TeleTrusT
Pioneers in IT security.

TeleTrusT-Mitgliederkonferenz

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Berlin, 29.11.2018

KI aus juristischer Sicht

Matthias Hartmann, HK2 Rechtsanwälte

Matthias Hartmann

- Rechtsanwalt
- Partner bei HK2 Rechtsanwälte
- Fachanwalt für Informationstechnologierecht

HK2 Rechtsanwälte

Künstliche Intelligenz

Neuronale Netze

Deep Learning

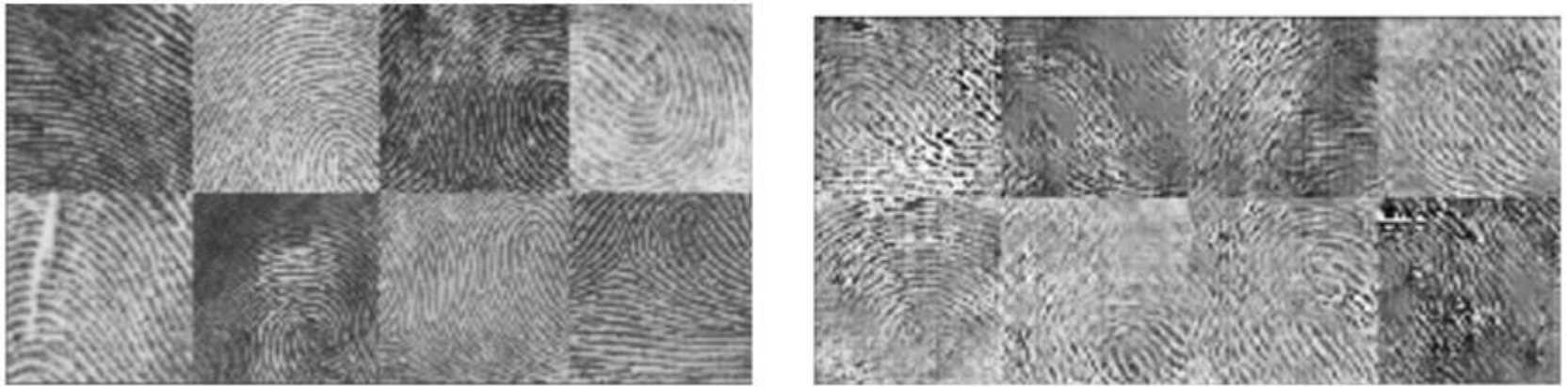
Machine Learning

Autonomes Entscheiden

Roboter

„Autonomes“ Entscheiden

- Mustererkennung
- Wahrscheinlichkeitsbasierte Reaktionen
- „Echte Autonomie“



(a) Real (left) and generated (right) samples for the NIST dataset.

DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution
Philip Bontrager, Aditi Roy, Julian Togelius, Nasir Memon, Arun Ross
https://arxiv.org/pdf/1705.07386.pdf

KI und IT-Sicherheit

- Bedrohung durch KI gestützte Angriffe
  - Skalierbare Ressourcen
  - „Optimierung“ von Angriffen
  - Unerwartete Angriffe

- Abwehr durch KI gestützte Systeme
  - Erkennung von Angriffsmustern in „Echtzeit“
  - Automatisierte Entscheidungen
  - Training mit „optimalem Angreifer“
  - Waffengleichheit gegen Angriffe durch KI

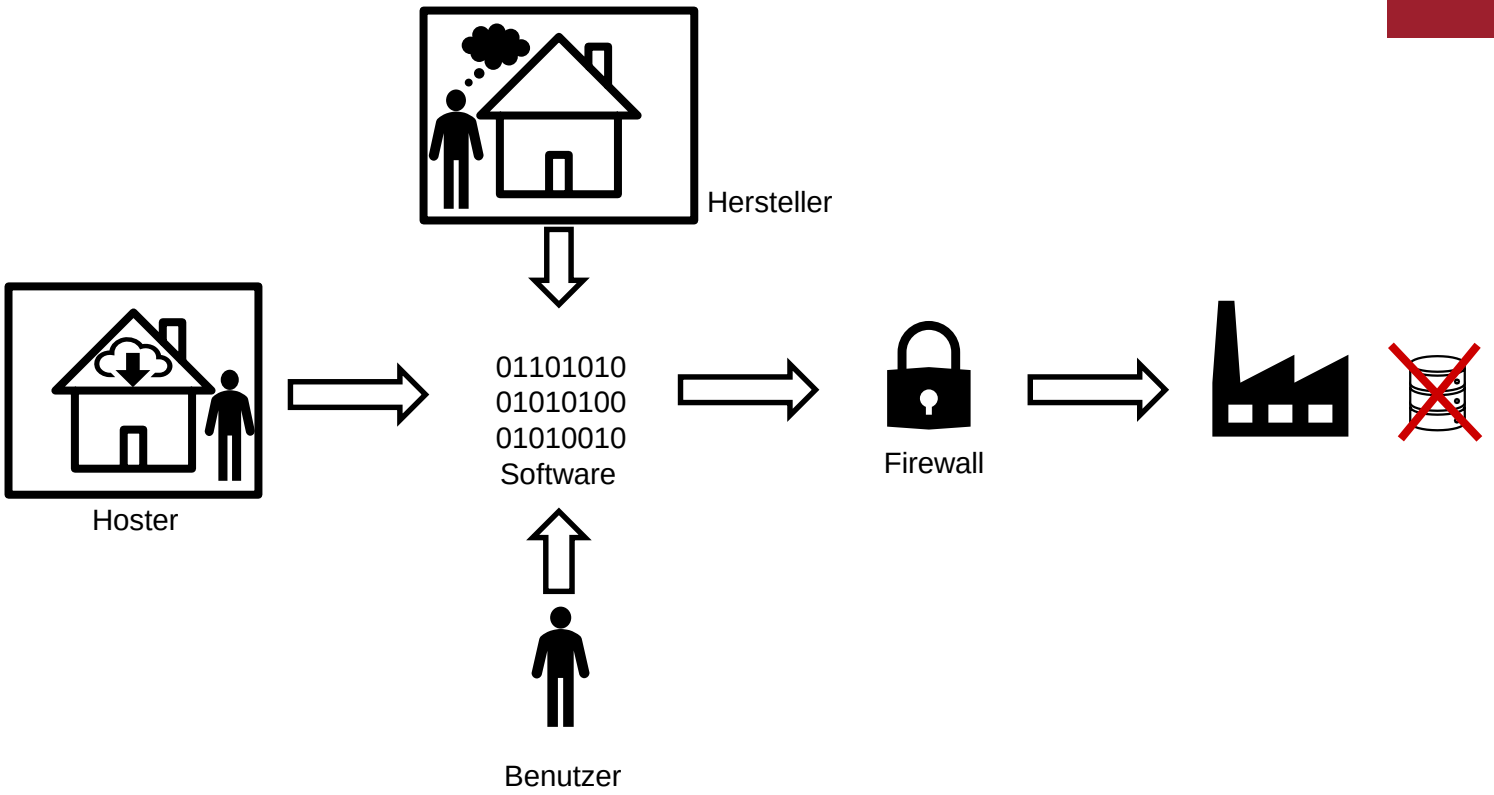
KI und Recht in der Diskussion

- Brauchen wir ein KI Gesetz?
- Brauchen wir neue Haftungsnormen?
- Brauchen wir eine digitale Person?

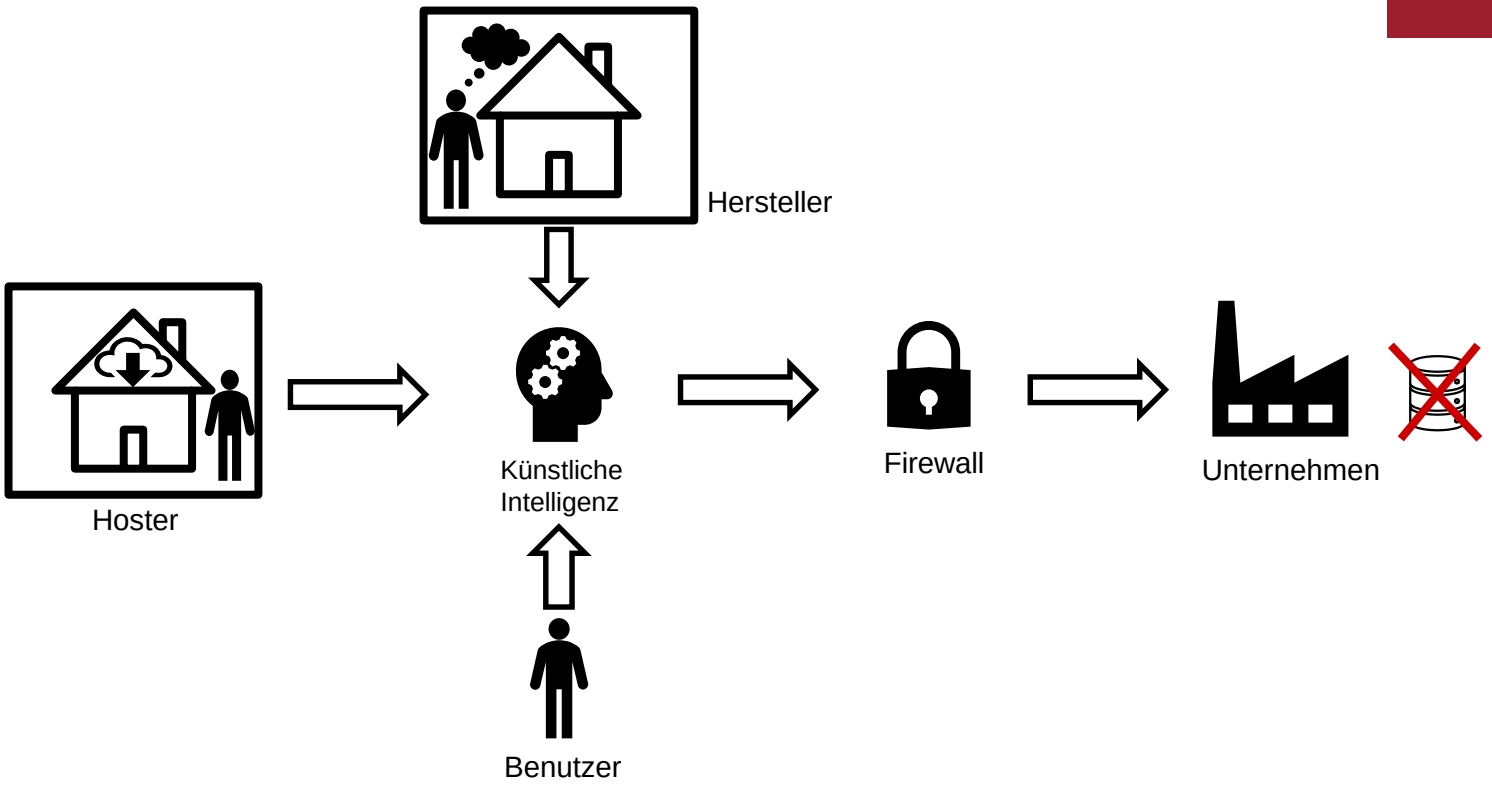
Rechtsfragen

- Verantwortung und Haftung für KI
- Rechte an und durch KI
- Datenschutz

Hackerangriff auf Daten eines Unternehmens



Hackerangriff mit KI oder durch KI



Strafnormen

HK2 Rechtsanwälte

1. Hack-spezifische Strafnormen

- Ausspähen von Daten, § 202a StGB
- Abfangen von Daten, § 202b StGB
- Vorbereiten des Ausspähens und Abfangens von Daten, § 202c StGB
- Datenveränderung, § 303a StGB
- Computersabotage, § 303b StGB
- Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen, § 108b UrhG

2. Beispiele allgemeiner Strafnormen

- Computerbetrug, § 263a StGB
- Betrug, § 263 StGB
- Körperverletzung, § 223 StGB
- Sachbeschädigung, § 303 StGB

Strafbarkeit des Herstellers oder Hosters
§ 202a StGB – Ausspähen von Daten durch KI

Obj. TB	Merkmale	Handlung	Kausalität	Obj. Zurechnung
	▪ Daten verschafft ▪ für ihn nicht bestimmt ▪ gegen Zugang besonders gesichert ▪ Überwindung der Sicherung	Erstellen und Aktivieren der KI Hosten der KI	Taterfolg ist kausal auf Handlung zurückzuführen	Handlung hat die rechtlich missbilligte Gefahr geschaffen, welche sich im tatbestandlichen Erfolg realisiert hat Ist die Tat typisch für, das was die Norm verbietet? Unterbricht die Entscheidung der KI die Zurechnung?
Subj. TB	Vorsatz			
	Handelte der Täter vorsätzlich bezüglich des objektiven Tatbestands? Eventualvorsatz oder Fahrlässigkeit (nur in bestimmten Fällen strafbar)			

Haftung für die KI (Zivilrecht)

Beispiel: ein „autonomes“ Fahrzeug ist in einen Unfall verwickelt

- Vertragliche Ansprüche des Käufers, wenn Pflichtverletzung
  - Auslieferung trotz Mangels
  - Schuldhafte Verletzung einer Nebenpflicht/ Sorgfaltspfliccht
- Deliktische Ansprüche aller Geschädigten
  - Haftung aus verschuldetem Unrecht, bspw. § 823 BGB
  - Gefährdungshaftung
    - Halterhaftung, § 7 StVG, Fahrerhaftung, § 18 StVG
    - Produkt-/ Produzentenhaftung:
      Haftung für „Fehler“ eines Produkts
      Haftung für Verletzung einer Verkehrssicherungspflicht

Wer trägt die Darlegungs- und Beweislast?

- Erleichterungen der primären/ oder sekundären Darlegungs- /Beweislast
  - bei Tatsachen aus der Sphäre des Gegners
  - bei mangelnder Dokumentation, wenn eine Pflichten zur Erstellung besteht
- Umkehr der Beweislast, Anscheinsbeweis
  - „Wer auffährt ist schuld“
  - „Wer rückwärts fährt ist schuld“
- Sachverständige zur Klärung der Tatsachen
- Vorlage von Unterlagen (auch Daten oder Software),
  - ➢ Halter muss bestimmte Daten bei Unfällen an Dritte herausgeben, § 63a Abs. 3 StVG
- Beschlagnahme bei Verdacht einer Straftat

Wo ist das Problem?

„Fehler“ einer KI, erforderliche Sicherheit einer KI

War die Reaktion des Fahrzeugs falsch (Daten oder Situation)?

„AF muss in der Lage sein, den an die Fahrzeugführung gerichteten Verkehrsvorschriften zu entsprechen“, § 1a Abs. 2 Nr. 2 StVG

Wie „sicher“ muss ein Auto fahren?

- Wie ein Mensch?
- Wie ein optimaler Fahrer?
- Mit einer Wahrscheinlichkeit von X?

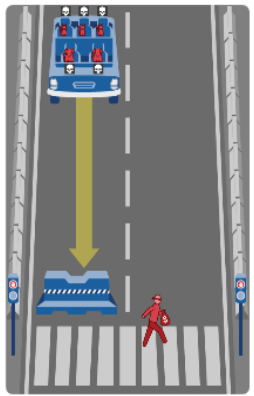
HK2
Rechtsanwälte

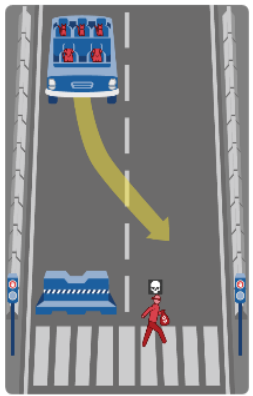
MORAL MACHINE

Start Beurteilen Klassik Designen Durchsuch

pets or illegal thief

Teilen Link 0 Likes Zufällig





Beschreibung einblenden

Beschreibung einblenden

Zahlen zum Straßenverkehr

- Tesla erster Vehicle Safety Report (Q3-2018)
  - „Autonom“ alle 3,34 Mio Meilen ein Unfall oder ähnliches Event
  - Fahrermodus alle 1,92 Mio Meilen ein Unfall oder ähnliches Event
  - NHTSA: alle 0,492 Mio Meilen ein Unfall ist Durchschnitt

- Verkehrsopfer in Europa 2017:
  - 25.300 Tote
  - 135.000 Schwerverletzte

- Welt (2013): 1,25 Mio Tote

Entschließung des Europäischen Parlaments vom 16.02.2017: Diskussionsvorschläge

- „Halterhaftung“ für KI
  - Registrierung von KI für Zuordnung
  - Verschuldensunabhängige Haftung für „alle Schäden“
  - Haftungsfond oder Versicherung für KI

HK2
Rechtsanwälte

$$\min_G \max_D \mathbb{E}_x[\log(D(x))] + \mathbb{E}_z[\log(1 - D(G(z)))]$$

Image © Obvious

Rechte und KI

- Rechte durch KI
  - Output als Schöpfung des Inhabers/ Herstellers der KI
  - Output als Schöpfung der KI
- Rechte an der KI
  - KI als Computerprogramm
  - KI als derivatives Werk
  - KI als Datenbank
  - KI als Werk eigener Art

Schutz der Daten vor KI

HK2 Rechtsanwälte

Prinzipien der DSGVO:

- Datenvermeidung
- Zweckbindung
- Verbotsgrundsatz
- Privacy by Design
- Anonymisierung
- Keine automatisierte Einzelfallentscheidung mit rechtlicher Wirkung

Prinzipien KI:

- Je mehr Daten, desto bessere Ergebnisse
- Möglichkeiten werden erst bei Nutzung der Daten erkennbar
- Manipulierte Daten erzeugen unerwünschte Artefakte
- KI kann schneller und besser entscheiden als ein Mensch

Beispiel: Abwehr von Angriffen auf ein Netzwerk

- IP Nummern gelten als personenbezogene Daten
- Jede Verarbeitung bedarf einer Rechtfertigung
- Nach h.M. dürfen IP Nummern wohl vom Provider für eine begrenzte Zeit gespeichert werden für Zwecke der Netzsicherheit (siehe aktuell BSI, Standards zum Umgang mit (Log-) Daten im Hinblick auf Cyber-Angriffe)
- Das Speichern der Daten eines Angriffes zum späteren Trainieren einer KI ist hiervon wohl nicht mehr umfasst und stellt eine Zweckänderung dar

➢ Rechtgrundlage Art. 6 Abs. 1 f) DSGVO fraglich

Handlungsbedarf im Datenschutz – im Hinblick auf KI

HK2 Rechtsanwälte

- Verbotsprinzip der DSGVO ist ein epochaler Fehler

- Auf „anonymisierte“ Daten zu verweisen ist meist untauglich

  - Bspw. § 63a StVG:

  Abs. 5: Unfallforschung ist zulässig mit „anonymisierten“ Daten nach Abs. 1

  Abs. 1: Kraftfahrzeuge speichern die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben.

- Wenn bei der Entwicklung von KI in der EU ein Risiko für Bußgelder und für die Daten besteht, werden Investoren die Entwicklung außerhalb bevorzugen

Wer macht das Rennen um die Weltklasse KI

Die EU kündigte an, ihre Förderung für KI zwischen 2018 und 2020 auf **1,5 Milliarden Euro zu erhöhen**. Über den Europäischen Fonds für strategische Investitionen (EFSI) sollen weitere 500 Millionen Euro in Start-ups fließen.

https://www.tagesspiegel.de/wirtschaft/investitionsprogramm-eu-fordert-20-milliarden-fuer-kuenstliche-intelligenz/21213898.html

Bis 2025 will der Bund insgesamt etwa **3 Milliarden Euro** für die Umsetzung der Strategie Künstliche Intelligenz bereitstellen.

https://www.bundesregierung.de/breg-de/aktuelles/ki-als-markenzeichen-fuer-deutschland-1549732

China kündigt an, bis 2030 die USA einholen zu wollen. Investiert werden sollen **150 Mrd US$**

https://www.forbes.com/sites/arthurherman/2018/08/30/chinas-brave-new-world-of-ai/#10f9ffc528e9

Wer macht das Rennen um die KI?

In den USA sitzen die besten Unternehmen

China hat die meisten Daten

- Europa erlässt die tollsten Gesetze

Haben Sie Fragen?

HK2 Rechtsanwälte

Rechtsanwalt

Matthias Hartmann

Fachanwalt für IT-Recht

Hausvogteiplatz 11 A
10117 Berlin

Telefon +49 (0)30 27 89 00 – 0
Telefax +49 (0)30 27 89 00 – 10
E-Mail hartmann@hk2.eu

www.hk2.eu