

WisteV-wistra-Neujahrstagung 2026

Rechtsanwältin Luise Kirsch, Frankfurt/M.

Begrüßt von dem Roboter „Peppa“ fanden sich die Teilnehmer und Teilnehmerinnen der 17. WisteV-wistra-Neujahrstagung am 16. und 17.1.2026 im Westin Grand Frankfurt/M. zusammen, um das Thema „Wirtschaftsstrafrecht und KI“ zu diskutieren.

Vor Beginn des Fachprogrammes erinnerte RA Prof. Dr. *Michael Tsambikakis* an Prof. Dr. *Robert Esser*, der am 19.11.2025 plötzlich und unerwartet im Alter von nur 55 Jahren verstorben ist. *Tsambikakis* betonte die Lücke an Wissen und Erfahrung, die sein Tod hinterlasse und würdigte seine Expertise im europäischen Wirtschaftsstrafrecht mit der Aussage, dass der Kreis der Juristen den besten Kenner der Rechtsprechung des EGMR vermissen werde.

Prof.'in Dr. *Charlotte Schmitt-Leonardy* eröffnete die Tagung im Namen der wistra. Sie hob zunächst – mit Verweis auf *Reid Hoffmann* („AI will fundamentally reshape every industry and job“) – die unzweifelhafte Bedeutung dieser technologischen Entwicklung für das Recht hervor. Wichtiger aber als die Frage, was KI sei und könne, müsse die Frage sein, „wer wir sein wollen in Anbetracht von KI“. Schon deshalb, weil KI imitiere, was von Menschen vorgegeben und vorgelebt würde, aber auch, weil entscheidend sei, dass die – insbesondere für die Rechtsanwendung zentrale – menschliche Fähigkeit zu kritischem Denken nicht verloren gehe. RA Dr. *Thomas Nuzinger* begrüßte die Teilnehmer ebenfalls und betonte die zunehmende Alltagsrelevanz von KI sowie die Vorsicht, die selbst OpenAI-Gründer *Sam Altman* empfehle. Die Tagung wolle faktenbasiert vorausschauen und die Entwicklung des Wirtschaftsstrafrechts im KI-Zeitalter beleuchten.

1. Den Auftakt zu den Fachvorträgen gestaltete *Nina Meier*. Als Anti-Money-Laundering Specialist erläuterte sie die Grenzen bestehender KYC-Verfahren, insbesondere bei alternativen Legitimationsprozessen wie eID, die oft keine belastbaren Daten lieferten. Ein zentrales Missbrauchsrisiko sei der „Look-alike-Fraud“, dessen Aufdeckung zunehmend KI-gestützte Verfahren erfordere, zugleich jedoch datenschutzrechtlich problematisch sei. Das Transaktionsmonitoring bilde das Kerninstrument der Geldwäscheprävention. Sie hob die Vorteile von Pre-Transaction-Screening hervor und wies auf die Einschränkungen durch Echtzeitüberweisung hin. KI könne hier besonders bei der Erkennung komplexer Tatstrukturen einen erheblichen Mehrwert bieten. Im Anschluss widmete sich *Hans Jürgen Rosenlehner* vom Bayerischen Staatsministerium der Finanzen und Heimat der steuerlichen Erfassung von Social-Media-Akteuren, deren Einnahmen über unterschiedliche Plattformen schwer nachvollziehbar seien. KI-gestützte Auswertungen könnten die Zuordnung von Accounts, Simulation von Reichweiten und mögliche Einkünfte erleichtern, welche als Grundlage für Anfangsverdachtsprüfungen dienen könnten. Herausforderungen bestünden insbesondere bei der Pseudonymisierung, der kurzfristigen Verfügbarkeit von Inhalten und aufgrund fehlender rechtlicher Klarheit. Die anschließende Diskussion unter Moderation von OStA'in Dr. *Martina Müller-Ehlen* konzentrierte sich auf die Ermächtigungsgrundlagen für den von *Rosenlehner* beschriebenen KI-Einsatz.

2. Die zweite Hälfte von Themenblock 1 eröffnete RA Dr. *Daniel Weiß*, LL.M. (Chicago) und stellte in seinem Vortrag KI als effizientes Instrument zur Auswertung großer Datenbestände vor, das klassische Suchwort-Methoden – insbesondere bei visuellen, auditiven oder fremdsprachigen Inhalten – übertreffe. Risiken würden allerdings in Transparenzdefiziten („Black Box“), Verzerrungen und fehlerhaften Ergebnissen bestehen. Entscheidend seien Prozessorganisationen, Qualitätskontrolle und menschliche Validierung („human in the loop“). KI löse keine neuen Rechtsfragen, müsse aber berufsrechtlichen Vorgaben wie z.B. § 43 BRAO und der Verschwiegenheitspflicht genügen. Im Anschluss beleuchtete Dr. *Laura Braam*, Leiterin der Rechtsabteilung der Landesmedienanstalt NRW, die seit 2017 bestehende Kooperation von Aufsichtsbehörden, Strafverfolgung und Medienhäusern bei KI-gestützter Überwachung digitaler Inhalte. Ziel sei die konsequente Strafverfolgung, nicht allein die Löschung missbräuchlicher und verbotener Inhalte. KI helfe zwar dabei potentiell rechtswidrige Inhalte zu identifizieren, diese müssten anschließend allerdings menschlich bewertet werden. Sie betonte, dass

insbesondere politischer Extremismus besonders schwierig zu erfassen sei. In der von RA Prof. Dr. *Markus Rübenstahl* moderierten Diskussion wurde sodann das Haftungsprivileg der Plattformen nach Art. 6 DSA als limitierender Faktor für Ermittlungen thematisiert.

3. RA Dr. *Alexander Paradissis* eröffnete den Themenblock 2 und warnte vor einer Überschätzung der Entscheidungsfähigkeit von KI. Bias, Halluzinationen und die Gefahr, den Menschen zu ersetzen, seien kritisch zu sehen. Prof. Dr. *Dominik Brodowski*, LL.M. (UPenn) stellte in seinem Vortrag klar, dass KI Wahrscheinlichkeiten erkenne, atypische Fälle jedoch leicht übersehe. KI ermögliche schnelle Datenanalysen und eine Entlastung der Ermittler (beispielsweise in Missbrauchsfällen), bringe aber zugleich Risiken bei Fehlerquoten, Transparenz und Datenschutz mit sich. Vor dem Hintergrund des BVerfG-Urteils zu Palantir (BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/10, 1 BvR 2634/20) und der Grenzen der KI-Verordnung (KI-VO) plädierte auch er für menschliche Kontrolle, Qualitätssicherung und transparente Nutzung von KI als Werkzeug. RA Dr. *Saleh Ihwas* erläuterte sodann die einschlägigen gesetzlichen Grundlagen für die Nutzung von KI in der Anwaltskanzlei (§§ 43, 43a, 43e BRAO; DSGVO; KI-VO 2024) anhand einer Beispielsakte und live-Demonstration der juristischen KI *libra.ai*. Er veranschaulichte dabei, wie KI bei der Strukturierung von Akten, dem Erkennen von Widersprüchen und dem Erstellen von Chronologien unterstützen könne. Auch *Ihwas* ging auf die Probleme des Bias, People-Pleasing sowie die Halluzinationen der KI ein, die allenfalls durch Prompt-Engineering und Schulungen abgefedert werden könnten.

Abschließend gingen Dr. *Martin Seelmann* und MLaw *Colin Carter* von der Universität Basel auf die Frage ein, ob KI bereits in der Lage sei automatisierte Strafbefehle zu erlassen, oder ob es nach wie vor menschlicher Richter bedürfe. Am Beispiel der Schweiz zeigten sie, dass automatisierte Strafbefehle bei komplexen Fällen rechtlich und technisch derzeit nicht realisierbar seien. Bedenken bestünden insoweit hinsichtlich Transparenz, Qualität der Rechtsprechung, demokratischer Legitimation und der Menschenwürde. KI könne aber unterstützend eingesetzt werden, etwa bei Masseverfahren.

4. Im abendlichen Streitgespräch, das von RA'in Dr. *Ricarda Schelzke* moderiert wurde, erörterten *Rainer Franosch* als Vertreter des Hessischen Justizministeriums, Prof. Dr. Dr. *Eric Hilgendorf* als Vertreter der Wissenschaft und LOStA *Markus Hartmann* aus Sicht der Strafverfolgung die Pläne zum weiteren Einsatz von KI in der Strafverfolgung. *Hartmann* schilderte zunächst die praktischen Herausforderungen der Strafverfolgung im Umgang mit Massendaten: KI werde bereits als Assistenzinstrument eingesetzt, etwa bei der Bildidentifikation, Übersetzungen in Haftsachen oder der Vorprüfung der Beweisrelevanz von Asservaten. Die Frage, ob KI Entscheidungen treffen solle, greife hier hingegen zu kurz. Entscheidend seien niederschwellige, unterstützende Anwendungen, die die Ermittlungsarbeit effizienter machten. Kontrovers diskutiert wurden sodann auch die rechtlichen und politischen Rahmenbedingungen. Unter anderem kritisierte *Franosch*, dass mit der KI-Verordnung der EU Justiz und Strafverfolgung regulatorischen Beschränkungen unterworfen seien, ohne zugleich tragfähige Ermächtigungsgrundlagen in der StPO zu schaffen. *Hilgendorf* stellte demgegenüber weniger die Regulierung als vielmehr die technologische Entwicklung in den Vordergrund und warnte vor einem Verlust europäischer Souveränität durch Abhängigkeiten von US-amerikanischen oder chinesischen Anbietern. *Hartmann* stellte daraufhin klar, dass digitale Souveränität keine Aufgabe der Justiz sei, sondern der Gesetzgeber klare Leitplanken für einen verantwortlichen Einsatz von KI setzen müsse, um Qualität, Wahrheitspflicht und die etablierten Standards der Strafverfolgung zu sichern. In der Schlussrunde verdichtete sich die Diskussion auf das Spannungsfeld zwischen dem „Traum“ eines effizienten, rechtsstaatlich eingebetteten KI-Einsatzes und dem Alptraum eines Kontrollverlustes, menschlicher Bequemlichkeit und Faulheit bei der Anwendung und Auslegung des Rechts.

5. Der zweite Tag der Tagung wurde von Moderator RA Dr. *Thomas Nuzinger* eröffnet und startete mit einem Vortrag von Prof.'in Dr. *Victoria Ibold* (Universität Passau). In ihrem Vortrag befasste sie sich mit der Frage strafrechtlicher Produktverantwortung in Bezug auf KI-Produkte. Sie differenzierte dabei zwischen KI als Tatmittel (z.B. Betrug via Stimmimitation) und legaler Nutzung mit schwerwiegenden Folgen (US-Fall: suizidales Kind nach Chatbot-Interaktion). Zentral sei die „Black-Box“-Problematik, da Entscheidungsprozesse statistisch geprägt und nicht nachvollziehbar seien und dadurch klassische Zurechnungsfragen verschärft würden. Das Strafrecht stoße aufgrund der Intransparenz von KI an seine Grenzen, weshalb die Regulierung primär im Bereich der zivilrechtlichen Produkthaftung liege. *Ibold*

sprach sich gegen KI als eigenständigen strafrechtlichen Akteur aus und favorisierte Modelle der Verbands- und Kollektivhaftung. Dr. *Kerstin Waxnegger* analysierte sodann die Risiken generativer und „agentischer“ KI. Zu diesen zählten Täuschung, automatisierter Betrug sowie Markt- und Wahlmanipulation. Sie betonte, dass bestehende Strafnormen technologieneutral seien und weitestgehend ausreichen würden, auch bei autonom agierenden Systemen. Die KI-VO klassifiziere Risikoklassen, wodurch potentielle neue Straftatbestände eher bereichsspezifisch als generisch entwickelt werden sollten. Konkrete Gefährdungsdelikte könnten präventiv wirken, Überkriminalisierung sei jedoch zu vermeiden. Am Beispiel des Vorschlags einer Neuregelung in § 201b StGB zu Deepfakes zeigte sie Chancen und Risiken neuer Tatbestände auf. Zwar könnten Schutzlücken geschlossen und Persönlichkeitsrechte gestärkt werden, zugleich drohten unbestimmte Tatbestände, Doppelregulierungen und Vollzugsprobleme. Ihr Fazit: Anpassungen des Strafrechts könnten punktuell sinnvoll sein, müssten jedoch eng, anwendungsbezogen und strikt als ultima ratio ausgestaltet werden. Den abschließenden Vortrag hielt LOSTA *Thomas Goger* und näherte sich dem Thema „GenAI-Angriffsfläche und Angriffsvektor auch für Straftaten“ aus dezidiert praxisorientierter Perspektive. KI werde bereits als Werkzeug bei Cybercrime genutzt, beispielsweise für Phishing, Social Engineering oder Malware-Generierung. Agentic-AI ermögliche automatisierte Übergriffe über alltägliche Tools wie beispielsweise Kalendereinträge. Insbesondere lokal betriebene Sprachmodelle ohne „Safety Training“ eröffneten Missbrauchspotentiale, die regulatorisch kaum erreichbar seien. Ebenso seien Deepfakes und KI-generierte Kinderpornografie realisierte Bedrohungen. Er betonte, dass sich die Strafverfolgung auf alltäglichen KI-Missbrauch einstellen müsse, da die Technologie bereits im Feld der Straftäter angekommen sei.

RA'in *Hannah Milena Piel* moderierte die anschließende Fragerunde des letzten Panels bevor sie das Schlusswort an RA Dr. *Thomas Nuzinger* übergab. Dieser schloss die Tagung mit der Erkenntnis, dass Strafrecht und KI keine Science-Fiktion mehr sei, sondern Realität. Wir verfügten bereits über ein strafrechtsdogmatisches Rüstzeug, das nun ins „Fine-Tuning“ zu bringen sei.