

# Protokoll: Künstliche Intelligenz und Datenschutz

Protokoll: Hagen Küchler

Prof. Dr. Sorge leitete zunächst das Thema ein, indem er den Zuhörern einen groben Überblick über das weite Feld der Künstlichen Intelligenz gab. Nach einem kurzen Ausflug in die Geschichte der Künstlichen Intelligenz. Erläuterte er die großen Fortschritte der letzten Jahrzehnte. Diese Fortschritte seien besonders auf den Einsatz maschinellen Lernens zurückzuführen. Anschließend folgte eine Einführung in die technischen Grundlagen der künstlichen Intelligenz, indem er erklärte wie sich die Verfahren von Tabellen und Modellen hin zu neuronalen Netzwerken weiterentwickelten. Nun ging Herr Prof. Dr. Sorge darauf ein welche Auswirkungen die künstliche Intelligenz auf den Datenschutz hat. Der Zusammenhang besteht im Wesentlichen darin, dass die Künstliche Intelligenz mittlerweile dem Menschen auf dem Gebiet der Mustererkennung weit überlegen ist. So ist es möglich, dass KI in der Lage ist, auf einem noch stark verpixelten Bild einzelne Personen zu identifizieren. Zudem ist eine Künstliche Intelligenz frei von üblichen Denkmustern und kann Zusammenhänge herstellen die ein Mensch nicht in Betracht ziehen würde.

Prof. Dr. Borges folgte mit seinem Vortrag „Von Alexa bis zu autonomen Fahren: Sensordaten als datenschutzrechtliche Herausforderung“. In diesem Vortrag ging er auf die rechtlichen Grundlagen der DSGVO für die Verarbeitung personenbezogener Daten ein. Insbesondere die Rechtfertigung der Verarbeitung von Trainingsbildern, die für das Training Künstlicher Intelligenz für das autonome Fahren verwendet werden. Zudem erörterte er den gesetzlichen Rahmen für die Verarbeitung von Sensorbildern.

Herr Dr. Kleinbauer griff in seinem Vortrag das Thema „Alexa“ wieder auf und erklärte, statt sich mit der Forschung an Bilder, mit der an Sprache zu beschäftigen. Dort zeigte er gerade im Bereich der Hausautomation große datenschutzrechtlich bedenkliche Beispiele auf. Anschließend brachte er den Zuhörern das Forschungsprojekt COMPRISE näher, indem versucht wird Trainingsdaten zu anonymisieren. Dabei stellt er sich der Schwierigkeit den Spagat zwischen größtmöglicher Unverfälschtheit der Daten und geeignetem Trainingswert für die künstliche Intelligenz zu gewährleisten.

Während den Vorträgen hatten die Zuhörer Gelegenheit Fragen zu stellen die teilweise Gegenstand einer allgemeinen Diskussion wurden. Insbesondere kam zur Sprache: die maschinelle Anonymisierung von Gerichtsurteilen, der Kameraeinsatz durch die Polizei, die Übermittlung von personenbezogenen Daten (die durch Fahrzeuge erfasst werden) an Hersteller, der wirtschaftliche Wert personenbezogener Daten sowie die praktische Umsetzung von Betroffenenrechten im Rahmen der DSGVO.