Rechtsanwältin Dr. Katharina Funcke

Tagungsbericht „Junges Wirtschaftsstrafrecht 7.0 – Technologic Technologic Technologic" am 10.10.2025

Die Tagung des Jungen Wirtschaftsstrafrechts fand auch in ihrer 7. Auflage in Frankfurt am Main und online statt. Sie beleuchtete das Thema „Wirtschaftsstrafverfahren und technologischer Fortschritt" aus einer Vielzahl unterschiedlicher Perspektiven. Dabei gelang es erneut, Theorie und Praxis in offenen Austausch miteinander zu bringen.

Grußwort

Der Schirmherr Prof. Dr. Matthias Jahn (Goethe Universität Frankfurt am Main) eröffnete die Tagung mit einem Grußwort, in dem er anhand aktueller Beispiele auf diverse Herausforderungen hinwies, die Technik und KI sowohl für den Justizstandort Deutschland, die Rechtspflege, die Beratungsbranche als auch die Wissenschaft bereithalten.

Panel I: Grundlagen

Die Moderation des ersten Panels „Grundlagen" übernahm sodann Prof. Dr. Charlotte Schmitt-Leonardy (Universität Bielefeld). In ihrer Einführung mahnte sie die Bewahrung zur Kritikfähigkeit im Umgang mit Technologie an. Sie nahm insofern Bezug auf Winfried Hassemer, der davor warnte, sich mit normativen Konzepten zu befassen, ohne deren Bezugsgegenstand zu kennen. Vielmehr müsse eben dieser ernst genommen und hinterfragt werden. Ziel sei, so Schmitt-Leonardy, weder besonderer Optimismus noch Technologiefeindlichkeit, sondern vielmehr ein Kontextualisieren.

Den ersten Vortrag des Tages hielten StAin GrL Britta Strelitz und StA Andreas Herzog zu dem Thema Cyberkriminalität. Sie berichteten aus ihrer Praxis in der auf Cybercrime und Geldwäsche spezialisierten, im Juli 2024 neu gegründeten Abteilung bei der Staatsanwaltschaft Nürnberg-Fürth. Sie seien dort zuständig für das Massengeschäft der Cyberkriminalität. KI, z.B. für Deepfakes, spiele derzeit noch keine Rolle. Vielmehr sei Hauptkriminalitätsphänomen das sog. Phishing, also das „Abfischen" von Daten. Täter zielen dabei auf persönliche Daten wie Namen und Adressen, Kreditkartendaten und Kontodaten inklusive Passwörter für Onlinebanking. Diese abgefischten Daten werden für die Einrichtung von Girokonten im Namen der unwissenden Geschädigten verwendet, um damit weitere Straftaten wie Betrug und Geldwäsche zu begehen. Auch Waren werden häufig auf Rechnung der Betroffenen bestellt.

StAin Strelitz präsentierte typische Phishing-Methoden wie das App-Tester- und das Verpacker-Scheme. Bei dem App-Tester-Scheme würden gutgläubige Personen angeworben, die Banking-Apps vermeintlich testen und bewerten sollen. Ihnen werde vorgespiegelt, es handele sich lediglich um Testläufe; tatsächlich würden mit den von ihnen eingegebenen Daten aber echte Konten eröffnet, die sodann zur Begehung weiterer (Betrugs- und Geldwäsche-)Taten genutzt würden. Das Verpacker-Scheme bediene sich gutgläubiger Minijobber, die nach Ankündigung Tatbeute (häufig hochwertige Elektrogeräte) umverpacken und weiter versenden sollen. Bei Sachverhalten der Abteilung sei in der Regel der Tatbestand des (Computer-)Betrugs sowie der Fälschung beweiserheblicher Daten erfüllt. Die Schadenssummen bewegten sich maximal im niedrigen dreistelligen Bereich. Vor besondere Schwierigkeiten stelle aber die Ermittlung die Identität der Täter: Die Geschädigten bemerkten die Tat oftmals erst nach einiger Zeit, sodass die Ermittlungen mit größerer Zeitverzögerung aufgenommen werden. Zudem führten Geldflüsse regelmäßig nicht zu den Tätern, sondern zu gutgläubigen Dritten.

StA Herzog führte sodann aus, dass sich die Staatsanwaltschaft häufig mit Nachweisproblemen konfrontiert sehe, ob jene Dritte leichtfertig i.S.d. § 261 Abs. 6 StGB gehandelt hätten – also aus Gleichgültigkeit oder grober Unachtsamkeit, obwohl sich die Herkunft des Gegenstands unter Berücksichtigung individueller Fähigkeiten und Kenntnisse aufdrängte. Bewährt habe sich mit Blick auf die Zukunft ein „Bösgläubig-Machen". Dabei füge die Staatsanwaltschaft der Einstellungsmitteilung eine Erklärung bei, sodass sich die vormals Beschuldigten nicht nochmal mit dem Hinweis, nicht gewusst zu haben, was sie taten, gegen die Strafverfolgung wehren könnten. Zudem würden die Möglichkeiten der Vermögenssicherungsmaßnahmen ausgeschöpft – das Geld erhielten die Dritten jedenfalls nicht zurück. StA Herzog schloss mit dem Appell an das Plenum, stets auf die eigenen Daten aufzupassen.

Die anschließende Diskussion drehte sich insbesondere um praktische Fragen der Einziehung in diesem Kontext, wie die Dauer und Höhe der Sicherungsmaßnahmen. Es kristallisierte sich ferner die Besorgnis heraus, dass Verfahrenseinleitung und Kontoeinfrierung erhebliche Auswirkungen auf die betroffenen Personen haben, insbesondere angesichts der Weite des § 261 StGB aber problematisch erscheinen und oftmals nicht die verantwortlichen Täter treffen. Es zeigte sich, dass in der praktischen Handhabung teils erhebliche Unterschiede zwischen den Bundesländern herrschen.

Doktorand Leonardo Braguinski referierte sodann zu dem grundlagenbezogenen Thema „Die Signatur des Digitalen im Strafrecht". Er beschrieb zunächst das neue Gepräge, das Digitaltechnik mit sich bringe: Digitale Welten seien immersiv (man tauche regelrecht in diese ein) und diese Wirkung werde absichtlich verstärkt. Dies führe zu mehreren ethischen Implikationen. Menschliche Schwäche werde ausgenutzt, indem Nutzerinnen und Nutzer nach Digitaltechnik süchtig gemacht würden. So sei der Mensch zwar Eigentümer des digitalen Produkts, aber ohne Kenntnis von dessen Funktionsweise und Urheberschaft, was zu einem Kontrollverlust führe. KI-Chatbots genössen eine Sonderstellung – ihnen würde mehr anvertraut als in manchem Beichtstuhl oder bei Therapien. Die Chatverläufe glichen Tagebüchern. Da diese Daten grundsätzlich sichergestellt werden könnten, führe

der digitale Fortschritt zu einer neuen Macht der Strafverfolgungsbehörden. Diese seien unstreitig effektiver geworden, riesige Datenmengen könnten ausgewertet und per Selbstleseverfahren in den Prozess eingeführt werden. Die Verteidigung könne dem wenig entgegensetzen – auch Sachverständige könnten die Ergebnisse der Ermittlungsbehörden nur ex post und von außen überprüfen. Herr Braguinski benannte dies als Herausforderung für den Grundsatz der Waffengleichheit und postulierte daher ein Gebot der Transparenz für Behörden.

Anknüpfend daran wandte er sich der bisherigen Reaktion der Rechtsprechung zu, die zwar die allgegenwärtige Nutzung von Smartphones sowie die Verwebung von Technik und Lebenswirklichkeit erkannt habe, aber die Bedeutung der Digitalität noch nicht ausreichend berücksichtige. So habe etwa der BGH in seiner viel beachteten Entscheidung zur zwangsweisen Entsperrung von Smartphones per Fingerauflegen (Az. 2 StR 232/24) den Unterschied zwischen Digitalisierung und Digitalität verkannt. Digitalisierung beschreibe die bloße Art und Weise der Abwicklung, die alternativ auch analog möglich wäre – z.B. die (digitale/analoge) Abnahme von Fingerabdrücken. Dagegen wäre es ohne Digitalität nicht möglich gewesen, dieselben Erkenntnisse ohne den Einsatz von Zwang zu erlangen. Herr Braguinski sah angesichts dieses neuen Wissensvorsprungs der Behörden die Rechte der Beschuldigten in Gefahr, denen die klassischen Prozessmaximen keinen ausreichenden Schutz böten. Die Rechtsprechung erkenne dies bislang nur teilweise. Aus seiner Sicht gebe es aktuell keinen normativen oder dogmatischen Weg, die Smartphone-Beschlagnahme zu verhindern. Zugleich dürfte aus Sicht des Gesetzgebers angesichts der Bestätigung der Zwangsentsperrung durch den BGH kein Änderungsbedürfnis bestehen. Es wurde die Frage aufgeworfen, wie man künftig rechtsstaatliche Kernanliegen auf KI-Ebene denken könne. Mangelnde Ressourcen dürften jedenfalls kein rechtspolitisches Argument sein. Als Ausblick stellte Herr Braguinski in den Raum, dass künftig mit einer Vergünstigung der Technik und dadurch einem überaus mächtigen digitalen Staatsapparat zu rechnen sei.

Den nächsten Vortrag „Künstliche Intelligenz – Revival der strafrechtlichen Produkthaftung" steuerte RA Dr. Mustafa Enes Özcan bei.

Einführend erläuterte er die Bedeutung strafrechtlicher Produkthaftung, deren prominentestes Beispiel die Lederspray-Entscheidung des BGH darstellt. Auch KI-Produkten, wie autonom fahrenden Fahrzeugen oder Medizinprodukten, könne ein erhebliches Schadenpotenzial innewohnen. Sofern ein Schaden entstehe, sei regelmäßig Kernstrafrecht einschlägig, namentlich Körperverletzungs- und Tötungsdelikte. Zentrale Frage sei hier die der Zurechenbarkeit. Besonderheiten stellten sich hier, weil KI – anders als festen Regeln folgende herkömmliche Algorithmen – selbstlernend agiert. Aufgrund verborgener Schichten zwischen Ein- und Ausgabeschicht (sog. Black Box) seien Ergebnisse nicht immer nachvollziehbar.

Im Rahmen der Fahrlässigkeitsstrafbarkeit gem. §§ 222, 229 StGB stellten sich zunächst bei der Prüfung der objektiven Sorgfaltswidrigkeit Schwierigkeiten. Denn KI sei trotz der KI-VO aktuell relativ schwach reguliert, sodass die Anforderungen an die bei der Herstellung erforderlichen Sorgfalt nicht auf gesetzliche Normen gestützt werden könnten. Ein denkbarer Fehler wären jedenfalls zu wenige bzw. falsche Trainingsdaten bei dem Training der später defizitären KI. Auch dann bedürfte es aber ferner des Nachweises eines Pflichtwidrigkeitszusammenhangs, also der Kausalität zwischen Sorgfaltswidrigkeit und Taterfolg. Die herrschende Meinung vertrete in dieser hoch streitigen Frage die Vermeidbarkeitsthese, fordere also eine an Sicherheit grenzende Wahrscheinlichkeit dafür, dass der Taterfolg ohne die Pflichtwidrigkeit ausgeblieben wäre. Dies werde sich aber wegen der Black-Box-Eigenschaft nicht sicher ermitteln lassen. Zu einem anderen Ergebnis könnte nur die Risikoerhöhungslehre gelangen, die aber von der Rechtsprechung nicht vertreten werde. Im Ergebnis sei daher eine Fahrlässigkeitsstrafbarkeit quasi ausgeschlossen.

RA Dr. Özcan führte weiter aus, dass auch eine Strafbarkeit wegen Vorsatzdelikten durch Unterlassen schwerlich feststellbar sei, wenn beispielsweise nach Markteinführung Fehler der KI erkannt würden. Zwar werde man eine Verletzung von Garantenpflichten bejahen müssen, wenn der Hersteller in einem solchen Szenario keine Maßnahmen (Warnung, Rückruf, Update) ergreife. Nichtsdestotrotz stellten sich bei der Prüfung der hypothetischen bzw. Quasikausalität dieselben Nachweisprobleme wie beim Merkmal des Pflichtwidrigkeitszusammenhangs. Das Fazit sei ernüchternd: De lege lata scheide eine Strafbarkeit trotz Fehlbarkeit der KI auch hier regelmäßig aus.

Vor diesem Hintergrund stellte RA Dr. Özcan die Frage, ob und ggf. wie auf ein ungestilltes Strafbedürfnis reagiert werden sollte. Er präsentierte abschließend verschiedene Vorschläge, die insofern in Rede stehen – von der reinen/abstrakten Gefährdungshaftung über eine objektive Bedingung der Strafbarkeit bis hin zu einer Unternehmenssanktionierung. Diese diskutierten die Teilnehmerinnen und Teilnehmer sodann gemeinsam. Zur Sprache kamen dabei auch zu bedenkende Nachteile, wie eine drohende Bremse technischer Innovation und die Zwickmühle, dass eine Produktverbesserung durch erheblich mehr Trainingsdaten rechtsstaatliche Grundsätze tief betreffe.

Vergabe WisteV Preis

Der Tradition entsprechend wurde auch in diesem Jahr der Preis für die beste wirtschaftsstrafrechtliche Dissertation aus der Perspektive der Praxis verliehen, den die WisteV traditionell zur Nachwuchsförderung vergibt. RAin Dr. Ricarda Schelzke hielt im Namen der WisteV die Laudatio. Gekürt wurde die bei Duncker & Humblodt veröffentlichte Dissertation von Dr. Juliane Schwarz-Ladach (Universität Rostock): „Bestechlichkeit und Bestechung von Mandatsträgern gemäß § 108e StGB – Eine Untersuchung der Strafbarkeit de lege lata und de lege ferenda unter besonderer Berücksichtigung auch des § 108f StGB".

Panel II: Materielles Recht

Nach der Mittagspause setzte das zweite Panel die Tagung fort, das sich nunmehr materiellem Recht zuwandte und von RA Dr. Moritz Lange moderiert wurde.

PD Dr. Andreas Werkmeister machte die Teilnehmerinnen und Teilnehmer mit den Perspektiven eines Datenwirtschaftsvölkerstrafrechts hinsichtlich (vermeintlich?) neutraler Plattformen vertraut. Er legte die Bedeutung der Datenwirtschaft dar und zeigte auf, dass Plattformen wie X (früher Twitter), Youtube oder Meta (früher Facebook) auf maximale Nutzungszeit und maximale Datensammlung ausgelegt seien. Shoshana Zuboff habe in diesem Zusammenhang den Begriff des allgegenwärtigen „Überwachungskapitalismus" geprägt, der als instrumentäre Macht diene. Angesichts dieses erheblichen Einflusses solcher Plattformen warf Werkmeister die Frage auf, unter welchen Umständen der Hass gegen Minderheiten eine Strafbarkeit der Plattform-Verantwortlichen auslösen könne.

Der Cambridge-Analytica-Skandal, bei dem die unrechtmäßige Datenauswertung von Millionen Nutzerdaten durch Facebook bekannt geworden war, habe gezeigt, dass jedenfalls deutsches Recht nicht jenseits des § 42 BDSG den strafrechtlichen Schutz des Kollektivs abbilde. Sodann richtete PD Dr. Werkmeister den Blick auf das Völkerstrafrecht.

In dem Fall der Repression und Vertreibung der Rohingya aus Myanmar habe der IStGH Verbrechen gegen die Menschlichkeit festgestellt. Diese Gewalt sei durch massive Hate Speech auf Facebook begleitet und mitinitiiert worden. Hass generiere die meiste Nutzungszeit – folglich habe der Algorithmus immer weitere Hassvideos empfohlen, ohne dass eine Moderation stattgefunden habe. Doch inwiefern könnte in einem solchen Fall eine strafrechtliche Verantwortlichkeit auch der Plattformbetreiber bestehen?

Historische Anknüpfungspunkte bestünden z.B. anhand des Internationalen Militärgerichtshofs gegen Julius Streicher im Jahr 1945. Der Herausgeber eines Nazi-Hetzblatts wurde wegen eines Verfolgungsverbrechens gem. Art. 6 lit. d. IMG-Statut verurteilt, das bereits ein Aufhetzen unabhängig von Kausalität für eine konkrete Tat völkerstrafrechtlich erfasste. Dieser Ansatz sei 1994 durch den IStGH für Ruanda im Prozess gegen den Direktor eines Radiosenders, der rassistische Hassbotschaften und Aufrufe zur Ausrottung verbreitet hatte, vertieft worden. Er wurde u.a. wegen „Aufwiegelung zum Völkermord" verurteilt. Dies zeige, so Werkmeister, dass unter bestimmten Umständen auch Vorbereitungshandlungen strafbar sein können.

Weiter zeigte er die Überschneidung zum Wirtschaftsstrafrecht auf: Es gehe um Wirtschaftsakteure, die von dem Hass monetär profitierten. In Fällen wie dem Rohingya-Fall stelle sich die Frage, ob Betreiber bewusst einen hasserfüllten Algorithmus ohne strafrechtliche Konsequenzen weiterlaufen lassen dürften – oder ob nicht zum Schutz von Minderheiten mehr getan werden müsste.

Eine Teilnahmestrafbarkeit nach dem IStGH-Institut setze jedenfalls eine Haupttat in Form der Verfolgungsverbrechen und Aufhetzung zum Völkermord (Art. 25 Abs. 3 lit. c oder lit. d IStGH-Statut) voraus. Dabei sei aber die deutsche Diskussion zu neutraler Beihilfe nicht übertragbar, da dolus eventualis im Völkerstrafrecht generell keine Strafbarkeit begründe. Kenntnis wiederum sei den Plattformbetreibern schwer nachweisbar. Auch wenn diese Beweisprobleme im Einzelfall überwunden würden, sei unklar, ob auch in objektiver Hinsicht die Schwelle des erlaubten Risikos überschritten sei. Dies sei zum Beispiel nicht bereits bei bloßer Überschreitung von Community-Regeln zu bejahen. Vielmehr bedürfe es einer inneren Verbindung – etwa, wenn verhetzende Inhalte so massiv verbreitet seien, dass sie der Gesamtausrichtung der Plattform ein Gepräge gäben.

Werkmeister zog das Fazit, dass eine völkerstrafrechtliche Verantwortlichkeit zwar nur eingeschränkt greifen dürfe, eine Strafbarkeit aber nicht ausgeschlossen sei. Mächtige dürften gerade nicht deshalb aus den Augen gelassen werden, weil sie besonders mächtig seien.

Im nächsten Vortrag beschäftigte Dr. Lena Leffer sich mit „Geldwäschebekämpfung durch Automated Suspicion Algorithms". Einführend benannte sie die durch Geldwäsche hervorgerufenen Schäden: So drohe eine Schattenwirtschaft und Marktverzerrung. Darüber hinaus liefere das erfolgreiche Waschen von Geld auch Anreize für weitere Vortaten und diene zugleich der Finanzierung weiterer Taten als sog. engine of crime. Auch gehe mit der Geldwäsche ein erheblicher Verlust von Steuereinnahmen und – schlimmstenfalls – gar ein Vertrauensverlust in den Rechtsstaat einher.

Dr. Leffer erläuterte die in drei Phasen unterteilte Funktionsweise der Geldwäsche. Erst gelte es aus Sicht Krimineller, beim sog. Placement Bargeld in den Kreislauf einzuspeisen, also zu Buchgeld zu machen. Beim sog. Layering werde anschließend die Herkunft des Geldes verschleiert und dieses schließlich bei der sog. Integration in neue Geschäfte investiert. Die Entdeckung von Geldwäschetaten durchlaufe ihrerseits ebenfalls regelmäßig mehrere Stufen: Banken erstellten Verdachtsmeldungen, die durch die FIU analysiert und ggf. an die Strafverfolgungsbehörden weitergeleitet würden. Dabei demonstrierten die Weiterleitungsquoten überdeutlich, dass das System wenig effektiv sei. Auf 340.000 Meldungen kämen 1.000 Urteile/Anklagen (wobei auch insofern eine Kausalität nicht sichergestellt sei). D.h., die Aufklärungsquote liege bei unter 1 %.

Dr. Leffer zeigte auf, dass trotz dieser unbefriedigenden Ausgangslage der Einsatz von KI kein Allheilmittel sei. Denn ein unregulierter Einsatz berge ebenfalls ein Schadensrisiko, konkret durch die Gefahr einer blinden automatisierten Navigation bei der automatisierten Informationsgewinnung und -verkettung. Systeme wie Palantir, Google, HAWK, Vespia, IBM oder Napier hätten jeweils eigene Geldwäsche-KI, die jedoch ohne staatliche Regulierung und Rechtsgrundlage agierten und an False-Positive-Rates von bis zu 99% litten. Diese Systeme fielen nicht unter die Hochrisiko-Definition der EU, sodass sich Anforderungen nur aus Datenschutzrecht und, so Dr. Leffer, aus der EMRK ergäben. Ihr Lösungsvorschlag sah daher ein zweigleisiges KI-System vor: Anonymisierte Meldungen an die FIU unter Einsatz von KI, die neue Begehungsweisen erkenne, und diese dann an die Banken zurückspielen. Auf diese Weise könne eine Datenbank mit Mustern neuer Begehungsweisen aufgebaut werden.

RA Niklas Wolf, LL.M. beleuchtete sodann Grundlagen und Probleme bei der Einziehung von Kryptowerten aus Perspektive der Verteidigung. Zum weiteren Verständnis umriss er zunächst die rechtlichen Definitionen von Kryptowerten und zeichnete deren wichtigste Merkmale an deren bekanntestem Beispiel, dem Bitcoin, nach. Kennzeichnend sei u.a. die dezentrale Aufzeichnung ohne Verzeichnis. Man benötige einen private key zum Zugang der Wallet, in welcher die Kryptowerte ähnlich einem Bankkonto gespeichert würden. Dabei sei die Dokumentation von Transaktionen, die in der Blockchain erfolge, öffentlich einsehbar.

Die gegenständliche Einziehung, also die Einziehung von direkt erlangten Kryptowerten, sei unproblematisch möglich; ebenso die von Surrogaten. Spannend sei hingegen die Wertersatzeinziehung gem. § 73c Satz 1 StGB. Meistens kenne die Staatsanwaltschaft nämlich nicht den für den Zugriff benötigten private key zum Zugriff auf die Wallet. Es stelle sich daher die Frage, ob somit die Einziehung unmöglich werde, oder es sich um ein reines Vollstreckungshindernis handele. Diese Unterscheidung sei von erheblicher Relevanz, weil sie sich auf den Zeitpunkt der Einziehung auswirke und sich der Wert von oft volatilen Kryptowährungen aufgrund von Kursschwankungen erheblich ändere.

Mit Blick auf das Sicherungsverfahren vertrat RA Wolf die These, dass die bestehenden gesetzlichen Regelungen nicht recht für Kryptowährungen passten, in der Praxis aber dennoch herangezogen würden – letzten Endes seien die §§ 111b ff. StPO subsumierbar. Sofern die Sicherstellung möglich sei, d.h. bei Vorliegen der private key, erfolge sie per Übertragung der Kryptowerte auf staatliche Wallets. Betreffend die spätere Verwertung von gesicherten Kryptowerten hob RA Wolf die Möglichkeit der Notveräußerung im Sicherungsverfahren bei drohendem Kursabsturz hervor. Für Betroffene sei freilich von erheblicher Bedeutung, wer hier das Risiko von Kursschwankungen trage.

Schließlich wurde der Blick auf die Phase nach Verfahrensabschluss gerichtet. Insofern sei § 77a StVollstrO maßgeblich. § 77a Abs. 2 Satz 1 StVollstrO sieht vor, dass die zu verwertenden virtuellen Währungen den in den Ländern bestimmten Zentralstellen zur Verwertung anzuzeigen und durch diese zu verwerten sind. So werde auf Länderebene entsprechendes know how gebildet. Unter den Voraussetzungen der §§ 77a Abs. 3, 66 Abs. 1 StVollstrO können Kryptowerte gar den Ermittlungsbehörden für Zwecke der Justizverwaltung zugewiesen werden, wenngleich bislang kein solcher Fall bekannt sei.

Der tatsächliche Zugriff auf Kryptowerte bzw. Bitcoin gestalte sich regelmäßig schwierig. Während die Blockchain zwar öffentlich einsehbar sei, bleibe deren Aufbereitung mühsam und die Identifizierung der jeweiligen Wallet-Inhaber äußerst schwierig. Sowohl kommerzielle Anbieter als auch Ermittlungsbehörden sammelten hierfür Daten zum Aufbau von Datenbanken. Da größere Umsätze die Einschaltung einer „Börse" erfordere, bei denen KYC-Erfordernisse bestünden, seien die Ein- und Ausgangspunkte eine Chance, Personen zu identifizieren.

Panel III: Strafprozessrecht

Zu technischen Ermittlungen nach der StPO – also Maßnahmen, die auf technischen Hilfsmitteln beruhen bzw. unter deren Einsatz erfolgen – in Wirtschaftsstrafverfahren referierte RA Dr. Lukas Schefer. Er zeigte zunächst die besondere Bedeutung insbesondere technischer offener Maßnahmen in datengetriebenen Wirtschaftsstrafverfahren auf. Seine weitere Betrachtung untergliederte er nach den unterschiedlichen Phasen des Zugriffs auf IT-Systeme (Sicherung zur Durchsicht – Beschlagnahme – Auswertung) und nahm die damit in der Praxis einhergehenden, oft ungeklärten Probleme in den Blick.

Im Rahmen von Durchsuchungen etwa erfolge vielfach bereits eine Auswertung, obwohl § 110 Abs. 1 StPO lediglich eine Durchsicht gestatte. Das BVerfG habe dem eine Absage erteilt und auch ein Antrag analog § 98 Abs. 2 Satz 2 StPO hatte jüngst vor dem LG Hamburg Erfolg. Gegenwehr der Verteidigung führe jedoch dazu, dass die Ermittlungsbehörden dann einen Antrag auf Beschlagnahme stellten, die dann regelmäßig erfolge. RA Dr. Schefer kritisierte, dass eine bewusste Umgehung des Richtervorbehalts ein Beweisverwertungsverbot nach sich ziehen müsste. Auch dürften nicht pauschal alle sichergestellten Gegenstände beschlagnahmt werden, da dies die Grenzen der Angemessenheit überschreite.

In der ersten Phase der Durchsicht könne sich darüber hinaus eine Vielzahl weiterer Problemen stellen – von der Frage nach dem Umfang der zulässigen Durchsicht gem. § 110 Abs. 3 Satz 1 StPO, dem Bestehen eines Anspruchs auf Spiegelung des Datenbestands, überlange Verfahrensdauern und Anwesenheitsrechte der Verteidigung bis hin zur Auslagerung der Durchsicht an Private.

Betreffend die zweite Phase der Beschlagnahme erinnerte RA Dr. Schefer daran, dass diese gem. § 94 Abs. 2 StPO auch Verhältnismäßigkeit voraussetze. Ein Exzess müsse daher verhindert und der Zugriff auf Notwendiges beschränkt werden, z.B. im Wege von Suchwortlisten. RA Dr. Schefer wies darauf hin, dass dementgegen das LG Bonn entschieden habe, eine Eingrenzung müsse nur kursorisch und für evident nicht Beweiserhebliches erfolgen. Er folgerte hieraus, dass nach dieser Ansicht nur der Bearbeitungsprozess angreifbar sei. Dringe die Verteidigung mit ihrer Kritik an einem Zugriffsexzess durch, stelle sich das Folgeproblem des Umfangs des Löschanspruchs.

Zur letzten Phase, der Auswertung, stellte RA Dr. Schefer sodann die divergierenden Meinungen betreffend deren Rechtsgrundlage vor. Hier stelle sich erneut die Frage, ob den Ermittlungsbehörden ein Outsourcing bzw. der Einsatz von KI gestattet sein sollte. Nach Ansicht von RA Dr. Schefer bedürfte es hierfür einer eigenständigen Rechtsgrundlage. De lege ferenda forderte er daher die Regelung des KI-Einsatzes durch Ermittlungsbehörden bei der Auswertung. Abschließend wies er zudem auf Friktionen beim Zugriff auf IT-Systeme hin: Der offene Zugriff habe sehr niedrige Voraussetzungen im Vergleich zum verdeckten Zugriff. Dies sollte angesichts der Eingriffsintensität auch des offenen Zugriffs angepasst werden.

RAin Dr. Anne Ulrichs Vortrag behandelte den Umgang mit Daten aus internen Untersuchungen.

Im Ausgangspunkt habe die Jones-Day-Entscheidung bereits im Jahr 2018 gezeigt, dass Daten aus internen Untersuchungen nach der Rechtsprechung beschlagnahmefähig seien. Zu denken sei etwa an Protokolle von Interviews, eigene EDV-Auswertungen, Memos, Gutachten etc. Fraglich sei aber, ob der Zugriff auch auf im Ausland liegende Daten zulässig sei, zumal sich die Jones-Day-Entscheidung hierzu nicht verhalte. Unproblematisch sei jedenfalls der Zugriff auf öffentliche Daten und ein Zugriff mit Einverständnis. Die Rechtsprechung sei uneins, ob § 110 Abs. 3 StPO auch darüber hinaus zum Zugriff auf nicht in Deutschland liegende Daten berechtige. Eine landgerichtliche Entscheidung habe dies unter Verweis auf das Souveränitätsprinzip abgelehnt. Ein Teil der Lehre lasse dagegen die bloße tatsächliche Erreichbarkeit der Daten vom Inland aus genügen. Die differenzierenden Entscheidungen des LG Koblenz und LG Berlin hatten den Zugriff zugelassen, wenn nicht feststellbar sei, wo die Daten liegen, bzw. der Zugriff unter Verwendung eines bei der Durchsuchung aufgefundenen Passworts erfolge. RAin Dr. Ulrich kritisierte die ergebnisorientierte Auslegung.

Anschließend wandte RAin Dr. Ulrich sich (unter Ausklammerung des Berufsrechts) möglichen Risiken zu, die in diesem Zusammenhang entstehen können. So analysierte sie die Frage, ob die bewusste Speicherung im Ausland eine strafbare Tathandlung gem. § 258 StGB darstellen könne. Hier näherte sich RAin Dr. Ulrich der Lösung über das Verteidigerprivileg an und zog den Grundsatz heran, dass prozessual zulässiges Verhalten nicht strafbar sein könne. Es bestehe keine pauschale Pflicht zur Bereithaltung der Daten für behördlichen Zugriff. Immerhin dürfte auch die (freiwillige) Herausgabe nicht erzwungen werden. Problematischer könne dagegen die aktive Löschung im Inland sein. Einerseits habe die aktive Löschung im Unterschied zur bloßen Speicherung möglicherweise eine andere Qualität. Andererseits bestehe auch insoweit keine prozessuale Pflicht zum Bereithalten der Daten. RAin Dr. Ulrich kam deshalb zu dem Schluss, dass ebenfalls eine Strafbarkeit abzulehnen sei, wenngleich die Rechtsprechung den Fall noch nicht entschieden habe.

Der Zugriff auf Daten im Ausland könne somit am ehesten vermieden werden bei statischem, klar dokumentierten Speicherort, sofern die Zugriffsdaten nicht für die Ermittlungsbehörden verfügbar seien. Die Rechtsprechung hierzu sei noch „im Fluss". De lege ferenda sei die Beschlagnahmefreiheit der Auslandsdaten zwar wünschenswert, aber praktisch unwahrscheinlich. In der nachfolgenden Diskussion kristallisierte sich u.a. heraus, dass jedenfalls Beschuldigte äußerste Vorsicht walten lassen müssten, weil Strafverfolgungsbehörden möglicherweise bei der Löschung von Daten von dem Haftgrund der Verdunkelungsgefahr ausgehen würden. Auch die Zulässigkeit verschiedener Handlungsoptionen von Rechtsanwältinnen und Rechtsanwälte wurde diskutiert.

Den letzten Vortrag des Tages hielt, online zugeschaltet, Nathalia Schomerus, MSt (Oxford), die derzeit als Legal Innovation Lead bei dem KI-Anbieter Legora tätig ist. Unter dem Titel „Technik und Trends in der Investigation und Compliance" legte Frau Schomerus dar, wie niedrigschwellig KI bereits heute (auch) in diesen Bereichen genutzt werden könne. Gerade für Interne Untersuchungen, in denen oftmals riesige Datenmengen auszuwerten seien, biete sich der Einsatz von KI an. Anhand einiger Beispiele demonstrierte Frau Schomerus live, wie etwa eine Vielzahl an Dokumenten analysiert, ausgewertet und aufbereitet werden könnte. Die Möglichkeiten hätten sich deutlich verbessert; so könne die KI nunmehr auch handschriftliche Aufzeichnungen auswerten und sei im Preis gesunken.

Problematisch sei aber zum einen, dass man sich mit der KI auch Bias einkaufe. Mittels Testfragen an eine chinesische und amerikanische KI legte Frau Schomerus dar, dass vor politischen Hintergründen auch stereotyp geprägte, unzutreffende oder mit den rechtsstaatlichen Standards in Deutschland unvereinbare Antworten generiert werden können. Zum anderen hob Frau Schomerus die Wichtigkeit eines ausreichenden (Daten)Schutzniveaus bei der beruflichen Verwendung von KI hervor. Insbesondere wies sie auf § 43e Abs. 4 BRAO hin, der die berufsrechtlichen Anforderungen bei der Inanspruchnahme von Dienstleistungen regelt. Aus Frau Schomerus Sicht unverzichtbar seien eine ISO-Zertifizierung, aufgrund von Berufsrecht eine in der EU gelegene Serverinfrastruktur, ggf. aus Datenschutzgründen sogar ein europäisches Unternehmen sowie Chinese Walls, die eine Datenweitergabe zu Trainingszwecken verhinderten.

In der anschließenden Diskussion wurden weitere Möglichkeiten des KI-Einsatzes im beruflichen Alltag erörtert, wie die sekundenschnelle Überprüfung von Zeugenaussagen auf Widersprüche im Rahmen der Hauptverhandlung. Zugleich wurde deutlich, dass Halluzinationen der KI noch immer ein ernstzunehmendes Problem darstellen. Frau Schomerus riet insofern, sowohl dem Stellen der richtigen Fragen (sog. Prompting) als auch der Auswahl der richtigen Tools besondere Aufmerksamkeit zu widmen: So nutze man für eine Rechtsrecherche beispielsweise den bei Beck veröffentlichten Aufsatz anstelle des Reddit-Forums.

Schluss

RAin Dr. Schelzke schloss die Tagung im Namen des WisteV-Vorstands und bedankte sich bei allen für den angeregten Austausch zu dem facettenreichen Oberthema. Zu den Klängen von Daft Punks „Technologic" entließ sie die Teilnehmerinnen und Teilnehmer zum anschließenden Get Together.