammenhang im Vergleich zu eins-zu-eins Kommunikationen besondere Anstrengungen und zusätzliche Spezifikationen erforderlich.

Funk ist ein eine beschränkungslose Methode der Kommunikation an eine unbegrenzte Zahl von Empfängern innerhalb der Reichweite eines Sendegeräts. Dementsprechend wird sich eine sinnvolle Methode zur Begrenzung der Verarbeitung gesendeter Information ausschließlich auf den Kontext der C-ITS-Anwendung (mittels Vermeidung einer unrechtmäßigen Verarbeitung durch andere Empfänger ohne Bezug zu C-ITS) auf die Existenz vertrauenswürdiger Partner und die Überlegung stützen, dass die Nutzung aus dem C-ITS stammender Daten zu anderen Zwecken als der Verkehrssicherheit eine strafbare Handlung darstellt.

Hier ist daran zu erinnern, dass der Gesetzgebungsvorschlag COM(2017)10 – die Verordnung über Privatsphäre und elektronische Kommunikation – äußerst strenge Beschränkungen der Nutzung „ausgesendeter Daten" wie CAM- und DENM-Meldungen enthält und in Artikel 8 Absatz 2 ein allgemeines Verbot der Nutzung ausspricht, sofern sie nicht ausschließlich zum Zweck der Herstellung einer Verbindung und für die dazu erforderliche Dauer erfolgt; dabei gilt die Voraussetzung, dass geeignete technische und organisatorische Maßnahmen, die ein dem Risiko angemessenes Schutzniveau nach Artikel 32 der Datenschutz-Grundverordnung gewährleisten, angewendet werden.

In der Unterlage wird der PKI-Mechanismus besonders als Möglichkeit zur Schaffung von Vertrauen im C-ITS-System hervorgehoben. Tatsächlich ist PKI eine Methode zur

[7] Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG.

Durchsetzung der Verbreitung einer bestimmten Informationsquelle (beim C-ITS sind dies digitale Zertifikate) im Rahmen einer beaufsichtigten Leitungsstruktur. PKI sieht keinen Durchsetzungsmechanismus zur Feststellung der tatsächlichen Absichten der Inhaber oder Aussteller der Zertifikate vor. Tatsächlich sind in letzter Zeit geheime Absprachen oder Sicherheitsvorfälle, die Zertifizierungsbehörden betrafen, häufiger geworden und es bestehen starke Anreize, Zertifizierungen allein zu dem Zweck zu erwerben, böswillige Handlungen zu begehen.[8]

Das Bestehen einer PKI-Architektur gewährleistet nicht per se, dass zwischen den Partnern Vertrauen hergestellt wird. Zur Stärkung des Vertrauens sind noch weitere, zusätzliche Maßnahmen erforderlich. Die Einführung von Mechanismen zur Gewährleistung von Sicherheit ist dabei ein wichtiges Element. Weitere relevante Faktoren sind genaue, regelmäßige Kontrollen der Arbeit der Zertifizierungsbehörden, die entweder in Form eines Quervergleichs zwischen Zertifizierungsbehörden oder mittels Audits oder Inspektionen stattfinden, die von den an der Förderung des C-ITS beteiligten öffentlichen Einrichtungen durchgeführt werden.

Für Integrität zu sorgen heißt, zu vermeiden, dass Daten in unzulässiger Weise verändert werden und damit das ordnungsgemäße Funktionieren eines Informationssystems verfälscht wird. Im Kontext des Funkbetriebs des C-ITS kann dies vorkommen, wenn Partner (sogar vertrauenswürdige Partner) das Bild des Umfeldes durch verdecktes Injizieren verfälschter Daten oder Daten, die einem Geschäftsinteresse und nicht dem öffentlichen Ziel der Verkehrssicherheit dienen, manipulieren. Das Herausfiltern von Ausreißern im Strom der CAM- und DENM-Meldungen, die auf außerhalb des Durchschnitts liegende Indikatoren hinweisen könnten, stellt einen wirksamen Abschreckungsmechanismus vor einer böswilligen Nutzung von C-ITS dar; dieses Herausfiltern verkörpert zudem eine Methode, mit der sichergestellt werden kann, dass es sich bei den ausgetauschten Daten um für den Zweck wesentliche Daten handelt.

Unter Verfügbarkeit ist die Fähigkeit von Informationen zur Erfüllung ihres Zwecks dann, wenn es erforderlich ist, zu verstehen. Dies ist ein Attribut, dessen Gewährleistung in einem Funkumfeld äußerst heikel ist, denn hier besteht ein Zielkonflikt zwischen Zeit und Datenqualität. Wird die Existenz (und somit die Verfügbarkeit) von Daten in Bezug auf eine mögliche Gefahr durch die parallel erfolgende, massive Aussendung von Meldungen über die betreffende Situation ausgelöst, könnte man, wenn man sich auf eine zu kleine Stichprobe von Meldungen verlässt, zahlreiche Fehlalarme auslösen; wartet man andererseits, bis eine ausreichende Zahl von Nachweisen aus vielen unterschiedlichen Quellen gesammelt worden ist, könnte dies für die Sicherheit der Menschen zu spät sein. Die Verhütung von Unfällen ist ein ganz wesentliches Ergebnis, das man sich von der Verarbeitung personenbezogener Daten im Kontext des C-ITS erwartet; die Artikel-29-Arbeitsgruppe empfiehlt den Softwareentwicklern, bei der Gestaltung von Softwareprogrammen, die unter anderem mittels einer kooperativen Erweiterung der Serviceparameter in der Lage sind, falsch positive und falsch negative Daten auszusortieren, damit keine Fehlalarme ausgelöst oder, im Gegenteil dazu, die Sichtbarwerdung tatsächlich gefährlicher Situationen für die betroffenen Personen beeinträchtigt wird, äußerste Sorgfalt walten zu lassen.

[8] Edelman, Benjamin. „Adverse Selection in Online 'Trust' Certifications and Search Results.“ [negative Auslese in online-„Vertrauenszertifizierungen“ und Suchergebnissen] Electronic Commerce Research and Applications 10, Nr. 1 (Januar–Februar 2011).

5 Erforderliche Maßnahmen

Die Artikel-29-Arbeitsgruppe begrüßt die von der Europäischen Kommission und der Arbeitsgruppe für Datenschutz und Schutz der Privatsphäre der kooperativen, intelligenten Verkehrssysteme von Anfang an unternommenen Anstrengungen, die Grundsätze des Datenschutzes in den Betrieb dieser neuen Anwendungen einzubeziehen.

Die von der C-ITS-Arbeitsgruppe geleistete Arbeit ist ein guter Ausgangspunkt, muss aber durch eine Reihe spezieller Maßnahmen auf unterschiedlichen Ebenen ergänzt werden. Die Artikel-29-Arbeitsgruppe betrachtet die folgenden Gesichtspunkte des Datenschutzes als besonders relevant:

- Die Kommission sollte branchenspezifische Verordnungen über die Erfassung und Verarbeitung von Daten auf dem Gebiet der intelligenten Verkehrssysteme einführen;
- Die Kommission sollte einen Fahrplan für die rechtmäßige Verarbeitung von Standortdaten der EU-Bürgerinnen und -Bürger im Zusammenhang mit C-ITS-Anwendungen festlegen, dessen Endziel im Erlass eines EU-weiten Rechtsaktes besteht (Artikel 6 Absatz 1 Buchstabe c der Datenschutz-Grundverordnung);
- Der Erlass dieser Rechtsakte sollte mit einer Bewertung der Erforderlichkeit und Verhältnismäßigkeit ihrer Bestimmungen beginnen; darüber hinaus sollte im Zuge des Gesetzgebungsverfahrens eine Folgenabschätzung (Artikel 35 Absatz 10) der Datenschutz-Grundverordnung) angeordnet werden, damit von Anfang an Risiken und Maßnahmen zu ihrer Eindämmung abgeklärt werden können;
- Auf die weiteren, in der Unterlage der C-ITS-Arbeitsgruppe vorgesehenen Rechtsgrundlagen (und zwar Einwilligung und Erfüllung eines berechtigten Interesses eines Unternehmers) könnte man sich nur dann stützen, wenn für die in der vorliegenden Stellungnahme bezüglich jeder dieser Rechtsgrundlagen ermittelten, kritischen Fragestellungen Lösungen gefunden werden;
- Nach jeder der gewählten Rechtsgrundlagen muss die Voreinstellung sämtlicher installierter C-ITS-Funktionen ausgeschaltet werden.
- Die Bestimmungen des Artikels 25 der Datenschutz-Grundverordnung (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) sind umzusetzen, sodass Endnutzer die Möglichkeit zur Wahl der ihren Vorlieben am besten entsprechenden Verfolgungsoptionen (Zeitpunkte, Häufigkeit, Standorte) erhalten;
- Die Sicherheit ist zur Begrenzung des Risikos einer unrechtmäßigen, den Rahmen rechtmäßiger Zwecke überschreitenden Nutzung zu erhöhen;

- Andere Abhilfemaßnahmen im Rahmen des Datenschutzes durch Technikgestaltung, beispielsweise Generalisierung oder Rauschinjektion, sind einzuführen, damit das Gesamtbild des Umgebungsstatus und die Möglichkeit der Entdeckung einer neuen Gefahr nicht beeinträchtigt, zugleich aber eine unnötige Exposition oder Langzeitverfolgung des Fahrers begrenzt wird;
- Besondere Aufmerksamkeit ist der Häufigkeit, in der die Zertifikate gewechselt werden, zu widmen, damit ein angemessenes Gleichgewicht zwischen der gewählten Häufigkeit und den Risiken einer Langzeitverfolgung geschaffen wird;
- Besondere Kategorien von Daten und Daten über strafrechtliche Verurteilungen und Straftaten sind nicht per Funk zu versenden;
- Die Datenqualität ist zur Eindämmung der Risiken einer nicht neutralen Nutzung des C-ITS, der Erzeugung von Fehlalarmen oder, im Gegenteil dazu, der Fehlinterpretation wirklicher Notlagen sorgfältig zu beurteilen;
- Die PKI-Mechanismen für die Verteilung von Zertifikaten sind im Detail öffentlich zu dokumentieren und streng zu überwachen, damit das Risiko geheimer Absprachen zwischen Zertifizierungsbehörden und Partnern oder das Eindringen böswilliger Akteure begrenzt werden kann;
- Die von allen an der C-ITS-Plattform beteiligten Parteien einzuhaltenden Aufbewahrungsfristen für die verarbeiteten Daten sind eindeutig anzugeben und die Einrichtung einer zentralen Datenbank der von den Akteuren des C-ITS ausgetauschten Meldungen ist zu verbieten.