Datenteilen unter der Technischen Aufsicht

Maria Walch

Institut für deutsches und europäisches Gesellschafts- und Wirtschaftsrecht
Universität Heidelberg

Datenteilen

Die technische Aufsicht, insbesondere iSd Art. 14 KI-VO sowie zB § 1d III StVG, kann als ein Element der Risikoregulierung (unüberwacht lernender) KI-Modelle und des damit notwendigerweise einhergehenden Datenteilens gesehen werden.

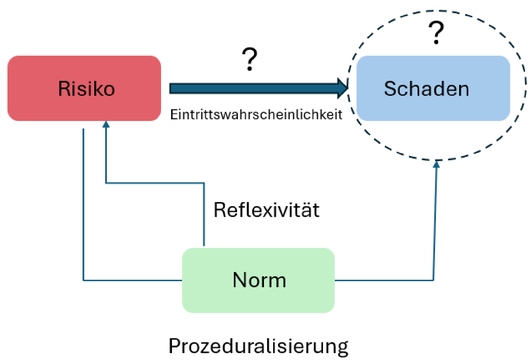

Figure 1. Risikoregulierung als normativer Umgang mit ungewissen Risiken, gekennzeichnet durch Prozeduralisierung, Akteurseinbindung und Reflexivität.

Risikoregulierung bezeichnet den normativen Umgang mit Risiken, deren Eintrittswahrscheinlichkeit und mögliche Schadensfolgen ungewiss sind. Sie ist durch eine starke Prozeduralisierung und die Einbindung verschiedener Akteure gekennzeichnet. Wesentlich ist zudem eine kontinuierliche Reflexivität, die gewährleistet, dass unbestimmte Rechtsbegriffe stets im Einklang mit gesellschaftlichen und technologischen Entwicklungen angewendet werden.

Menschliche Aufsicht zur Risikominimierung

Risikoregulierung soll zu einer ausgewogenen Abwägung von Chancen und Risiken einer Technologie führen. Die menschliche Aufsicht nach Art. 14 KI-VO muss dabei insbesondere folgende Anforderungen erfüllen:

- **Möglichkeit**: effektive Eingriffsmöglichkeit während der Anwendung des KI-Systems.
- **Wirksamkeit**: tatsächliche Vermeidung und Minimierung von Risiken.
- **Angemessenheit**: Verhältnis der Aufsichtsmaßnahmen zu den jeweiligen Risiken.

Menschliche Aufsicht und Risiken

Das Konzept einer menschlichen Überwachung zur Kontrolle technologischer Risiken findet sich zB. in:

- **Kernenergie:** Restrisiko und Überwachung, §§ 7, 19ff. AtG.
- **Lebensmittel:** Überwachung und Proben, Art. 137, 138 VO (EU) 2017/625; § 39ff. LFGB.
- **Medizinprodukte:** Klinische Studien und Produktbeobachtung, Art. 10, 15, 83 ff. VO (EU) 2017/745; §§ 30ff., 62ff. MPDG.
- **Arzneimittelrecht:** Prüfungs- und Zulassungsverfahren sowie Vigilanz, VO (EU) 536/2014; VO (EG) Nr. 726/2004; RL 2001/83/EG; AMG; §§ 40ff., 21ff. 62ff. AMG.

Dies verdeutlicht, dass die menschliche Aufsicht nach KI-VO und StVG – verstanden als Modell dauerhafter menschlicher Präsenz – im Risikoregulierungrecht einen systematischen Fremdkörper bildet.

Technische Aufsicht

KI-Systeme im automotiven Bereich, insbesondere in autonomen Fahrzeugen, sind Hochrisiko-KI-Systeme iSd KI-VO (Köllner 2025).

Figure 2. Ohne (unüberwacht lernende) KI ist autonomes Fahren nicht möglich (Zhang et al. 2024; Fraunhofer-Institut für Experimentelles Software Engineering (IESE) 2025). Eine Vielzahl an Daten müssen in Echtzeit verarbeitet werden um die Fahraufgabe zu bewältigen.

Technische Aufsicht nach dem StVG

Nach § 1d III StVG iVm § 14 AFGBV ist die technische Aufsicht eine natürliche Person mit technischer Ausbildung, welche in gesetzlich geregelten Situationen in den autonomen Fahrprozess eingreifen können soll. Dies setzt voraus, dass die technische Aufsicht in der Lage ist, die mit einem autonomen Fahrkonzept verknüpften immensen Datenströme in Echtzeit zu erfassen und zu interpretieren. Dies ist zum einen praktisch nicht durchführbar (Holzinger, Zatloukal, and Müller 2025), zum anderen aber auch aus psychologischen Gesichtspunkten riskant (**automation bias**, Laux and Ruschemeier 2025, **weitere Problempunkte** in Sayles 2024).

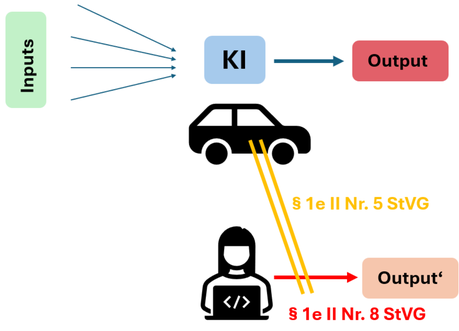

Figure 3. Die notwendig in einem autonomen Fahrzeug implementierte KI verarbeitet vorhandene Inputs zu einem Output (i.e. einem Fahrmanöver). Die technische Aufsicht soll in Echtzeit den Output der KI überschreiben können, jedoch verbleibt nach § 1e II Nr. 5 StVG die abschließende Risiken- und Folgenabschätzung bei der KI.

Die Einbindung einer menschlichen Kontrollinstanz als *intervenierende Instanz* im KI-Fahralgorithmus führt zu rechtlichen Friktionen.

Ist ein Fahrmanöver nach § 1e Abs. 2 Nr. 5 StVG fortzusetzen, selbst wenn dies dem Eingreifen der Passagiere oder der technischen Aufsicht widerspricht, sofern das KI-System autonom erkennt, dass dies die dem Schutz der betroffenen Rechtsgüter bestmöglich dienende Handlung darstellt?

Technische Nach-Sicht

Wir schlagen vor, die technische Aufsicht konform zu bereits bestehenden Risikoregulierungsansätzen an einer Stelle anzusetzen, an welcher diese auch tatsächlich dem Gesetzeszweck dienen kann, ohne dabei die Anwendung der Technologie komplett zu verhindern.

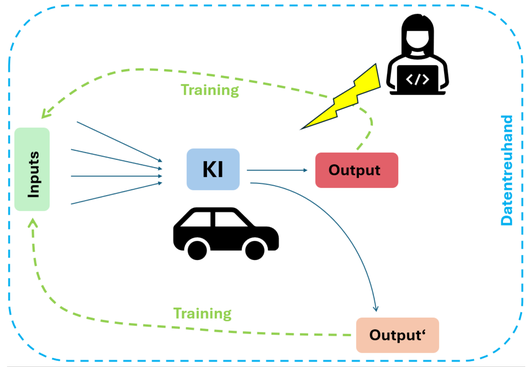

Figure 4. Eine unüberwacht lernende KI passt ihre Parameter fortlaufend an. Die technische Nach-Sicht dient dazu, unerwünschte Ausgaben von der weiteren Parametrisierung des KI-Modells auszuschließen und damit deren zukünftige Wiederholung zu verhindern.

Technische Nach-Sicht und KI-Modell

Damit die technische Nach-Sicht im Sinne einer wirksamen Risikoregulierung greifen kann, sind sowohl an das KI-System selbst als auch an die rechtliche Ausgestaltung und Prozeduralisierung Anforderungen zu stellen, die mit europäischem und nationalem Recht vereinbar sind:

- strenge Transparenz- und Erklärbarkeitsvorgaben für das KI-Modell,
- datenschutz- und datenrechtskonforme Treuhandmodelle für die Zusammenführung und Auswertung der Daten durch die technische Nach-Sicht,
- geeignete Sicherheitstests im Zulassungsverfahren, basierend auf belastbaren statistischen Maßstäben.

Referenzen

Fraunhofer-Institut für Experimentelles Software Engineering (IESE) (2025). *Autonomes Fahren*. Institutsseite. https://www.iese.fraunhofer.de/de/trend/autonomes-fahren.html (visited on 09/14/2025).

Holzinger, A., K. Zatloukal, and H. Müller (2025). "Is human oversight to AI systems still possible?" In: *New Biotechnology* 85, pp. 59–62. doi: https://doi.org/10.1016/j.nbt.2024.12.003. https://www.sciencedirect.com/science/article/pii/S1871678424005636.

Köllner, C. (Feb. 3, 2025). *Was bedeutet das KI-Gesetz für die Autoindustrie?* https://www.springerprofessional.de/kuenstliche-intelligenz/automatisiertes-fahren/was-bedeutet-das-ki-gesetz-fuer-die-autoindustrie-/26700940.

Laux, J. and H. Ruschemeier (July 2025). "Automation Bias in the AI Act: On the Legal Implications of Attempting to De-Bias Human Oversight of AI". In: *European Journal of Risk Regulation*, pp. 1–16. doi: 10.1017/err.2025.10033. http://dx.doi.org/10.1017/err.2025.10033.

Sayles, J. (2024). *Principles of AI Governance and Model Risk Management. Master the Techniques for Ethical and Transparent AI Systems*. 1st ed. Berkeley, CA: Apress. doi: 10.1007/979-8-8688-0983-5.

Zhang, L., Y. Xiong, Z. Yang, S. Casas, R. Hu, and R. Urtasun (2024). *Copilot4D: Learning Unsupervised World Models for Autonomous Driving via Discrete Diffusion*. https://arxiv.org/abs/2311.01017.

Kontakt

maria.walch@igw.uni-heidelberg.de