EINSATZ VON KÜNSTLICHER INTELLIGENZ IN DEN TUNNELANLAGEN – WIRD TUNNELSICHERHEIT ZU EINEM RECHTLICHEN MINENFELD?

Jessica Fleisch / Jakob Zanol / Lennard Alms / Daniel Demetz / Lorenz Wickert

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

Lorenz Wickert, Wissenschaftlicher Mitarbeiter, Fraunhofer IAIS
Schloss Birlinghoven 1, 53757 Sankt Augustin, DE

Lennard Alms, Wissenschaftlicher Mitarbeiter, Fraunhofer IAIS
Schloss Birlinghoven 1, 53757 Sankt Augustin, DE

Daniel Demetz, Wissenschaftlicher Mitarbeiter/Projektleiter, Fraunhofer IAIS
Schloss Birlinghoven 1, 53757 Sankt Augustin, DE

Schlagworte: ***Tunnelsicherheit, künstliche Intelligenz, Cooperative Intelligent Transport System (C-ITS), V2I, I2V, KI-Verordnung, IRIS2023***

Abstract: *Der Einsatz von künstlicher Intelligenz in Tunnelanlagen insbesondere auch in Zusammenschau mit den Entwicklungen im Bereich der Mobilität 4.0. (v.a. C-ITS-Informationsaustausch) rückt zunehmend in den Vordergrund. Nicht nur von technischer Seite gibt es künftig noch einige Hürden zu bewältigen, sondern auch die Rechtslage de lege lata lässt einige Rechtsfragen offen. Wenig verwunderlich erscheint es deshalb, dass auf europäischer Ebene in den letzten Jahren regulatorische Instrumente vorgestellt wurden, die künftig Rechtsklarheit und -sicherheit schaffen sollen. In diesem Beitrag sollen deshalb die aktuellen Entwicklungen und die Auswirkungen auf die geplanten Vorhaben im Bereich der Tunnelsicherheit dargestellt werden.*

1. Einleitung

Bereits in den letzten Jahren hat sich gezeigt, dass technologische Entwicklungen wie der Einsatz von künstlicher Intelligenz auch in Zusammenschau mit der Mobilität 4.0 im Bereich des Tunnelsicherheitsmanagement künftig breite Anwendung finden wird und einiges an Verbesserungspotential besitzt. Vor diesem Hintergrund erscheint es deshalb zunehmend unzumutbar, sich auf ein rein sinnesorganbasiertes Monitoring menschlicher Operatoren zu verlassen. Bereits zum aktuellen Zeitpunkt werden deshalb neben konventionellen Methoden der Tunnelüberwachung auch innovativere Ansätze zur Gefahrendetektion[1] genutzt, deren Nutzungspotential

[1] In Österreich ist für den Betrieb, den Bau und die Planung (im Vergleich zu Deutschland) eine zentrale Stelle verantwortlich. Als Tunnelmanager nach dem STSG ist die ASFINAG ernannt, die derzeit 9 Tunnelleitzentralen in Österreich betreibt und insgesamt 169 Tunnelanlagen überwacht. Die ASFINAG setzt unterschiedliche Überwachungssysteme ein. Ein Beispiel für eine innovativere Überwachungsmethode ist das System „AKUT“. AKUT ist ein System, dass akustisch auffällige Geräusche (u.a. Reifenplatzer) in

allerdings bedingt durch den (noch) beschränkten infrastrukturellen Ausbau, der allgemeinen Architektur des Mobilitätsektors und dem Stand der Technik an sich noch nicht vollumfänglich erreicht worden ist.

Das bestehende Tunnelmanagement der letzten Jahre bestätigt zwar, dass in den Tunnelanlagen mittlerweile ein hohes Maß an Sicherheit besteht, allerdings scheinen gewisse Abläufe zur Gefahrendetektion stark verbesserungsbedürftig zu sein. Insbesondere die menschlichen Operatoren, die in den Tunnelleitzentralen als zentrale Überwachungsstelle der 169 Tunnelanlagen in Österreich fungieren, sind einem enormen Handlungs- und Leistungsdruck ausgesetzt. Eine Entlastung durch technische Hilfsmittel wäre wünschenswert, um sowohl den Operatoren ihre Monitoring-Arbeit zu erleichtern und somit menschliche Fehler zu reduzieren als auch die Tunnelsicherheit noch weiter zu steigern (v.a. die Sicherheit der Verkehrsteilnehmer und den Schutz der Tunnelbauwerksubstanz).

Die künftigen Methoden der Gefahrendetektion im Bereich des Tunnelmanagements könnten sich mit dem Ausbau eines vernetzten Verkehrs insbesondere dem flächendeckenden Einsatz von kooperativen intelligenten Verkehrssystemen (*„Cooperative Intelligent Transport System", kurz: „C-ITS"*) nachhaltig verändern. C-ITS bezeichnet einen umfassenden automatisierten multidirektionalen Informationsaustausch basierend insbesondere auf (teil)standardisierten Nachrichten[2] (wie beispielsweise: „Cooperative Awareness Messages"[3]; kurz: „CAM" oder „Decentralized Enviromental Notification Messages"[4]; kurz: „DENM"), der sowohl zwischen den einzelnen Verkehrsteilnehmern („Vehicle-to-Vehicle"; kurz: „V2V") als auch der Infrastrukturkomponenten („Vehicle-to-Infrastructure"; kurz: „V2I" oder „I2V") stattfinden soll. Die Informationen sollen dabei direkt und in Echtzeit aus dem Verkehrsfluss übertragen werden und könnten auch für weitere Systeme und somit weitere Anwendungsmöglichkeiten zur Verfügung gestellt werden. Diese stetig wachsende Verfügbarkeit von Daten[5] hat in den letzten Jahren zu einer revolutionären Entwicklung und Anwendung von KI-Modellen geführt und somit weitreichende Auswirkungen auf alle Aspekte unseres täglichen Lebens.

Auch in der Forschung hat man die Bedeutung dieser Technologie und die aktuelle tunnelsicherheitsspezifische Problematik erkannt und verfolgt im Rahmen des kooperationsübergreifenden FFG KIRAS Projektes „Künstliche Intelligenz zur Verbesserung der Sicherheit von Tunneln und Tunnelleitzentralen (kurz: „KITT")" den Ansatz, ein auf künstlicher Intelligenz basierendes System zu konzipieren, das künftig gewisse Ereignisszenarien aus dem C-ITS-Informationsfluss in Echtzeit ableiten und dem menschlichen Operator präzise Handlungsanweisungen vorschlagen soll.

Die endgültige Letztentscheidung soll auch beim Einsatz dieses neuartigen Systems weiterhin bei den menschlichen Operatoren in den jeweils tätigen Tunnelleitzentralen verbleiben (etwa, ob und auch welche Maßnahmen schlussendlich zur Gefahrenreduktion oder idealerweise -vermeidung eingeleitet werden sollen). Das sogenannte „KITT-System" wird als „*add-on*" lediglich zusätzliche Informationen für die Bewertung von Ereignisszenarien aufbereiten und soll somit die Entscheidungsfindung der Operatoren erleichtern und auch zur wesentlichen Reduktion deren Handlungs- und Leistungsdruck beitragen.

Das bisherige Sicherheitskonzept in den Tunnelanlagen soll demnach an die rasant fortschreitenden technologischen Entwicklungen angepasst werden, stets von der Prämisse geleitet, die Verkehrssicherheit weiter zu verbessern. Mit der durch die europäische Mindestharmonisierung[6] aus dem Jahr 2004 ist der erste regulato-

---

den Tunnelanlagen detektiert und dies an den Tunneloperator in der Tunnelleitzentrale meldet. Es besteht allerdings keine gesetzliche Verpflichtung zur Implementierung solcher Systeme.

2 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.

3 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.

4 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.

5 Nicht nur im Bereich des Mobilitätssektors.

6 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; Die Europäische Richtlinie wurde in Österreich in dem Straßentun-

rische Eckpfeiler und somit eine einheitliche Grundlage für ein adäquates Sicherheitsniveau in den Tunnelanlagen im Verlauf des transeuropäischen Verkehrsnetzes geschaffen worden. Es ist allerdings nicht zu leugnen, dass die Europäische Tunnelsicherheits-Richtlinie zunehmend veraltet erscheint, insbesondere in Hinblick auf den normierten Sicherheitsmaßnahmenkatalog,[7] der die technisch möglichen Methoden zur Gefahrenreduktion und -vermeidung nicht ansatzweise ausschöpft. Die in der Richtlinie vorgesehenen Sicherheitsmaßnahmen betreffen überwiegend architektonische und ausstattungsbezogene Vorgaben.

Hinsichtlich technischer Überwachungsmaßnahmen sieht die Richtlinie und auch die österreichische Umsetzung im Straßentunnelsicherheitsgesetz (STSG)[8] lediglich den Betrieb eines Videoüberwachungs- und Videodetektionssystems vor. Aufgrund der Fehleranfälligkeit dieser Systeme[9] wird dieser Methode zur Gefahrendetektion in der Praxis allerdings lediglich eine marginale Bedeutung zugeschrieben. Die meisten innovativeren Systeme, die bereits heute von der ASFINAG[10] betrieben werden, werden aus eigenem Antrieb (d.h. in Wahrnehmung der eigenen gehobenen Sorgfaltspflicht gegenüber den Verkehrsteilnehmern), ohne ausdrückliche rechtliche Verpflichtung eingesetzt[11]

Hinzu kommt, dass der Einsatz von künstlicher Intelligenz im Bereich der Tunnelsicherheit eine Fülle an unbeantworteten Rechtsfragen aufwirft. Aufgrund der noch weitgehend unklaren Rechtslage *de lege lata*, ergeben sich zahlreiche offene Rechtsfragen, die dringend zu klären sind.[12] Auch die aktuellen Entwicklungen auf europäischer Ebene *de lege ferenda* müssen vor diesem Hintergrund bereits jetzt in der juristischen Analyse des Projektvorhabens Berücksichtigung finden.

In diesem Beitrag sollen dementsprechend die spezifischen rechtlichen Problemstellungen, die sich durch den Einsatz von künstlicher Intelligenz im Bereich der Tunnelsicherheit ergeben, aufgezeigt, sowie die sich künftig ändernde Rechtslage mit besonderen Blick auf den bereits von der EU-Kommission vorgeschlagenen Entwurf zur Regulierung von Künstlicher Intelligenz berücksichtigt werden.

2. Funktion der KI in KITT

Innerhalb der C-ITS-Infrastruktur werden unterschiedliche teil(standardisierte) Nachrichten zwischen Verkehrsteilnehmer und Infrastrukturkomponenten ausgetauscht.

Wie oben bereits erwähnt, werden CAM-Nachrichten beispielsweise als „Puls"-Nachrichten, von jedem entsprechend konfigurierten Fahrzeug regelmäßig an alle in unmittelbarer Umgebung befindlichen Fahrzeuge und Infrastrukturkomponenten gesendet, um Informationen über Anwesenheit, Position und den grundlegenden Status[13] zu übertragen. Zusätzlich enthalten sie auch Informationen über das Fahrverhalten eines

nel-Sicherheitsgesetz (STSG) umgesetzt: Bundesgesetz über die Sicherheit von Straßentunneln (Straßentunnel-Sicherheitsgesetz – STSG), BGBl. I Nr. 54/2006 i.d.F. 96/2013.

7 Als Anhang auch im STSG zu finden.

8 Vgl. § 4 (5) STSG.

9 Im Zuge des Projektes KITT sind bereits Experteninterviews durchgeführt worden. Die Fehlalarmquote der Videodetektion wurde von den Experten als hoch eingestuft. Am weitesten verbreitet sind aufgrund der geringeren Fehlalarmquoten die Meldungen hinsichtlich Falschfahrererkennung und Meldung hinsichtlich liegengebliebener Fahrzeuge.

10 Die „Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft" (ASFINAG) betreibt die Straßeninfrastruktur für den überwiegenden Teil der Autobahnen und Schnellstraßen (einschließlich der zugehörigen Tunnel) in Österreich, https://www.asfinag.at/verkehr-sicherheit/.

11 Teilweise erfolgt der Einsatz innovativerer Methoden aus eigenem Antrieb, teilweise ist deren Einsatz auch durch die zwar gesetzlich nicht bindenden, aber freiwillig anerkannten österreichischen Richtlinien und Vorschriften für das Straßenwesen (kurz: „RVS") vorgegeben.

12 Rechtliche Problemfelder wurden bereits bei der IRIS2022 angesprochen. Siehe dazu: Fleisch/Geidel/Zanol, in Schweighofer/Saarenpää/Eder/Zanol/Schmautzer/Kummer/Hanke (Hrsg.) IRIS 2022 – Recht DIGITAl – 25 Jahre IRIS, Tunnelsicherheit: Rechtsfragen zum Einsatz von C-ITS und künstlicher Intelligenz, 40–49.

13 Vgl. SANTA, Vehicle-to-Infrastructure Messaging Proposal Based on CAM/DENM Specifications. Wireless Days (WD). DOI:10.1109/WD.2013.6686514.

Fahrzeuges wie Geschwindigkeit, Fahrtrichtung, Beschleunigung usw. Die CAM-Nachrichten werden im regelmäßigen Abstand von maximal einer Sekunde gesendet und somit an ihre Umgebung „gebroadcastet“.[14]

Innerhalb des C-ITS-Informationsaustausches können auch DENM-Nachrichten übertragen werden. DENM-Nachrichten sind ereignisausgelöste Meldungen, die gesendet werden, um Verkehrsteilnehmer vor einem gefährlichen Ereignis zu warnen.[15] Es handelt sich dabei um eindeutige Nachrichten, die auf ein bestimmtes, schon eingetretenes Ereignis oder auf eine akute Gefahrensituation hinweisen.

Während CAM-Nachrichten primär für die Kommunikation von Fahrzeugen untereinander verwendet werden sollen z.B. im Bereich des autonomen Fahrens, bedarf es für die laufende Verkehrsüberwachung und akkurate Lagebeurteilung in Tunneln weitergehender Analysemethoden. Hierbei bieten sich vor allem moderne Methoden der künstlichen Intelligenz an, die große Mengen an Echtzeitinformationen aus dem Verkehrsfluss effektiv und rasant verarbeiten können. Allerdings bringt die Gefahrenanalyse durch eine KI basierend auf DENM-Nachrichten keinen direkten Mehrwert für die Ereignisdetektion als solche, da sich diese Meldungen in der Regel lediglich auf ein bereits eingetretenes Ereignis beziehen. Diese Informationen können allerdings für Validierung und Bestätigung der Gefahrendetektion durch die KI aus den CAM-Nachrichten nützlich sein.

Moderne KI-Methoden werden in verschiedenen Bereichen bereits effektiv für die Anomalieerkennung verwendet. Da es sich bei den vom KITT-System zu detektierenden Risikosituationen und Verkehrsereignissen um seltene Ereignisse handelt, können diese als „Anomalien“ bezeichnet werden. Konkret bedeutet dies nun zum einen, dass das KITT-System den stetigen Verkehrsfluss mittels der oben erwähnten CAM-Nachrichten auf solche Anomalien untersucht und zum anderen kann die KI zusätzlich analysieren, ob die CAM-Nachrichten selbst durch Cyber-Angriffe manipuliert wurden.

Die KI übernimmt somit in KITT zwei zentrale Kernaufgaben:

1.) Konkret sind Anomalien im ersten Anwendungsfall als CAM-Nachrichten definiert, die Informationen über eine **gefährliche Verkehrssituation im Tunnel** enthalten, und somit eine Situation beschreiben, die sich vom Normalverhalten im Tunnel unterscheidet. Dabei soll die KI nicht die konventionellen Systeme ersetzen, sondern die neu verfügbaren C-ITS Informationen nutzen und den Tunneloperator in seinen Entscheidungen mit diesen zusätzlichen Informationen unterstützen. So kann die KI die Wahrscheinlichkeit für das Eintreten eins Unfallereignisses berechnen, welche in einer nachgeschalteten Echtzeitrisikoanalyse zu konkreten Handlungsempfehlungen übersetzt werden kann. Zusätzlich erlaubt die Detektionen von verschiedenen Risikosituationen die Einleitung von in den Alarm- und Gefahrenabwehrpläne (kurz „AGAP“)[16] definierten Präventivmaßnahmen.
2.) Im zweiten Anwendungsfall soll durch die Erkennung von **Cyber-Attacken mittels C-ITS Nachrichten**, verhindert werden, dass die Situationswahrnehmung des menschlichen Operators manipuliert wird, wodurch falsche, potenziell gefährliche Maßnahmen ausgelöst werden könnten. Auch solche Cyber-Attacken können häufig als Anomalien erkannt werden, da die empfangenen Nachrichten vom Normalverhalten abweichen.

Zusammenfassend schließt sich aus der obigen Beschreibung, dass eine Gefahrendetektion durch die Analyse von CAM-Nachrichten mithilfe von KI-Methoden zu einer Verbesserung der Situationsbewertung der menschlichen Operatoren beitragen kann. Diese Situationsbewertung kann durch die Aufbereitung von DENM-Nachrichten ergänzt werden. Da die Durchdringungsrate von C-ITS Technologien im Straßenverkehr allerdings auch noch in naher Zukunft sehr gering sein wird, ist zu erwarten, dass viele Ereignisse und Ge-

[14] Sollten sich Parameter schneller ändern, werden CAMs in noch kürzeren Zeitintervallen gesendet.

[15] Vgl. SANTA, Vehicle-to-Infrastructure Messaging Proposal Based on CAM/DENM Specifications. Wireless Days (WD). DOI:10.1109/WD.2013.6686514.

[16] Alarm- und Gefahrenabwehrpläne dokumentieren das Vorgehen im Falles eines Störfalls für Betriebsbereiche oder Anlagen, die den erweiterten Pflichten der Störfall-Verordnung unterliegen, wie z.B. Tunneln.

fahrensituationen nicht direkt aus den DENM-Nachrichten detektiert werden können. Daher wird der Fokus auf der Auswertung der CAM-Nachrichten liegen.

3. Vorschlag der EU-Kommission zur Regulierung von Künstlicher Intelligenz

Hinsichtlich der rechtlichen Beurteilung stellt sich die Frage, welche regulativen Anforderungen ein KI-System erfüllen muss, um in der Europäischen Union zulässig zu sein. Nach geltender Rechtslage sind vor allem datenschutzrechtliche Implikationen ausschlaggebend, die jedoch für die Regulierung von KI-Systeme als solche eher ephemer erscheinen und somit nur bedingt geeignet sind.[17]

Im Juni 2021 legte die EU-Kommission deshalb den weltweit ersten Verordnungsentwurf zur Regulierung von künstlicher Intelligenz vor.[18] Die Europäische Union will mit diesem durchaus prestigeträchtigen Regulierungsvorhaben eine weltweit führende Rolle im Umgang mit KI einnehmen und einen regulatorischen Kompromiss zwischen Innovationsförderung und Grundrechtsschutz finden. Mit dieser irreführend als „KI-Gesetz" titulierten europäischen Verordnung[19] sollen europaweite einheitliche Mindestanforderungen geschaffen werden, die zum einen die Förderung der Entwicklung, die Verwendung und Dissemination von KI gewährleisten und zum anderen die Funktionalität des Binnenmarktes durch einen vertrauenswürdigen, einheitlichen und sicheren Rechtsrahmen stärken soll.[20]

3.1. Anwendungsbereich: KI-Verordnung

Die KI-Verordnung verfolgt grundsätzlich einen horizontalen und risikobasierten Regulierungsansatz und soll für alle Anbieter, die in der Union ein KI-System in Verkehr bringen oder in Betrieb nehmen, für alle Nutzer, die sich in der Union befinden und für alle Anbieter und Nutzer, die zwar in einem Drittland ansässig sind, aber das vom System hervorgebrachte Ergebnis in der Union verwendet werden soll, anwendbar sein.[21] Somit entfaltet die KI-Verordnung exterritoriale Wirkung und zeichnet sich durch einen äußerst weit formulierten Anwendungsbereich aus, der unglücklicherweise auch aufgrund der breitgefächerten Definition von KI selbst einige Unklarheiten mit sich bringt. Der Definitionsversuch[22] von künstlicher Intelligenz sorgt aufgrund seiner unscharfen und weitreichenden Formulierung bereits jetzt für Abgrenzungsschwierigkeiten.[23] Schließlich soll künftig beinahe jegliche Art von Software von der KI-Verordnung umfasst werden.[24]

---

17 Die Europäische Datenschutz-Grundverordnung (DSGVO) regelt die Verarbeitung von personenbezogenen Daten. KI-spezifische Probleme werden durch den Datenschutzrechtrahmen nur am Rande mitreguliert, allerdings legt die DSGVO keine konkreten Anforderungen an die KI selbst fest. Lediglich in Art. 24 ff DSGVO lassen sich Ansätze erkennen, die allerdings vorzugsweise auf die Datenverarbeitung selbst abzielen und nicht auf ein KI-System als solches.

18 Verordnung (EU) des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final vom 21.04.2021.

19 Als europäische Verordnung ist diese selbstverständlich ein „Rechtsakt" (vgl AI-Act); die Bezeichnung als „Gesetz" impliziert jedoch eine „Bundesstaatlichkeit" der Europäischen Union, die jedoch weder im faktischen (Stichwort „Brexit"; jüngere Rspr des VfGH) noch den rechtlichen Vorgaben entspricht: daher wird in weiterer Folge die Bezeichnung „KI-Verordnung" (oder schlicht der „Verordnungsentwurf") verwendet.

20 Vgl. ErwGr 1 und 5 des Verordnungsentwurfes.

21 Art. 2 (1) des Verordnungsentwurfes.

22 Art. 3 (1) Z1 legt fest, dass ein KI-System „*eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren*" ist. In Anhang I werde zusätzlich Techniken und Konzepte der KI genannt, die von der Definition KI mitumfasst sein sollen.

23 Steege, Definition von Künstlicher Intelligenz in Art. 3 Nr 1. KI-VO-E, MMR 2022, 926 (927 ff).

24 Ausführliche Erläuterungen hinsichtlich des (sehr weit definierten) KI-Begriffes siehe: Zanol/Buchelt/Tjoa/Kieseberg, in Schweighofer/Saarenpää/Eder/Zanol/Schmautzer/Kummer/Hanke (Hrsg.) IRIS 2022 – Recht DIGITAL – 25 Jahre IRIS, What is „AI"? Exploring the scope of the „Artificial Intelligence Act", 25–32.

3.2. Vier Risikokategorien für den Einsatz von KI

Unzweifelhaft mag der weite Anwendungsbereich auf den ersten Blick verwunderlich erscheinen, allerdings muss berücksichtigt werden, dass – sollte der Anwendungsbereich eröffnet sein – durch die regulatorische Umsetzung eines risikobasierten Ansatzes den rechtlichen Anforderungen an ein KI-System Grenzen gesetzt werden.

Nach Steege stellt der risikobasierte Ansatz allerdings kein umfassendes restriktives Korrektiv zum weiten Anwendungsbereich dar, da Unternehmen mangels trennscharfer Unterscheidung von KI und herkömmlicher Software künftig unter den sachlichen Anwendungsbereich der KI-VO fallen werden und der risikobasierte Ansatz schließlich erst nach Eröffnung des Anwendungsbereich zum Greifen kommt. Unternehmen entsteht somit ungeachtet dessen ein beachtlicher Mehraufwand, da sie im ersten Schritt prüfen müssen, ob ihre Software vom KI-Begriff der KI-VO umfasst ist und dann im zweiten Schritt beurteilen müssen unter welche Risikokategorie ihr System fällt.[25]

Denn aufgrund des gewählten Regulierungsansatzes der KI-VO sollen KI-Systeme nicht in jedem Anwendungsfall in allumfassender Detailtiefe reguliert werden, sondern abhängig von ihrer Einordnung in die vier verschiedenen Risikokategorien (KI-System mit geringem, minimalen, hohen oder unannehmbaren Risiko) unterschiedlichen gesetzlichen Anforderungen unterliegen.

Wohingegen KI-Systeme mit minimalen und geringen Risiko kaum bis gar keiner Regulierung unterliegen werden, werden sogenannte KI-Systeme mit unannehmbaren oder hohen Risiko[26] künftig einem umfassenden Anforderungskatalog (Hochrisiko-KI-Systeme) entsprechen müssen bzw. einem weitgehenden Verbot (KI-Systeme mit unannehmbaren Risiko) unterliegen.[27]

3.2.1. Einsatz von Hochrisiko-KI-Systeme im Betrieb kritischer Infrastrukturen

Art. 6 des Verordnungsentwurfes regelt die Klassifizierungsvorschriften von Hochrisiko-KI-Systemen und sieht grundsätzlich zwei unterschiedliche Kategorien von Hochrisiko-KI-Systemen vor. Art. 6 Abs. 1 des Verordnungsentwurfes sieht solche KI-Systeme als hochriskant, die als Sicherheitskomponenten von Produkten verwendet werden sollen, die unionsrechtlichen Harmonisierungsvorschriften unterliegen.[28]

Art. 6 Abs. 2 des Verordnungsentwurfes verweist auf den Anhang III der geplanten KI-Verordnung und normiert, dass auch sonstige eigenständige KI-Systeme in den dort ausdrücklich angeführten Bereichen als hochriskant gelten. Für jeden der insgesamt acht Bereichen[29] sind zusätzliche Bedingungen erlassen worden.

Als Punkt 2 führt Anhang III den Bereich „Verwaltung und Betrieb kritischer Infrastrukturen“ an und definiert weiters, dass „*KI-Systeme, die bestimmungsgemäß als Sicherheitskomponenten in der Verwaltung und im Betrieb des Straßenverkehrs sowie in der Wasser-, Gas-, Wärme- und Stromversorgung verwendet werden sollen*“ als hochriskant gelten. Zudem wird im Verordnungsentwurf selbst angeführt, dass solche Systeme deshalb als hochriskant gelten sollten, da „*ihr Ausfall oder Störung in großem Umfang das Leben und die Gesundheit von Menschen gefährden und zu erheblichen Störungen bei der normalen Durchführung sozialer*

---

25 Siehe Fn. 23.

26 Siehe auch Art. 5 des Verordnungsentwurfes „Verbotene KI-Praktiken“.

27 Allerdings wirft die Einstufung des System in die Risikokategorien aufgrund zahlreicher unbestimmter Gesetzesbegriffe einige Probleme auf.

28 Siehe insbesondere Anhang II des KI-VO-E; Darunter fällt beispielsweise Spielzeug, Aufzüge, Sportboote und Wassermotorräder, etc.

29 Laut Anhang III der vorgeschlagenen KI-Verordnung sind folgende Bereiche mitumfasst: Biometrische Identifizierung und Kategorisierung natürlicher Personen; Verwaltung und Betrieb kritischer Infrastrukturen; Allgemeine und berufliche Bildung; Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit; Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen; Strafverfolgung; Migration, Asyl und Grenzkontrolle; Rechtspflege und demokratische Prozesse (Stand: November 2022).

und wirtschaftlicher Tätigkeit führen kann".[30] Der zweite Anwendungsfall von Hochrisiko-KI-Systeme könnte insbesondere für KITT interessant sein und gilt dementsprechend zu prüfen.

3.3. Einstufung von KITT als hochriskant?

Im Zusammenhang mit KITT stellt sich die Frage, ob der Einsatz von künstlicher Intelligenz zur Gefahrendetektion insbesondere deren bestimmungsgemäßen Gebrauch als „add-on" vom Verordnungsentwurf insbesondere von der Klassifizierung als Hochrisiko-KI-System umfasst wird und wenn dies zu bejahen sein sollte, welche rechtlichen Anforderungen zu berücksichtigen sind.

Sollte KITT als hochriskant einzustufen sein, müsste das KI-System dem umfassenden Maßnahmenkatalog[31] und somit dem Herzstück der KI-Verordnung entsprechen. Das würde einen zusätzlichen monetären und organisatorischen Aufwand nach sich ziehen, dem bestenfalls durch die Berücksichtigung der geplanten rechtlichen Regulierung mit der Arbeit aus diesem Projekt entgegengesteuert werden kann.

3.3.1. Das KITT-System als Sicherheitskomponente in der Verwaltung und im Betrieb des Straßenverkehrs?

Tunnelanlagen sind Teil der Infrastrukturkomponenten der Straßenverkehrsinfrastruktur,[32] weshalb der Einsatz von KITT zur Verbesserung der Tunnelsicherheit zur Verwaltung und Betrieb des Straßenverkehrs zugeordnet werden kann.

Als nächster Prüfungsschritt gilt zu klären, ob KITT bestimmungsgemäß als Sicherheitskomponente eingesetzt werden soll. Als Sicherheitskomponente wird ein „*Bestandteil eines Produkts oder Systems, der eine Sicherheitsfunktion für dieses Produkt oder System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Sachen gefährdet*" angesehen.[33]

Die in KITT eingesetzte KI soll durch die Detektion ausgewählter Ereignisszenarien zur Verbesserung der Tunnelsicherheit beitragen, indem die menschlichen Operatoren in ihrer Monitoring-Tätigkeit unterstützt werden. Zusätzlich soll die KI auch manipulierte CAM-Nachrichten erkennen und somit potentielle Cyber-Angriffe abwehren. Anzumerken ist allerdings, dass KITT lediglich als technisches Hilfsmittel zu bereits bestehenden Prozessen angedacht ist, weshalb die KI keine eigenständigen Entscheidungen trifft, die unmittelbar zur Einleitung entsprechender Maßnahmen (beispielsweise Tunnelschließung) führt. Der menschliche Operator soll lediglich in seiner Entscheidungsfindung unterstützt werden und somit zielgerichteter und vor allem mit entsprechenden Geschwindigkeitsvorteil[34] entsprechende Sicherheitsmaßnahmen zur Gefahrenreduktion oder -vermeidung einleiten.

Es ist deshalb auch eher anzuzweifeln, dass bei etwaiger Störung oder Ausfall von KITT eine Gefährdung der Gesundheit und Sicherheit der Verkehrsteilnehmer oder der Tunnelsubstanz zumindest im ersten Anwendungsfall von KITT zu erwarten ist, da im Normalfall ein umfassendes Monitoring durch die Operatoren aufrechterhalten werden kann.

Zusätzlich könnte im zweiten Anwendungsfall auch diskutiert werden, dass der Ausfall oder die Störung von KITT künftig in einem hochautomatisierten Verkehr eine gewisse Sicherheitsgefährdung nach sich ziehen

30 Siehe Erwägungsrund 34 des Verordnungsentwurfes.
31 Kapitel II des Verordnungsentwurfes.
32 Art. 17 der Verordnung (EU) Nr. 1315/2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU, L 348/1.
33 Art. 3 (1) Z14 des Verordnungsentwurfes.
34 Die Einleitung von Sicherheitsmaßnahmen sind äußerst zeitkritisch und können im schlimmsten Fall über Leben oder Tod entscheiden.

kann, sollten manipulierte CAM-Nachrichten im Bereich der Tunnelsicherheit nicht erkannt werden.[35] Auch wurde im Projektkonsortium bereits von den Praktikern angemerkt, dass die menschlichen Operatoren in den Tunnelleitzentralen zwar äußerst routiniert und erfahren (teilweise mehr als zwanzig Jahre Berufserfahrung) sind, allerdings überwiegend nicht das technische Verständnis besitzen Störungen des C-ITS-Informationsaustausches oder des KITT-Systems adäquat nachzuvollziehen, geschweige denn in der Lage sind, solche Störungen oder Ausfälle zu beseitigen. Zusätzlich darf auch nicht außer Acht gelassen werden, dass die Implementierung solcher Hilfssystemen in der Praxis dazu führen kann, dass gerade Systemen mit geringer Fehlalarmquote äußerst viel Vertrauen entgegengebracht wird und die Operatoren einem „*automation bias*“[36] unterliegen könnten.

4. Ausblick

Für das Projekt ergeben sich durch das umfassende Regulierungsvorhaben zahlreiche interessante Rechtsfragen, die bestenfalls bereits im jetzigen Projektstand Berücksichtigung finden müssen. Von rechtlicher Seite ist schließlich ausdrücklich festzuhalten, dass die Einstufung von KITT als hochriskant nicht zur Folge hat, dass KITT rechtlich unzulässig ist. Die Einstufung als Hochrisiko-KI-System bedingt lediglich, dass KITT den rechtlichen Anforderungen des Kapitel II des geplanten Verordnungsentwurfes zu entsprechen hat.

KITT würde zwar als potenziell hochriskant gelten, dieses Risiko soll allerdings durch die Implementierung der normierten Maßnahmen auf ein annehmbares Maß reduziert werden, sodass der Einsatz von KITT in der Europäischen Union auch in Zukunft zulässig wäre. Unzweifelhaft bedeutet die Einordnung von KITT als Hochrisiko-KI-System einen nicht unbeachtlichen Mehraufwand für die Unternehmen, aber auch für die Softwareentwickler.

Aufgrund der oben dargestellten Problematik und der Fülle an unbestimmten bzw. unzureichend konkretisierten Rechtsbegriffen der KI-Verordnung ist zu erwarten, dass die KI-Verordnung – ähnlich dem Modell der DSGVO – künftig nur parallel mit Judikatur und Leitlinien lesbar sein wird. Für Rechtsunterworfene würde dies nicht die erhoffte Rechtsicherheit erbringen, die doch in einem so durchdringlichen und wichtigen Regulierungsbereich wünschenswert wäre.

5. Fördergeber

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.

[35] Wie auch die traurigen Ereignisse (Mont-Blanc-Tunnel 1999) der Vergangenheit bestätigen, fordern Unfälle im Bereich der Tunnelanlagen nicht nur eine hohe Anzahl an Verkehrstoten, sondern ziehen auch erheblich monetären Aufwand nach sich.

[36] Unbewusster, einer neuen Technologie vielfach zugedachter Vertrauensvorschuss (*bias* = ein Trugschluss).