Ist die Providerhaftung im Lichte vernetzter autonomer Systeme noch zeitgemäß?

Bardia Kian, LL.M. (LSE)
Bundesministerium für Wirtschaft und Energie

Das Zeitalter vernetzter autonomer Systeme

- Systeme die vollkommen frei von menschlichen Eingriffen agieren und kommunizieren
- Konventionelle Systeme werden mit den Möglichkeiten der IT verknüpft und angereichert
- Intelligenz und Gedächtnis
- Eigene Sensoren, Messinstrumente (Kameras, Abstandmesser, etc.)
- Rückgriff auf externe Informationen und Kommunikation nach außen

Das Zeitalter vernetzter autonomer Systeme

- Prominente Vertreter:
  - **Autonomes Fahren**
  - **Industrie 4.0**

- Fokus verschiebt sich vom Nutzer zur Eigenständigkeit der Maschine

- Mensch steht bei der Bedienung und Betrieb nicht mehr im Mittelpunkt

- Aber: Anforderungen an den Menschen steigen im Vorfeld, um die Systeme zu entwickeln und zu gestalten.

Autonomes Fahren

- Fahrer soll sich zurücklehnen
- Fahrzeug fährt selbstständig von A nach B
- Beschleunigt und bremst intelligent
- Kann Gefahren einschätzen und reagieren

- Bereits vorhandene Elemente:
  - Selbstlenkende Einparkhilfen
  - Totwinkel-Assistenten
  - Intelligente Tempomaten
  - etc.

Autonomes Fahren

- Namhafte Fahrzeughersteller forschen rege
- Auch in der IT-Branche(z.B. Telekom, Google)
- Vielversprechende Konzepte vorgestellt

- Marktreife laut Hersteller in diesem Jahrzehnt, jedenfalls aber in den nächsten zehn Jahren.

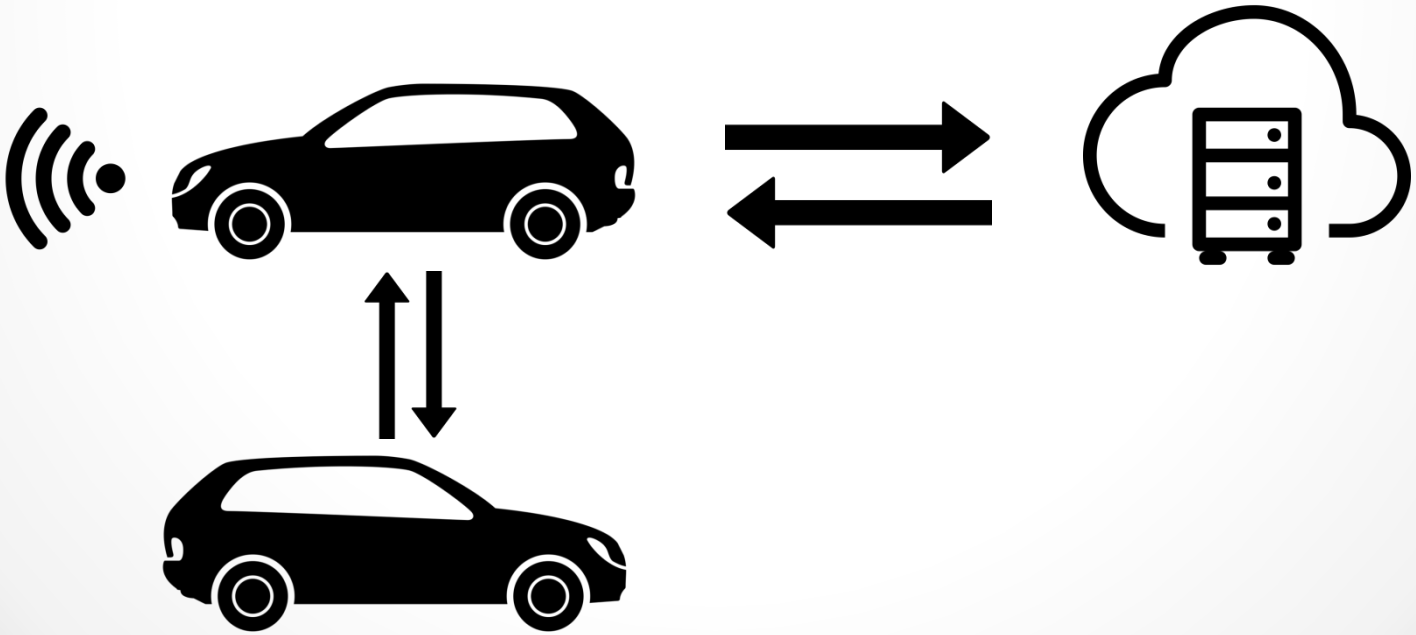
- Auch auf Staatenebene rechnet man mit der Etablierung
- Änderungsvorschläge zum Wiener Übereinkommen

Autonomes Fahren und Vernetzung

- Vollständige Vernetzung autonomer Fahrzeuge schreitet rapide voran
- Zugriff auf Fahrzeuginformationen und Fahrzeugfunktionen per Smartphone
- Internetanbindung in Fahrzeugen
- Sichtbarkeit als Knoten im Internet
- Fernzugriff für Kunden und Hersteller
- Einstellungen und Softwareupdates

Autonomes Fahren

- Autonome Fahrzeuge sind für die reibungslose Funktion auf Zugang zu einer Vielzahl von Informationen angewiesen
- Informationen können nicht immer selbst erzeugt werden sondern müssen abgerufen bzw. passiv in Empfang genommen werden

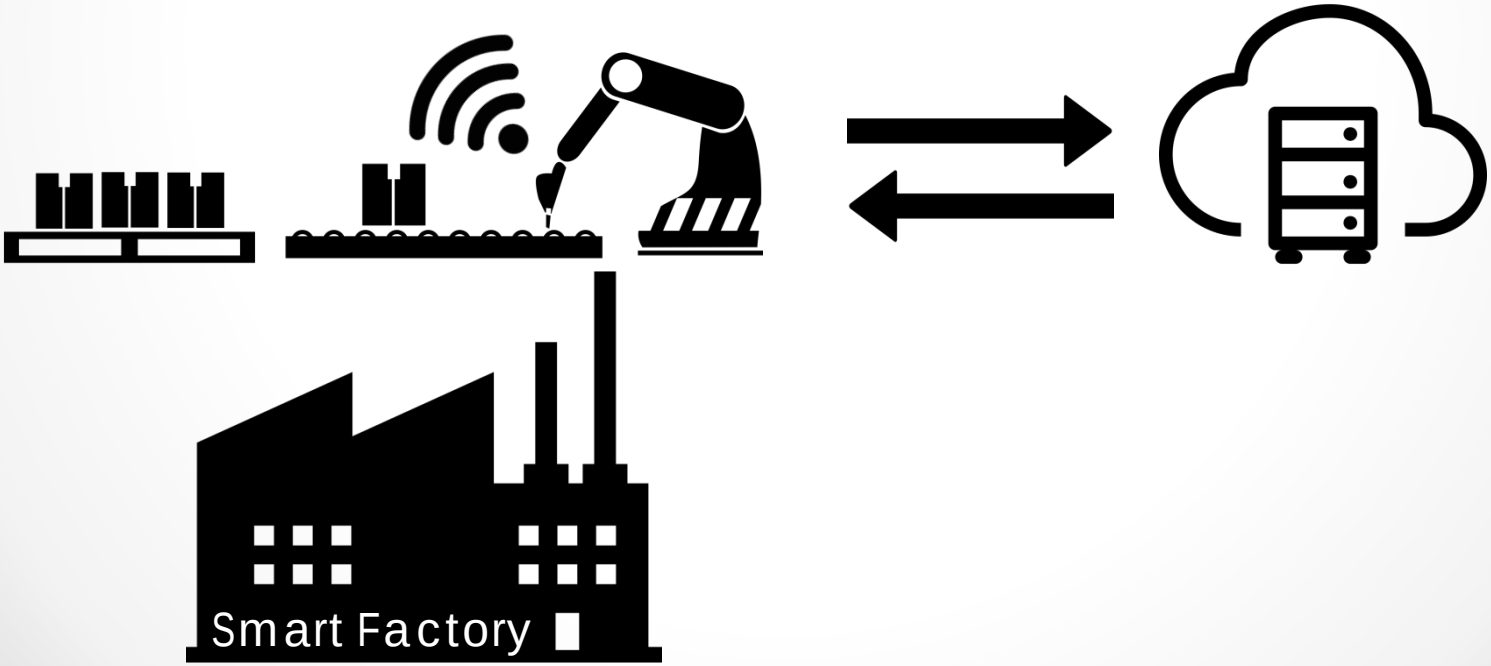


Industrie 4.0

- Vierte industrielle Revolution
- Etablierung ist schon in vollem Gange
- Konsequente Automation
- Verschmelzung der IT mit der Welt der Produktion
- Verbindung von Maschinen, Diensten und Technologien mit Kommunikationsmöglichkeiten des Internets

Industrie 4.0

- Derart vernetzte autonome Maschinen bilden Smart Factory
- Ganze Produktionsabläufe können gesteuert werden
- Bereitstellung des notwendigen Materials
- Internet der Dinge (Internet of Things)



Vorteile

- Effizientere Entscheidungsfindung
- Einsparung von Kosten
- Einsparung von Zeit
- Einsparung von Ressource
- Keine Einflüsse wie Zeitdruck und Stress
- Rationalere Entscheidungsfindung
- Angemessenere Reaktion

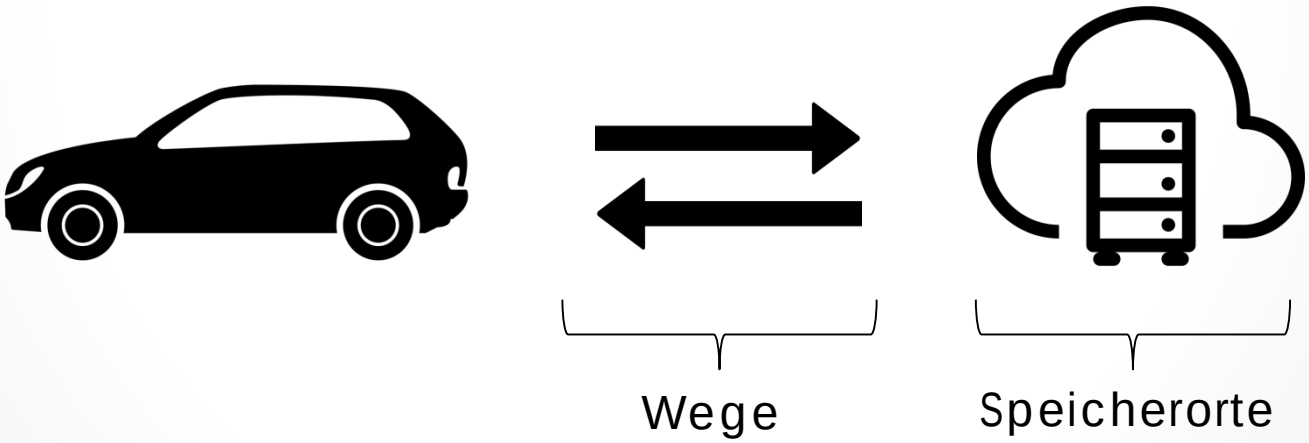
Risiken

- Risiko von Sach- und Personenschäden erhöht
- Systeme sind auf externe Informationen angewiesen
- Die erforderlichen Kommunikationswege bilden Einfallstore für die Einspeisung schädigender Informationen
- Fehlfunktionen am System und anderen Systemen
- Außerhalb des Machtbereichs der Hersteller

Risiken

Abruf von manipulierten Informationen:
Kartenmaterial
Wetterdaten
Straßeninformationen
Stauinformationen

Manipulativer Einfluss auf das System:
Falsche Anweisungen
Beschleunigen und Bremsen
Lenken



Risiken

- Gründe für Angriffe gibt es viele:
  - Schädigungsabsicht
  - Vorteile
  - Erpressung
  - Berühmt werden
  - Langeweile
  - etc.

Risiken

- Einfluss auf vernetze Systeme in der Vergangenheit:
  - Stuxnet-Wurm: Tangierung der Zentrifugen einer Urananreicheungsanlage
  - Center for Automotive Embedded Systems Security: Deaktivierung des Bremssystems eines Fahrzeugs über Bluetooth-Schnittstelle

➔ Angriffe waren in diesen Fällen nur lokal und überschaubar.

- Vernetzte autonome Systeme:
  - Durch Vernetzung müssen Schädiger nicht mehr anwesend sein.
  - Automatisierte Angriffe können Schädigungspotential zusätzlich erhöhen
  - Allgemeine Sicherheit, Ordnung, insb. Rechtgüter der Allgemeinheit empfindlich tangiert
  - Vorteile und v.a. Vertrauen gehen verloren

Provider und vernetzte autonome Systeme

- Etablierung autonomer Systeme wird weltweiten Datenverkehr deutlich ansteigen lassen
- Provider mit Kontakt zu autonomen Systemen werden immer öfter in Anspruch genommen

Das Konzept der Providerhaftung

- §§ 7 ff. TMG basierend auf Art. 12 ff. der Richtlinie 2000/31/EG (E-Commerce-Richtlinie)
- Europäischer Gesetzgeber wollte mitgliedstaatliche Regelungen zur Verantwortlichkeit von Anbieter interaktiver Dienste harmonisieren.
- Beeinträchtigung des elektronischen Verkehrs durch straf- und haftungsrechtliche Risiken der Provider.
- Wettbewerbsverzerrungen und race to the bottom.

Das Konzept der Providerhaftung

- **Haftung nach Zivil- und Strafrecht wird ausgeschlossen**.
- Erfasste Provider:
  - Access-Provider (§ 8 TMG)
  - Network-Provider (§ 8 TMG)
  - Caching-Provider (§ 9 TMG)
  - Hosting-Provider (§ 10 TMG)
  - Content-Provider (§ 7 Abs. 1 TMG)
- Abgestufte Haftung
- Je näher ein Provider mit den Inhalten in Kontakt steht, desto größer der Umfang der Verantwortlichkeit
- Zudem gemäß § 7 Abs. 2 TMG wird festgestellt, dass diese Provider nicht zur Überwachung der übermittelten oder gespeicherten Informationen sowie zur Nachforschung bezüglich rechtswidriger Tätigkeiten verpflichtet sind.

Haftung der Provider für Schäden

- Konfliktpotential?
- Vielzahl von Risiken durch vernetzte autonome Systeme **PLUS** deutlich erweiterter Einfluss von Providern **vs.** Haftungsprivilegierung für Provider

- Informationsaustausch unterfällt dem Wirkbereich der Provider
- Provider profitieren deutlich von der Inanspruchnahme vernetzter autonomer Systeme
- Haften jedoch oft nicht – trotz fehlender technischer Vorkehrung zur Abwehr von Angriffen ➔ Grund: §§ 7 ff. TMG

- Demgegenüber:
  - Mögliche Haftung der Hersteller
  - Schädiger können selten ermittelt und in Anspruch genommen werden

- **Interessenkonflikt!**

Lösung

- Bei der Gestaltung des TMG spielte die vollkommene Vernetzung von Maschinen keine prägende Rolle (Richtlinie 2000/31/EG)
- Die überragende Stellung der Provider war kein Thema – vernetzte autonome Systeme hatte niemand im Blick
- Förderung des elektronischen Geschäftsverkehrs unter Berücksichtigung des freien Dienstleistungsverkehrs
- Wer nur in dienender Funktion auftritt und gleichzeitig den elektronischen Geschäftsverkehr ermöglicht, soll nur in bestimmten Fällen haften.

Lösung

- ➔ Diese überragende Stellung ist jedoch mit Blick auf die Risiken die in der Sphäre der Provider bestehen, zu berücksichtigen

- **Nur Provider die taugliche technische Sicherungsmaßnahmen vornehmen, um unbefugten Zugang zu Daten und Datenfluss zu verhindern, sollten in den Genuss der Privilegierung kommen.**

- **Aber Wortlaut der §§ 7 ff. TMG lässt keinen Spielraum!**

Änderung des TMG möglich?

- **Hindernis 1:** Auferlegung einer allgemeinen Überwachungspflicht ist nicht erlaubt. (Art. 15 ECRL)
- *Vorliegend geht es aber nur um die Verhinderung eines Drittzugriffs*

- **Hindernis 2:** Vollharmonisierung. Von geregeltem Bereich der ECRL darf nicht abgewichen werden. Geregelter Bereich bezieht sich darauf, dass Provider Datenfluss oft nicht effektiv kontrollieren können und daher nicht haften sollen.
- *Hier geht es aber um eine vorgelagerte Ebene*

- ➔ Keine Hindernisse durch die E-Commerce-Richtlinie

Vorschlag

§ 2 TMG
Im Sinne dieses Gesetzes
(…)
7. ist autonomes System jedes System, das im Einzelfall nicht von einem Menschen abhängt und welches ohne menschliche Eingabe intelligent reagieren kann.

§ 8 TMG
(1) (…)
[3] S. 1 findet im Zusammenhang mit autonomen Systemen, die solche Informationen empfangen nur Anwendung, wenn die Diensteanbieter Maßnahmen getroffen haben, die geeignet sind zu gewährleisten, dass Unbefugte keinen Zugang zu deren Datenverarbeitungsystemen und Übermittlungsvorgängen erlangen können, insbesondere Informationen während ihres Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

§ 9 TMG
(…)
[3] S. 1 findet im Zusammenhang mit autonomen Systemen, die solche Informationen empfangen nur Anwendung, wenn die Diensteanbieter Maßnahmen getroffen haben, die geeignet sind zu gewährleisten, dass Unbefugte keinen Zugang zu deren Datenverarbeitungsystemen und Übermittlungsvorgängen erlangen können, insbesondere Informationen während ihres Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

§ 10 TMG
(…)
[3] S. 1 findet im Zusammenhang mit autonomen Systemen, die solche Informationen empfangen nur Anwendung, wenn die Diensteanbieter Maßnahmen getroffen haben, die geeignet sind zu gewährleisten, dass Unbefugte keinen Zugang zu deren Datenverarbeitungsystemen und Übermittlungsvorgängen erlangen können, insbesondere Informationen während ihres Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Vorschlag

- Ohne Anpassung des geltenden Rechts würde die Entwicklung vernetzter autonomer Systeme und wirtschaftliches Potential empfindlich beeinträchtigt

- Ohne Anpassung würden Anreize zur Investition in nötige Schutzvorkehrungen fehlen.

- Aber: Nachweis ausreichender technischer Vorkehrungen sollte durch Vorlage von Prüfberichten unabhängiger Stellen möglich sein

Strafrechtliche Verantwortlichkeit von Access-Providern

- Im „Offline“-Bereich gilt Strafbarkeit wegen Beihilfe zu einer Straftat durch Unterlassen, wenn trotz positiver Kenntnis und Garantenstellung die Verwirklichung des Straftatbestandes gefördert wird.

- Im „Online“-Bereich werden für die strafrechtliche Verantwortlichkeit von Providern verschiedene Ansichten vertreten.

- Nicht zuletzt ist mit Blick auf vernetzte autonome Systeme ist eine Klarstellung notwendig.

Strafrechtliche Verantwortlichkeit von Access-Providern

- Es geht um die Auslegung des § 8 Abs. 1 TMG:

> (1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie
> 1. die Übermittlung nicht veranlasst,
> 2. den Adressaten der übermittelten Informationen nicht ausgewählt und
> 3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

- Von Kenntnis ist hier keine Rede.

Strafrechtliche Verantwortlichkeit von Access-Providern

- § 7 Abs. 2 S. 2 überlagert § 8 Abs. 1 TMG (lex specialis)
- Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach **allgemeinen Gesetzen** bleiben **unberührt**.
- Auch Vorschriften des Strafrechts fallen unter allg. Gesetze.
- Wer also Pflicht zum Tätigwerden hat haftet auch strafrechtlich

Strafrechtliche Verantwortlichkeit von Access-Providern

- Verantwortlichkeit ergibt sich auch aus der E-Commerce-Richtlinie.
- Erwägungsgrund 42 besagt, dass **nur wer Informationen durchleitet** und ansonsten **passiv bleibt**, **ohne Kenntnis oder Kontrolle** über die durchgeleiteten Informationen zu haben privilegiert ist.
- Wer aber trotz Kenntnis den Zugang zu rechtswidrigen Informationen nicht versperrt, obwohl es ihm möglich ist, ist nicht privilegiert.

Strafrechtliche Verantwortlichkeit von Access-Providern

- Im Übrigen gebietet bereits das **hohe Schädigungspotential** durch vernetzte autonome Systeme diese Sichtweise.
- Wer sich weigert, großflächigen Schädigungen Einhalt zu gebieten kann nicht von der Verantwortlichkeit freigestellt werden.
- Dies kann nicht anders beurteilt werden als ein Postzusteller, welcher positive Kenntnis davon hat, dass er im Begriff ist, eine Briefbombe an einen Empfänger zu übergeben und dennoch nicht davon Abstand nimmt.
- **Auch Access-Provider können sich einer Straftat wegen Beihilfe durch Unterlassen strafbar machen.**

Zusammenfassung

- Vernetzte autonome Systeme versprechen viele Vorteile
- Vernetzung bringt aber auch Risiken des unbefugten Eingriffs von außen
- Übertragungswege und Speicherorte essentieller Daten
- Hersteller stehen alleine da bzw. Geschädigte können Verursacher nicht ermitteln

Zusammenfassung

- Provider oft durch Vorschriften des TMG privilegiert obwohl ihr faktischer Einfluss immens wächst
- Fehlende Sicherheitsvorkehrungen der Provider wirken sich nicht auf deren Haftung für Schäden aus
- Unter Abwägung der Interessen ist eine **zusätzliche Prämisse** für die Privilegierungsvorschriften des TMG zu fordern.
- Es sind **geeignete Maßnahmen** zu treffen, welche den **unbefugten Zugang zu DV-Systemen und Übermittlungsvorgängen verhindern**.

Zusammenfassung

- Die Vorschrift des § 8 Abs. 1 TMG ist so zu verstehen, dass Access-Provider die den **Zugang zu rechtswidrigen Daten vermitteln** und von der Rechtswidrigkeit **positive Kenntnis** haben bei Vorliegen der weiteren Voraussetzungen **Beihilfe durch Unterlassen** zu einer Straftat begehen.

Vielen Dank für Ihre Aufmerksamkeit