TUNNELSICHERHEIT: RECHTSFRAGEN ZUM EINSATZ VON C-ITS UND KÜNSTLICHER INTELLIGENZ

Jessica Fleisch / Robert Geidel / Jakob Zanol

Jessica Fleisch, Wissenschaftliche Projektmitarbeiterin, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10–16/2/5, 1010 Wien, AT
Jessica.Fleisch@univie.ac.at

Robert Geidel, Wissenschaftlicher Projektmitarbeiter, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10–16/2/5, 1010 Wien, AT
Robert.Geidel@univie.ac.at

Jakob Zanol, Wissenschaftlicher Projektmitarbeiter/Managing Scientist, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10–16/2/5, 1010 Wien, AT
Jakob.Zanol@univie.ac.at

Schlagworte: ***Tunnelsicherheit, Künstliche Intelligenz, Cooperative Intelligent Transport System (C-ITS), V2I, I2V, Datenschutzrecht, Haftung, IRIS2022***

Abstract: *Tunnelbauwerke sind komplexe bauwerkliche Anlagen, in denen die Sicherheitsanforderungen stets auf höchstem Niveau zu halten sind, um die Verwirklichung von Risiken zu verhindern und sowohl Leib und Leben der Nutzer als auch die Tunnelsubstanz selbst zu schützen. Durch den raschen technologischen Fortschritt im Bereich der C-ITS-Kommunikation stellt sich die Frage, inwiefern künstliche Intelligenz konventionelle Überwachungstechniken komplementiert und zur Erhöhung der Tunnelsicherheit beitragen kann. Dabei ergeben sich insbesondere datenschutz- und haftungsrechtliche Fragestellungen, welche in diesem Beitrag dargestellt werden sollen.*

1. Einleitung

Bereits konventionelle Tunnelüberwachungspraktika tragen wesentlich dazu bei, das Sicherheitsniveau in den einzelnen Tunnelbauwerken in einem angemessenen und vertretbaren Rahmen zu halten. Dabei offenkundiger Weise stets von der obersten Prämisse geleitet, die Sicherheit der einzelnen Verkehrsteilnehmer und Tunnelmitarbeiter, aber auch der Tunnelbauwerksubstanz selbst zu gewährleisten.

Bei Tunnelbauwerken handelt es sich grundsätzlich um äußert komplexe bauwerkliche Anlagen, die nicht nur einer strengen baurechtlichen Reglementierung unterliegen, sondern auch nach ihrer Inbetriebnahme in regelmäßigen Abständen und unter strenger Kontrolle auf ihre Sicherheitsarchitektur und ihr Sicherheitsmanagement überprüft werden müssen.[1] Wie auch die traurigen Ereignisse der Vergangenheit (Mont Blanc und Tauern Tunnel 1999 etc.) bedauerlicherweise bestätigen, kann ein gänzlicher oder zumindest teilweiser Ausfall der Sicherheitsarchitektur und/oder ein Mangel eines probaten Sicherheitsmanagements verheerende Folgen nach sich ziehen und zu katastrophengleichenden Zuständen mit zahlreichen Todesfällen führen. Zudem dürfen auch wirtschaftliche Faktoren nicht außer Acht gelassen werden. So ist bei einem längerfristigen Ausfall einer Tunnelanlage – insbesondere bei den wichtigen transeuropäischen Verkehrsschlüsselverbindungen – nicht nur mit monetären Nachteilen, gemessen am Schaden der Tunnelsubstanz, sondern auch mit teils

[1] Bundesgesetz über die Sicherheit von Straßentunneln (Straßentunnel-Sicherheitsgesetz – STSG), BGBl. I Nr. 54/2006 i.d.F. 96/2013; vgl. § 3 Abs. 5 STSG hinsichtlich der Verpflichtung von der Durchführung von behördlichen Inspektionen; § 6 STSG hinsichtlich der Durchführung von periodischen Übungen.

regionalen, aber auch schlimmstenfalls mit gesamteuropäischen wirtschaftlichen Auswirkungen zu rechnen. Dies ist selbstverständlich in Abhängigkeit zu Intensität und Ausmaß des eingetretenen Schadens, der örtlichen Lage der betroffenen Anlage und deren Ersatzroutenmöglichkeiten zu sehen. Wenig verwunderlich scheint es deshalb, dass bereits 2004 auf unionsrechtlicher Ebene eine Mindestharmonisierung im Bereich der Sicherheitsanforderungen der im transeuropäischen Straßennetzes[2] verlaufenden Tunnelbauwerke stattgefunden hat, um dort für ein ausreichendes, homogenes und konstantes Niveau bei der Sicherheit, den Diensten und dem Komfort zu sorgen.[3]

Aufgrund der rasch fortschreitenden technologischen Entwicklungen auch auf dem Gebiet des autonomen Verkehrs ist es überlegenswert, das bisherige Sicherheitskonzept der Tunnelbauwerke und Tunnelleitzentralen zu überdenken und an innovativeren Lösungsansätzen anzuknüpfen, um sicherheitsbezogene Prozesse im Tunnelsicherheitsmanagement zu optimieren und deren Anfälligkeit gegenüber Fehlern signifikant zu verbessern. Gerade die in den Tunnelleitzentralen sitzenden menschlichen Operatoren sind einem starken und äußerst nervenaufreibenden Leistungs- und Handlungsdruck ausgesetzt, da sie stets gefordert sind das Tunnelgeschehen adäquat zu beobachten, Ereignisfälle, die unmittelbaren Handlungsbedarf benötigen, zu erkennen und unverzüglich entsprechende Schritte einzuleiten, die dazu geeignet sind, den Schadenseintritt bestmöglich abzuwehren bzw. den Schaden vorzugsweise auf ein minimales Ausmaß zu reduzieren. Sollte sich bei dieser, auf den menschlichen Sinneswahrnehmungen beruhenden Entscheidungskette, ein Fehler einschleichen, kann dies im wahrsten Sinne eine Entscheidung über Leben oder Tod darstellen.

Im Rahmen des kooperationsübergreifenden Projektes „Künstliche Intelligenz zur Verbesserung der Sicherheit von Tunneln und Tunnelleitzentralen (KITT)“ wird an der soeben abgebildeten Problemstellung angeknüpft, und versucht konventionelle Tunnelüberwachungstechnik durch innovative Verfahren der Gefahrendetektion zu ergänzen. Dabei sollen insbesondere die Operatoren, die die volle Kontrolle über die Tunnelbauwerke ausüben, in den einzelnen Tunnelleitzentralen entlastet und durch den Einsatz von schwacher Künstlicher Intelligenz in ihrer Entscheidungsfindung unterstützt werden.[4] Da die zeitliche Dimension der Gefahrenerkennung ausschlaggebend ist, sollte gerade der damit implizierte, wenn auch durchaus idealistische Anspruch der sekundenschnellen Handlungsentscheidung bestmöglich optimiert werden. Dabei wird als Ziel des Projektvorhabens die Entwicklung eines Echtzeit-Risikobewertungssystems mittels Daten eines C-ITS[5] basierten Informationsaustausches zwischen Infrastruktur und Verkehrsteilnehmer sowie den bereits bestehenden Daten der konventionellen Tunnelüberwachung angestrebt. Voraussetzung für eine Echtzeit-Risikobewertung ist die adäquate und akkurate Abbildung des aktuellen Verkehrsgeschehens. Dies setzt allem voran voraus, dass eine entsprechende Infrastruktur implementiert und auch auf Seiten der einzelnen Verkehrsteilnehmer auf C-ITS-fähige Fahrzeuge flächendeckend aufgerüstet wird, damit künftig der Informationsaustausch direkt zwischen den Verkehrsteilnehmer selbst und der Infrastruktur (u.a. V2V, V2I und I2V-Kommunikation) stattfinden und somit Informationen in Echtzeit einerseits an die Infrastruktur übermittelt, aber auch von den Road-Side-Units (RSU) direkt an die Verkehrsteilnehmer ausgesendet werden. In Akkumulation mit anderen Daten aus den unterschiedlichsten Datenquellen (aus bereits vorhandenen Überwachungskameras, Wetterdaten, Daten vor dem Tunnel, etc.) soll ein stetig aussagekräftiges Lagebild des aktuellen Verkehrsgeschehens geliefert werden können, welches jeweils durch die künstliche Intelligenz aufbereitet wird. Der flächendeckende Ausbau einer C-ITS-fähigen Infrastruktur ist auch eine wesentliche Voraussetzung für einen hochautomatisierten Verkehr.

---

2 Entscheidung Nr. 1692/96/EG, Nr. L 228/1.

3 ErwGr. 2 Richtlinie 2004/54/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über Mindestanforderungen an die Sicherheit von Tunneln im transeuropäischen Straßennetz, ABl. L 2004/167, 39.

4 Nach dem derzeitigen Projektstand wird die finale Entscheidung weiterhin durch die menschlichen Operatoren zu treffen sein. Somit findet keine ausschließlich automatische Entscheidungsfindung durch eine KI i.S.v. Art. 22 DSGVO statt („schwache“ KI).

5 Kurz für: Kooperatives Intelligentes Verkehrssystem („Cooperative Intelligent Transport System C-ITS“).

Aus juristischer Sicht wirft der Einsatz von künstlicher Intelligenz (KI) zur Gefahrendetektion und deren verfolgte Echtzeit-Risikobewertung in den Tunnelbauwerken zahlreiche offene rechtliche Fragestellungen auf, die mithin im Projekt in Form einer umfassenden Compliance-Analyse bestmöglich geklärt und an dieser Stelle in einer holistischen Zusammenschau präsentiert werden sollen. Nachfolgend werden deshalb einzelne in Frage kommende Rechtsgebiete und die darin auftretenden (möglichen) Rechtsproblemen abgebildet und interessante Kernpunkte dargestellt.

2. Datenschutz und Tunnelsicherheitsrecht

Erste Experteninterviews zeigen, dass gerade datenschutzrechtliche Aspekte einen ganz wesentlichen Erfolgsfaktor zur Umsetzung des Forschungsprojekts darstellen, denn die Reichweite des Anwendungsbereichs der Datenschutz-Grundverordnung (DSGVO[6]) ist nicht zu unterschätzen. Der Europäische Gerichtshof (EuGH) hat in seiner Leitentscheidung in der Rechtssache *Breyer* klargestellt, dass bereits Informationen, die einer natürlichen Person nach allgemeinem Ermessen wahrscheinlich[7] zuordenbar sind, als personenbezogene Daten zu qualifizieren sind.[8] Konkret hatte der EuGH dynamische IP-Adressen zu qualifizieren, welche durch einen Webseitenbetreiber gespeichert wurden, jedoch von diesem nicht eigenständig einer natürlichen Person zugeordnet werden konnten. Der EuGH führte aus, dass die Speicherung der IP-Adressen u.a. zu Zwecken der Strafverfolgung erfolgte und ferner, dass Strafverfolgungsbehörden im Falle einer Anzeige über rechtliche Mittel verfügten, diese IP-Adressen (wiederum unter Mithilfe Dritter![9]) einer natürlichen Person zuzuordnen. Da somit eine Identifizierung einer natürlichen Person „nach allgemeinem Ermessen wahrscheinlich" sei, wurden „dynamische IP-Adressen" als personenbezogen qualifiziert.

Gerade dieser weite Anwendungsbereich des Datenschutzrechts, der spätestens mit der Geltung der DSGVO wohl weithin bekannt ist, führt dazu, dass datenschutzrechtliche Aspekte gerade im Kontext des C-ITS berücksichtigt werden müssen, welches zur Erfassung zusätzlicher Daten herangezogen werden soll. Hier sei vorab angemerkt, dass im Bereich des automatisierten Fahrens in diesem Zusammenhang vereinzelt argumentiert wird, dass eine kurzfristige Verarbeitung in „Echtzeit" bereits gar nicht als „Verarbeitung"[10] qualifiziert werden sollte.[11] Vertreter dieser Ansicht müssten dies konsequent auch auf andere Bereiche übertragen, wenngleich diese Ansicht im Ergebnis abzulehnen ist, so muss ihr doch immerhin zugestanden werden, dass derartige Echtzeit-Verarbeitungen, wie sie auch im Bereich des C-ITS durchgeführt werden sollen, in der Regel eine besonders geringe Eingriffsintensität aufweisen.

Dies lässt sich dadurch erklären, dass bei Datenverarbeitungen im Verkehrssystem, wie es in KITT beabsichtigt ist, die Daten – soweit möglich – bloß in aggregierter und damit anonymisierter Form genutzt werden sollen. Hier liegt jedoch die Schwierigkeit darin, dass sich jene Verarbeitungsvorgänge, die im Bereich des C-ITS stattfinden, nur selten gänzlich anonymisieren und somit außerhalb des Anwendungsbereichs der

---

6 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ABl. L 2016/119, 1.

7 Vgl ErwGr. 26 DSGVO: „*Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.*"; siehe bereits ErwGr. 26 DSRL.

8 Die betroffene Person gilt diesfalls als „identifizierbare" Person.

9 Der Telekommunikationsbetreiber.

10 Art. 4 Z. 2 DSGVO.

11 So etwa Klink-Straub/Straub, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, S. 3201 (3202); dahingehend auch Wendt, Autonomes Fahren und Datenschutz – eine Bestandsaufnahme, ZD-Aktuell 2018, S. 6034.

DSGVO verorten lassen.[12] Im Rahmen eines C-ITS basierten Informationsaustauschs werden sogenannte *Cooperative-Awareness-Messages* (CAM) und/oder *Decentralized Environmental Notification Messages* (DENM) zwischen den Verkehrsteilnehmer selbst und der Infrastruktur ausgetauscht. Sowohl CAMs[13] als auch DENMs[14] enthalten nach dem jeweiligen ETSI-Standard[15] eine Fahrzeugidentifikationsnummer und nehmen mit einem eigenen privaten Schlüssel an einer Public-Key-Infrastruktur (PKI) teil.[16] Über diese Informationen werden Fahrzeugnutzer zwar gerade nicht direkt „identifiziert", sind jedoch weiterhin „identifizierbar" i.S.d. Art. 4 Z. 1 i.V.m. ErwGr. 26 DSGVO.[17] Allein aus einer datenschutzrechtlichen Perspektive erscheint es zunächst kontraintuitiv, dass mit der Nutzung der Möglichkeiten im C-ITS eine Vielzahl neuer Datenquellen geschaffen werden soll, welche zu weiten Teilen den „gleichen" Informationsgehalt besitzen, wie die bereits genutzten Datenquellen[18] und somit als „redundant" betrachtet werden können. Gerade mit Blick auf den Grundsatz der Datenminimierung erscheint es somit auf den ersten Blick fraglich, ob sich eine zusätzliche Erhebung von personenbezogenen Daten rechtfertigen lässt, wenn bereits eine einzige Datenquelle (etwa Bilder durch die Videoüberwachung) eine adäquate Überwachung von Tunneln gewährleistet. Dabei ist jedoch zu bedenken, dass gerade diese Redundanz aus Sicherheitsüberlegungen wichtig ist, um die jeweils anderen Datenquellen zu verifizieren oder zumindest zu plausibilisieren und somit zu verhindern, dass sich durch eine einzige Fehlerquelle ein Risiko verwirklicht. Die Sicherheit wird in diesem Fall durch derart „redundante" Daten erhöht.[19]

Erklärtes Ziel des Projektes ist die Vorgaben aus dem Datenschutzrecht bereits bei der Etablierung der Verarbeitungsverfahren zu berücksichtigen, damit das Ergebnis bereits in größtmöglichem Umfang dem Grundsatz des Privacy-by-Design[20] gerecht wird. Geht man von einem Personenbezug in einer Vielzahl der Verarbeitungsvorgänge aus (seien diese auch noch so „flüchtig"[21]), so stellt sich in weiterer Folge die Frage nach der Zulässigkeit der Verarbeitung.

Auf unionsrechtlicher Ebene legt die Richtlinie 2004/54/EG über „Mindestanforderungen an die Sicherheit von Tunneln im transeuropäischen Straßennetz" für die sich im transeuropäischen Straßennetzes verlaufenden Tunnelbauwerke mit einer Länge von über 500m einheitliche Mindestsicherheitsanforderungen für organisa-

---

12 So etwa noch Buchner, Datenschutz im vernetzten Automobil, DuD 2015, S. 372 (374); aA ua Weichert, Datenschutz im Auto – Teil 1, Das Kfz als großes Smartphone mit Rädern, SVR 2014, S. 201; Kinast/Kühnl, NJW 2014, S. 3057 (3058); zur geltenden Rechtlage unter der DSGVO siehe insbesondere EDSA, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0, 2021, S. 5: *„Darüber hinaus generieren vernetzte Fahrzeuge immer größere Datenmengen, von denen die meisten als personenbezogene Daten betrachtet werden können, da sie sich auf Fahrer oder Insassen beziehen."* [Anm: auch wenn der EDSA Verarbeitungsvorgänge im C-ITS in dieser Stellungnahme grundsätzlich nicht thematisieren möchte, gelten die Grundsätze des vernetzten Fahrens wohl auch für die hier interessierenden Vorgänge]; vgl zuvor Art-29-Datenschutzgruppe, Stellungnahme 03/2017 zur Verarbeitung personenbezogener Daten im Kontext Kooperativer, Intelligenter Verkehrssysteme (C-ITS), WP 252, 2017, 4.

13 ETSI, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1, ETSI EN 302 637-2, 2019.

14 ETSI, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service V1.3.1, ETSI EN 302 637-3, 2019.

15 Zur generellen Struktur des ITS siehe auch ETSI, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions, ETSI TR 102 638 V1.1.1, 2009.

16 Siehe Art-29-Datenschutzgruppe, Stellungnahme 03/2017 zur Verarbeitung personenbezogener Daten im Kontext Kooperativer, Intelligenter Verkehrssysteme (C-ITS), WP 252, 2017, S. 4 [auf diese nunmehr verweisend: EDSA, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0, 2021, S. 13].

17 Siehe oben zur EuGH Rechtsprechung und der angeführten Reichweite des Personenbezugs.

18 Siehe für Österreich insbesondere die ausführliche Darstellung der Verarbeitungsvorgänge durch die österreichische Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft (ASFINAG). https://www.asfinag.at/privacy/ (aufgerufen am 25.10.2021).

19 Etwa Erhart/Ruehrup, Safe, green, smart: C-ITS is the game-changer in transport, Proceedings of the 27th ITS World Congress, Hamburg 2021, S. 3 (*„[...] Redundancy is important for infrastructure services, therefore e.g. every safety trailer works autonomously and avoids single point of failure. [...]"*).

20 Datenschutz durch Technikgestaltung, Art. 25 DSGVO.

21 Siehe bereits oben zur Echtzeit-Verarbeitung (FN 11).

torische, strukturelle, technische sowie betriebliche Aspekte von Straßentunneln in den einzelnen Mitgliedstaaten fest und normiert auch einen gesetzlichen Erlaubnistatbestand zur Videoüberwachung. Vorgegebene und oberste Prämisse ist die Verwirklichung eines einheitlichen, konstanten und hohen Schutzniveaus in den Straßentunneln der Mitgliedstaaten durch die Etablierung eines gemeinsamen Mindestsicherheitsstandards.[22]

In Österreich ist diese Richtlinie 2006 als Straßentunnel-Sicherheitsgesetz (STSG) und hinsichtlich der Bestimmungen für die Verkehrszeichen in die Straßenverkehrsordnung (StVO) umgesetzt worden, allerdings mit der nationalen Besonderheit, dass nicht nur die Tunnelbauwerke im Verlauf des transeuropäischen Straßenverkehrsnetzes, sondern alle Tunnelbauwerke mit einer Gesamtlänge von über 500m im Verlauf der österreichischen Bundesstraßen A und S erfasst sind.[23] Für alle anderen Tunnelanlagen mit einer Gesamtlänge von weniger als 500m bzw. die sich nicht im Verlauf der Bundesautobahnen und Bundesschnellstraßen befinden, gelten die einschlägigen Bestimmungen der Straßenverkehrsordnung (StVO) bezüglich der Verkehrsüberwachung.[24]

Aufgrund der nationalen Erweiterung des sachlichen Anwendungsbereiches sind in Österreich mehr Tunnelbauten durch die Vorgaben des STSG reglementiert und unterliegen somit auch dessen strengen Sicherheitsanforderungskatalog.[25] Kettenreaktionär zieht dies aufgrund des normierten Datenverarbeitungserlaubnistatbestandes zum Betrieb eines Videoüberwachungsanlage auch datenschutzrechtliche Auswirkungen (v.a. hinsichtlich Speicherdauer, Umfang der Überwachung, etc.) nach sich. Der *verba legalis* des STSG zufolge besteht grundsätzlich eine Pflicht *expressis verbis* des Straßenerhalters[26] ein solches System zur automatischen Erkennung von Verkehrsstörungen zu betreiben.[27] Die Videoüberwachungsanlage bezweckt dabei die möglichst frühzeitige und deutliche Erkennung von Gefahren und soll den Tunnel-Manager und die Einsatzdienste im Ereignisfall bei der Gefahrenbewältigung unterstützen.[28] Die Terminologie der Verkehrsstörung ist im tunnelsicherheitsrechtlichen Sinne einem weitem Verständnis zugängig und umfasst sowohl stehen gebliebene Fahrzeuge, Unfälle und sonstige unvorhersehbare (erhebliche) Ereignisse. Inwiefern sich innovative Kommunikationstechniken zur Gefahrendetektion unter diesen Tatbestand subsumieren lassen, bleibt vorerst offen.

Da ein C-ITS-basierter Informationsaustausch allerdings nicht nur auf der Datenverarbeitung mittels Videoüberwachungssystem basiert, wird der Umfang der zusätzlich erfassten Daten über das Verständnis der in der STSG normierten Bestimmung hinausgehen. Die Zulässigkeit der Verarbeitung von personenbezogenen Daten richtet sich allerdings – wie auch die Videoüberwachung selbst – nicht ausschließlich nach dem STSG, sondern nach den allgemeinen Zulässigkeitsbestimmungen des Art. 6 Abs. 1 DSGVO, weshalb für die Datenverarbeitung nicht unbedingt auf einen gesetzlichen Erlaubnistatbestand zurückgegriffen werden muss (hier kommen insbesondere auch die [Maut-]Vertragserfüllung oder überwiegende berechtigte Interessen des Verantwortlichen oder Dritter [Verkehrsteilnehmer] in Betracht). Interessant ist auch die rechtliche Beurteilung, inwiefern und ab wann ein innovative C-ITS basierte Überwachung die in der Anlage normierten Sicherheitsmaßnahmen des STSG ersetzen könnten. Dies steht auch in engem Kontext mit der Beurteilung der Erforderlichkeit der Datenverarbeitung, insbesondere wird hier die Frage der Erforderlichkeit einer Effizienzsteigerung im Detail beleuchtet werden müssen.

---

22 ErwGr. 6 Richtlinie 2004/54/EG.

23 Bundesgesetz vom 6. Juli 1960, mit dem Vorschriften über die Straßenpolizei erlassen werden (Straßenverkehrsordnung 1960 – StVO 1960) BGBl. Nr. 159/1960 i.d.F. BGBl. Nr. 154/2021.

24 Vgl. §§ 98 ff. StVO hinsichtlich der besonderen Vorschriften für die Verkehrsüberwachung mittels bildverarbeitender technischer Einrichtungen.

25 Da ohnehin auch innerstaatliche Richtlinien und Vorschriften für das Straßenwesen (RVS) zu berücksichtigen gewesen wären, sind in Österreich noch weitere Tunnelbauwerke in den Anwendungsbereich aufgenommen worden: Erläuterungen zur Regierungsvorlage: ErlRV 1328 BlgNR XXII. GP, 5.

26 In Österreich für die Bundesstraßen: ASFINAG (siehe FN 18).

27 § 4 Abs. 5 STSG.

28 § 4 Abs. 5 Z. 2 STSG.

3. Haftungsrecht und Sicherheitsanforderungen an die Tunnelbetreiber

Neben den datenschutzrechtlichen und tunnelsicherheitsrechtlichen Implikationen stellen sich auch zahlreiche haftungsrechtliche Problemstellungen. Gerade bei dem Einsatz von Software, welche sich künstlicher Intelligenz bedient – und sei sie auch noch so „schwach“[29] – stellen sich notwendigerweise auch Fragen der Haftung für etwaige entstandene Schäden, die aus dem Einsatz dieser Software resultieren. Als zentrale haftungsrechtliche Rechtsnorm für den Softwarehersteller kann dabei das Bundesgesetz für die verschuldensunabhängige Haftung für ein fehlerhaftes Produkt[30] (Produkthaftungsgesetz, PHG) herangezogen werden. Nach dem PHG haftet der Hersteller verschuldensunabhängig für jene Produkte, die im Zeitpunkt des Inverkehrbringens fehlerhaft sind und dadurch Personen verletzt oder getötet bzw. eine vom Produkt verschiedene körperliche Sache beschädigt wird. Hier ist jedoch bis heute strittig, ob bereits eine bloße Software als „Produkt“ iSd PHG zu qualifizieren ist, welches dem Wortlaut nach ausschließlich „körperliche Sachen“ umfasst.[31] Da die europäischen Vorgaben grundsätzlich keine „Körperlichkeit“ eines Produktes voraussetzen[32], wird in der Literatur vereinzelt eine Analogie unkörperlicher Sachen/Software vertreten, dies ist allerdings weiterhin sehr umstritten.[33] Subsumiert man Software unter den Produktbegriff des PHG, müsste die Reichweite der Haftung geklärt werden. Die Produkteigenschaft einer Sache geht durch den Einbau in eine andere Sache grundsätzlich nicht unter.[34] Der Teilhersteller bringt das Produkt mit Übergabe an den Endhersteller in Verkehr und könnte sohin für Schäden, die auf das Teilprodukt zurückzuführen sind und im Endprodukt eingebaut wurden, im Rahmen des PHG haftbar gemacht werden.[35] Nach stRsp[36] haftet der Teilhersteller, der nicht auch Hersteller des Endproduktes ist, für am Endprodukt verursachte Schäden jedoch nur dann, wenn der Geschädigte das Teilprodukt als selbständiges Produkt erworben hat. Dies ist (mangels vertraglicher Vereinbarung) nach der Verkehrsauffassung zu beurteilen. Inwieweit Software, die beispielsweise in einem Fahrzeug oder in der Verkehrsinfrastruktur zum Einsatz kommt, als eigenständiges Produkt zu qualifizieren ist, wurde noch nicht abschließend geklärt.

Darüber hinaus unterliegt der Hersteller einer solchen Software bereits nach allgemeiner Verschuldenshaftung einer „Produktbeobachtungspflicht“, gemäß der er das Produkt auf Gefahren hin beobachten muss und gegebenenfalls Maßnahmen zur Gefahrenabwehr zu treffen hat. Diese Produktbeobachtungspflichten leiten sich aus den Verkehrssicherungspflichten ab und stellen besondere Sorgfalts- und Einstandspflichten des Herstellers dar.[37] Aus diesen resultieren besondere Warn- und Rückrufpflichten für den Hersteller.[38]

---

29 Bei einer „schwachen KI“ wirkt diese bloß unterstützend für menschliche Handlungsträger.

30 Bundesgesetz vom 21. Jänner 1988 über die Haftung für ein fehlerhaftes Produkt (Produkthaftungsgesetz), BGBl. Nr. 99/1988 (im Folgenden „PHG“).

31 § 4 PHG: „Produkt ist jede bewegliche körperliche Sache, auch wenn sie ein Teil einer anderen beweglichen Sache oder mit einer unbeweglichen Sache verbunden worden ist, einschließlich Energie“.

32 Dazu bereits Koziol/Apathy/Koch, Haftpflichtrecht III[3], Jan Sramek, Wien 2014, S. 453 m.w.N.; für einen Überblick über die derzeitige Diskussion zur Ausweitung der Produkthaftung auf Software und KI auf europäischer Ebene siehe etwa Seehafer/Kohler, Künstliche Intelligenz: Updates für das Produkthaftungsrecht?, EuZW 2020, S. 213.

33 Hiezu siehe Zöchling-Jud, In: Reindl-Krauskopf/Grafl, Künstliche Intelligenz – Fluch oder Segen, Verlag Österreich, Wien 2020, S. 78; Posch/Terlitza In: Schwimann/Kodek (Hrsg), ABGB: Praxiskommentar VII[4], Lexis Nexis, Wien 2016, § 4 PHG, Rz. 10; Larcher, Medizinprodukte-Software: Abgrenzung und Produkthaftung, Recht der Medizin, Manz, Wien 2018, S. 133 ff; Rabl, Kommentar zum Produkthaftungsgesetz[1], Lexis Nexis, Wien 2016, § 4 PHG, Rz 52–55; Wagner, Produkthaftung für autonome Systeme, Archiv für die civilistische Praxis, Mohr Siebeck, Tübingen 2017, S. 718ff.

34 § 4 PHG.

35 Hiezu siehe Koziol/Apathy/Koch, Haftpflichtrecht III[3], Jan Sramek, Wien 2014, B Rz. 96 ff; Harnoncourt, Haftungsrechtliche Aspekte des autonomen Fahrens, ZVR, 2016/228, S. 550.

36 OGH 3. Februar 1994, 8 Ob 536/93; OGH 30. Jänner 1996, 1 Ob 555/95; OGH 30. November 2016, 7 Ob 175/16k.

37 Pyka, Zeitpunkt und Umfang der Produktbeobachtungspflicht, ÖJZ 2017, S. 588; Sosnitza, Das Internet der Dinge – Herausforderungen oder gewohntes Terrain für das Zivilrecht?, Computer und Recht, 770; Schmid, Pflicht zur „integrierten Produktbeobachtung“ für automatisierte und vernetzte Systeme, Computer und Recht, Rz 4.

38 OGH 13. September 2012, 6 Ob 215/11b; BGH 16. Dezember 2018, VI ZR 170/07, BGHZ 179, 157–168 (Pflegebetten).

Unabhängig von der Haftung des Herstellers, unterliegt selbstverständlich auch der Tunnelbetreiber Sorgfaltspflichten, die aus dem Vertrag zwischen Tunnelbetreiber und Fahrzeugnutzer resultieren, etwa dann wenn der Betreiber des Tunnels als Verkehrsinfrastrukturbetreiber ein Benützungsentgelt („Vignettenmaut") erhebt und dadurch ein Nutzungsvertrag geschlossen wird.[39] In diesem Zusammenhang wird in der Literatur diskutiert, inwieweit auch Handlungen sogenannter „technischer Gehilfen" dem Vertragspartner zugerechnet werden, wozu sich mitunter auch eine unterstützende Software zählen ließe.[40]

Aber auch außerhalb der vertraglichen Haftung, treffen den Tunnelbetreiber sogenannte „Verkehrssicherungspflichten" gegenüber den Nutzern des Tunnels. Dabei handelt es sich um eine Ausprägung der außervertraglichen Haftung, welche in diesem speziellen Fall durch § 1319a ABGB[41] eigens normiert ist. Demnach haftet der Betreiber für Personen- und Sachschäden die durch den „mangelhaften Zustand eines Weges" verursacht wurden.[42] Darunter sind auch auf dem Weg befindliche und dem Verkehr dienliche Anlagen wie Brücken und Tunnelbauwerke zu subsumieren.[43] Beurteilungsmaßstab für die Mangelhaftigkeit eines Weges sind das Verkehrsbedürfnis und die Zumutbarkeit entsprechender Maßnahmen.[44] Welche Maßnahmen ein Wegehalter im Einzelnen zu ergreifen hat, richtet sich dabei nach der Art des Weges, besonders nach seiner Widmung, seiner geografischen Situierung, das daraus resultierende Maß seiner vernünftigerweise zu erwartenden Benutzung (Verkehrsbedürfnis) und all jenes das für seine Instandhaltung angemessen und nach objektiven Maßstäben zumutbar ist.[45] Stellt ein Wegehalter die Benützung seines Weges kostenlos zur Verfügung, darf für diesen, nach der Ratio des § 1319a ABGB, die Haftung nicht überspannt werden.[46]

Betrachtet man die angeführten Sorgfaltspflichten, so zeigt sich, dass sich diese mit dem technischen Fortschritt durchaus wandeln. Der zunehmende Einsatz von C-ITS-Systemen und die zunehmende Vernetzung von Verkehrsinfrastruktur und Verkehrsteilnehmern könnten auch die Sicherheitsanforderungen an die Tunnelbauwerke ändern. Es ist durchaus denkbar, dass sich künftig auch die Bereitstellung von Informationen durch den Verkehrsinfrastrukturbetreiber an die Verkehrsteilnehmer über Road-Side-Units als Standard etabliert und entsprechende (auch normative) Erwartungen gestellt werden können. Darüber hinaus ist aber davon auszugehen, dass sich die Nutzung von Daten aus dem C-ITS für Tunnelbetreiber bereits in naher Zukunft als Sorgfaltsstandard herauskristallisiert, sollte dadurch eine Erhöhung der bzw. eine gleichwertige Tunnelsicherheit erreicht werden.[47] An dieser Stelle lediglich angemerkt sei die Frage, inwieweit sich durch die technologische Entwicklung und die zunehmende Abhängigkeit autonomer und teilautonomer Fahrzeuge auch die Haftung von Fahrzeugnutzern auf jene Akteure verschiebt, welche die Informationen bereitstellen (worunter auch der Tunnelbetreiber künftig im Bereich I2V zu zählen sein wird).[48]

---

39 Diese äußern sich in einer Beweislastumkehr für das „Verschulden" (zulasten des vermeintlichen Schädigers) und einer Zurechnung aller „Erfüllungsgehilfen" (OGH 26. April 2001, 2 Ob 133/00y; OGH 17. März 2005, 2 Ob 57/05d; OGH 29. November 2007, 2 Ob 10/07w).

40 Hiezu siehe Ondreasova, Haftung für technische Hilfsmittel de lege lata, ÖJZ, 445, 446; Koziol, Österreichisches Haftpflichtrecht II – Haftung für eigenes und fremdes Fehlverhalten, Jan Sramek, Wien 2018, S. 951; Roubik, Zivilrechtliche Haftungsfragen im Umgang mit künstlicher Intelligenz, Linde, Wien 2020, S. 31, 32; Harnoncourt, Haftungsrechtliche Aspekte des autonomen Fahrens, ZVR 2016/228, S. 546, 549.

41 § 1319a ABGB regelt die Haftung „durch einen Weg", wozu auch Straßen und Tunnelbauwerke zählen.

42 Siehe aber die Einschränkung der Haftung durch Handlungen der „Leute" des Haftpflichtigen nur bei Vorsatz oder grober Fahrlässigkeit gemäß § 1319a Abs. 3 ABGB.

43 Obermayr, Die Wegehalterhaftung gem. § 1319a ABGB unter besonderer Berücksichtigung des Einsatzes von Hilfspersonen, Manz, Wien 2019, S. 179.

44 OGH 18. November 1999, 2 Ob 314/99m; OGH 31. Jänner 2006, 1 Ob 260/05z; OGH 28. Juni 2016, 8 Ob 58/16m; OGH 19. April 2017, 6 Ob 39/17d.

45 § 1319a Abs. 2 ABGB; OGH 17. Dezember 2008, 2 Ob 115/08p.

46 OGH 8. August 2002, 2 Ob 181/02k.

47 Zum Thema „redundante" Daten, siehe oben zum Datenschutzrecht.

48 Zu diesen Fragen siehe auch Schweighofer/Zanol, Verkehrsinfrastruktur für automatisiertes Fahren und C-ITS – Rechtliche und Gesellschaftliche Aspekte, OCG, Wien 2021.

Nicht unerwähnt soll in diesem Zusammenhang der Haftungstatbestand nach der DSGVO bleiben, aufgrund dessen der Verantwortliche und der Auftragsverarbeiter[49] gemäß Art. 82 DSGVO für materielle oder immaterielle Schäden resultierend aus der Datenverarbeitung einzustehen haben.

Jedenfalls zeigt sich, dass die Implementierung neuer (auch KI gestützter) Software nicht nur unterschiedliche Haftungsregime berührt, sondern vielmehr auch, dass angesichts der gebotenen hohen Sorgfalt, der Einsatz neuer Technologien geboten sein kann, wodurch dieses Rechtsgebiet in einem wechselseitigen Spannungsverhältnis mit den übrigen (einschließlich des Datenschutzrechts) steht.

4. Ausblick

Es ist klar, dass künftig neue Technologien und Innovationen auch zur Erhöhung der Tunnelsicherheit genutzt werden und auch genutzt werden sollten. Diese erste überblicksartige Darstellung der rechtlichen Aspekte zeigt jedoch bereits auf, dass sich aus dem Zusammenspiel zwischen Haftungsrecht, rechtlichen Vorgaben zur Tunnelsicherheit und Datenschutzrecht besonders interessante rechtliche Spannungsverhältnisse ergeben, die es im Rahmen dieses und gleichgelagerter Forschungsprojekte zu lösen gilt.

Von besonderer Relevanz ist es, die für die Zweckerreichung wesentlichen Daten und Datenverarbeitungsvorgänge zu definieren. An dieser Stelle ist bereits festzuhalten, dass auch die Erhebung von „redundanten" Daten zur Plausibilisierung der übrigen Datenquellen und zur Verringerung des Risikos falscher Informationen in besonders risikointensiven Szenarien (wie sie sich auch in Tunneln stellen) durchaus zur Erhöhung der zur entsprechenden Zweckerreichung (Tunnelsicherheit) erforderlich sein kann.

Mit dem Einsatz innovativer Technologien in der Tunnelüberwachung, stellen sich auch wichtige haftungsrechtliche Fragen. Gerade in dem Bereich der Tunnelsicherheit sind hohe Erwartungen an das Ausmaß der Produkt- und Verkehrssicherungspflichten des Herstellers sowie an den vertraglich oder außervertraglich geschuldeten Zustand des Tunnels durch den Verkehrsinfrastrukturbetreiber gestellt. Geht man von einem breiten Einsatz von C-ITS Stationen in naher Zukunft aus, so kann sich daraus auch eine Pflicht zur Nutzung dieser leicht verfügbaren Informationen durch den Infrastrukturbetreiber ergeben, insbesondere dann, wenn dies zu einer erheblichen Erhöhung des Sicherheitsniveaus für die Verkehrsteilnehmer in Tunnelbauwerken führt.

5. Danksagung

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des deutschen Bundesministeriums für Bildung und Forschung (BMBF) im Rahmen der Bekanntmachung „Künstliche Intelligenz in der zivilen Sicherheitsforschung" sowie des österreichischen Bundesministeriums für Landwirtschaft, Regionen und Tourismus (BMLRT) im Rahmen des Förderungsprogramms für Sicherheitsforschung KIRAS gefördert und vom VDI Technologiezentrum sowie der Österreichischen Forschungsförderungsgesellschaft (FFG) abgewickelt.

Das Projekt wird von der Arbeitsgruppe Rechtsinformatik, Juridicum, Universität Wien, unter der Leitung von Prof. Dr. Dr. Erich Schweighofer durchgeführt. Die Autoren danken für die wesentliche Unterstützung und wichtige Hinweise.

[49] I.S.d. Art. 4 Abs. Z. 7 („Verantwortlicher") und Z. 8 („Auftragsverarbeiter") DSGVO.