TAGUNGSBERICHT

Erlanger Cybercrime Tag 2025 – Digitale Beweismittel in der Hauptverhandlung

*von Franka Härtlein, Dipl.-Jur. Leila Khayati und Ass. iur. Tabea Seum**

Der Tagungsbericht enthält sprachlich bereinigte und teils vom Englischen ins Deutsche übersetzte Zusammenfassungen der Transkriptionen der Vorträge und Diskussionsbeiträge des Erlanger Cybercrime Tages 2025. Der Vortragsstil der einzelnen Beiträge wurde überwiegend beibehalten. Der Erlanger Cybercrime Tag 2025 und die Erstellung dieses Tagungsberichts wurden von der Dr. Germain-Schweiger-Stiftung gefördert.

I. Einleitung

Auch im Jahr 2025 öffnete der Wassersaal der Orangerie der Friedrich-Alexander-Universität wieder seine Tore für alle Cybercrime Interessierten. Am 20.3.2025 fand der 9. Erlanger Cybercrime Tag statt. Das hybride Konzept der Veranstaltung ermöglichte es auch dieses Jahr, dass sich zahlreiche Teilnehmende präsent oder auch virtuell austauschen konnten. Das Publikum war, wie auch in den vorherigen Jahren, bunt gemischt und setzte sich aus Vertretern der Wissenschaft, der Strafrechtspraxis, wie der Justiz als auch der Anwaltschaft, Fachvertreter:innen und auch Studierenden zusammen. Der angeregte Dialog in den Q&A-Sessions führte zu einem fruchtbaren Austausch aller. *Professor Dr. Christoph Safferling LL.M. (LSE)* und sein ICLU-Team waren hoch erfreut, dass sich mal wieder die Mühen im Vorfeld gelohnt hatten und eine erfolgreiche Tagung stattfinden konnte.

Gegenstand der diesjährigen Veranstaltung war das hochaktuelle und in der Fachliteratur wie auch in der Praxis intensiv diskutierte Thema "Digitale Beweismittel in der Hauptverhandlung". Die grenzüberschreitende Relevanz der Thematik spiegelte sich in der Beteiligung nationaler, sowie internationaler Referent:innen wider. Obwohl die Verwendung digitaler Beweismittel im Strafprozess längst keine Besonderheit mehr ist, bestehen mangels Regulierungen und Vorgaben Unsicherheiten im Umgang mit diesen. Im Rahmen der Veranstaltung wurde sich dabei unter anderem mit der Rolle des Sachverständigen befasst. Weiterhin wurde sich mit den unterschiedlichen Sprachsystemen der Rechtswissenschaft und Informatik und der damit einhergehenden Übersetzungsproblematik für Beteiligte auseinandergesetzt, Fragen und Herausforderungen mit Big Data, sowie der Durchsicht und Beschlagnahme von Datenträgern diskutiert und beleuchtet. Darüber hinaus wurde ein Blick auf den internationalen Umgang mit digitalen Beweismitteln geworfen und Reformvorschläge durch die Referent:innen präsentiert.

Eröffnet wurde die Tagung mit den Begrüßungsworten des Präsidenten der FAU Erlangen-Nürnberg, *Prof. Dr. Joachim Hornegger* und sich einer daran anschließenden Begrüßungsrede von *Professor Dr. Christoph Safferling, LL.M. (LSE),* wobei die zentralen Problemstellungen und Fragen der Thematik aufgegriffen und zugleich inhaltlich in den Themenbereich eingeführt wurde. Die Referent:innen, *Dr. Nicole Scheler* (DFG-Graduiertenkolleg 2475 Cyberkriminalität und Forensische Informatik), *Marion Liegl* (FAU Erlangen-Nürnberg), *Matthew Cross* (*IStGH* Den Haag), *Dr. Eren Basar* (Wessing&Partner) und Gregory Kochneff (BLKA) stellten die aufgeworfenen Fragen und Probleme dann anschaulich in ihren Vorträgen dar.

II. Die Beweiswürdigung des IT-Sachverständigen von Dr. Nicole Scheler (DFG-Graduiertenkolleg 2475 Cyberkriminalität und Forensische Informatik)

Den Erlanger Cybercrime Tag durfte dieses Jahr Frau *Dr. Nicole Scheler* mit ihrem Vortrag beginnen. Die ehemalige Doktorandin und noch Assoziierte des Graduiertenkollegs Cyberkriminalität und Forensische Informatik präsentierte die Ergebnisse ihrer jahrelangen Forschung und Dissertationsschrift, die sich mit der Beweiswürdigung des IT-Sachverständigen im deutschen Strafverfahren befasste.[1] In ihrem anregenden Vortrag führte sie das Publikum anhand eines juristischen Falles durch die theoretischen Kernaspekte, die bei der Beweiswürdigung des IT-Sachverständigen beachtet werden müssen.

1. Allgemeine Grundsätze zur Beweiswürdigung

Aufgrund des stetigen technologischen Fortschritts treffen vor Gericht oft zwei Wissenschaften aufeinander: die Rechtswissenschaft und die Informatik. Wohingegen erstere klare und deutliche Antworten verlangt, arbeitet die Informatik, als Naturwissenschaft mit Wahrscheinlichkeiten und Fehlerquoten. Diese gegensätzlichen Pole und

* *Franka Härtlein* ist und *Leila Khayati* war Studentische Hilfskraft am Lehrstuhl von *Prof. Dr. Christoph Safferling*, LL.M. (LSE) an der Friedrich-Alexander-Universität Erlangen-Nürnberg. *Tabea Seum* ist wissenschaftliche Mitarbeiterin im DFG Graduiertenkolleg 2475 Cyberkriminalität und forensische Informatik, sowie wissenschaftliche Mitarbeiterin am Lehrstuhl von *Prof. Dr. Christoph Safferling*.

1 vgl. *Scheler*, Die Tätigkeit der IT-Sachverständigen im deutschen Strafverfahren.

verschiedenen Sprachsysteme in Einklang zu bringen, ist Aufgabe des IT-Sachverständigen.

a) Die freie, richterliche Beweiswürdigung, § 261 StPO

Die freie richterliche Beweiswürdigung gem. § 261 StPO bedeutet, dass das Gericht aufgrund eigener, persönlicher und freier Überzeugung aus dem Inbegriff der Verhandlung, unabhängig von Beweisregeln formaler Art, eine Entscheidung trifft. Im Rahmen der Beweiswürdigung wird die Bedeutung des Beweises, seine mögliche Verwertung für den Tatvorwurf und die darauf aufbauende tatrichterliche Überzeugung eingeschätzt. Diese richterliche Überzeugung ist eine persönliche, subjektive Gewissheit von der objektiven Wahrheit, sodass es zur Erlangung dieser Wahrheit an einem sehr hohen Maß an Wahrscheinlichkeit bedarf, sowie der inneren Gewissheit der Richterin von der Wahrheit des Geschehens. Untermauert und begründet wird diese subjektive Ansicht durch Wissen und Argumente, die sich kommunikativ vermitteln lassen. Das Resultat der Wahrheitsfindung im Strafprozess sollte ein festgestellter Sachverhalt sein, der mit objektiv hoher Wahrscheinlichkeit mit der Wirklichkeit übereinstimmt. Begünstigt wird dies durch eine hohe Qualität der Tatsachenbasis. Eine solch hohe Qualität ergibt sich durch eine Nähe der Tatsachen zum subsumtionsfähigen Sachverhalt (Haupttatsache oder Indizien) und einer zuverlässigen Aussagekraft, mithin eines hohen Beweiswerts.

b) Abgrenzung eigene Wahrnehmung der Richter:innen und Notwendigkeit der Bestellung eines Sachverständigen

Ein eigenständiges Tätigwerden des Gerichts ist regelmäßig geboten, wenn es über ausreichend eigene Sachkunde verfügt. Dann können die Richter:innen selbstständig z.B. eine Inaugenscheinnahme oder eine Bewertung der Tatsachen, wie beim einfachen Lesen oder Nachzählen, vornehmen.

Nr. 69 RiStBV bestimmt, dass Sachverständige nur dann hinzugezogen werden sollen, wenn es für die Sachverhaltsaufklärung unentbehrlich ist. Dies lässt die Schlussfolgerung zu, dass es auf die Person der Richterin und des individuellen Kenntnis- und Wissensstands ankommen kann. Soweit eine Richterin mehr als nur Allgemeinwissen in der Forensik hat, kann sie die entsprechende Entscheidung in diesem Gebiet eigenständig treffen, wobei dann eine explizite Darlegung und Begründung im Urteil gefordert ist. Eine solche individuelle Sachkunde kann zum Beispiel durch repetitives Aufkommen der gleichen Problematiken und Lösungen in Fällen erworben werden, durch jahrelange Erfahrung auf diesem Gebiet oder Weiterbildungen.

Hingegen ist es nicht erlaubt, dass Richter:innen gezielt Wissen im Freibeweisverfahren erwerben und somit den Sachverständigen umgehen. Die Rechtsprechung hat dahingehend Fallgruppen fachfremder Gebiete herausgearbeitet, bei welchen sich Richter:innen die Beantwortung der Fragen nicht selbst zutrauen dürfen, wie im Bereich der Medizin oder Psychiatrie. Demgegenüber gibt es auch Standardfälle, bei welchen die richterliche Sachkunde als ausreichend erachtet wird – Stichwort: antizipierte Sachverständigengutachten. Beispielhaft kann hier die Funktionsfähigkeit und Messgenauigkeit von standardisierten Messverfahren bei Geschwindigkeitsmessungen im Bußgeldverfahren genannt werden.

2. Status Quo der forensischen Informatik

Aufgrund der Schnelllebigkeit und stetigen Fortentwicklung kann der jetzige Stand der Forschung über die Methodik und Erfahrungssätze der forensischen Informatik nicht als gesichertes Erfahrungswissen definiert werden[2]. Bezeichnungen wie "zertifizierte und standardisiert anerkannte Software" sind demnach kritisch zu beäugen. Vielmehr sollten zur besseren Nachvollziehbarkeit und Verlässlichkeit bei Beweisfragen, umfangreiche Prüf- und Darstellungsanforderungen bezüglich der Methodik, Erfahrungssätze und der zugrundeliegenden Prämisse, herangezogen werden.

Diese Forderung lässt sich auch aus der Wissenschaft, dem Gesetz (vgl. § 110 StPO), und der aktuellen Rechtsprechung herauslesen, die eine durchschnittliche Sachkunde zur Auswertung von IT-Asservaten nicht als ausreichend erachten. Eine zentrale Ursache dafür ist die meistens bestehende Notwendigkeit einer Interpretation der gespeicherten Daten. Daneben überfordern die schieren Datenmengen Laien. Weiterhin weisen digitale Daten Besonderheiten in ihren Charakteristika auf: Sie sind flüchtig und leicht veränderbar. Um diesen Umständen gerecht zu werden, ist konsequenterweise der IT-Sachverständigenbeweis bei Fragestellungen zur forensischen Informatik das bestmögliche und sachnächste Beweismittel für digitale Spuren. Die Referentin zeigt auf, dass sich eine Pflicht zur Bestellung auch aus §§ 244 II, 261 StPO ableiten lässt.

3. Herausforderungen mit dem IT-Sachverständigen

Bei der Bestellung eines IT-Sachverständigen ergeben sich typischerweise die folgenden Schwierigkeiten: die Auswahl geeigneter Expert:innen, die verständliche Formulierung konkreter Beweisfragen für beide Seiten, die Schaffung einer gemeinsamen Kommunikationsbasis und ein einheitliches Spurenverständnis (Übersetzungsproblematik). Diese Herausforderungen erwachsen unter anderem daraus, dass mehrere Disziplinen die Wurzeln der digitalen Forensik bilden: die Informatik, die Physik und die mathematische Theorie. Bei der Auswahl können sich Schwierigkeiten ergeben, weil sich IT-Sachverständige dadurch auszeichnen, dass sie eine spezifische technologische Sachkunde auf einem konkreten Gebiet der forensischen Informatik vorweisen müssen, um die jeweiligen

[2] Nach Ansicht der Referentin bildet u.a. die Datenträgerforensik hiervon eine Ausnahme.

Beweisfragen beantworten zu können. Zum Beispiel könnte das eine besondere Expertise auf dem Gebiet der Datenträger sein.

4. Beantwortung der Beweisfragen

Die Beantwortung der Beweisfragen erfolgt objektiv seitens des Sachverständigen. Daneben lassen sich seine Antworten in verschiedene Kategorien einordnen.

a) Grenzen der Objektivität

Bei der Beantwortung der Beweisfrage darf sich der IT-Sachverständige nur im Rahmen seines Auftrages bewegen. Die Pflicht zur Objektivität gem. § 79 Abs. 2 StPO ist dem Wesen des Sachverständigenbeweises immanent. Er arbeitet unabhängig und weisungsfrei von den anderen Verfahrensbeteiligten. Ermittelt er über diese Grenzen der Beweisfrage hinaus, so kann unter Umständen der Vorwurf der Befangenheit im Raum stehen.

b) Aussagekategorien der Antworten

Die Beantwortung der Beweisfragen kann man in drei Aussagekategorien unterteilen: Erfahrungssätze, Schlussfolgerungen mithilfe der Sachkunde und Befundtatsachen.

aa) Erfahrungssätze
Die 1. Kategorie umfasst die Mitteilung von Erfahrungssätzen aufgrund besonderer Sachkunde. Dabei handelt es sich um abstrakte Mitteilungen, die noch keinen Bezug zum Sachverhalt aufweisen, wie bspw. Erklärungen von Fachausdrücken oder die Übermittlung von Forschungsergebnissen.

bb) Schlussfolgerungen mithilfe der Sachkunde
In die 2. Kategorie werden Schlussfolgerungen eingeordnet, die aus feststehenden konkreten Tatsachen des Sachverhalts mithilfe der Sachkunde gezogen werden können. Dabei handelt es sich also um eine Art Sachverhaltsbewertung und um die häufigste und wichtigste Kategorie. Darunter zählen zum Beispiel die Mitteilungen, ob eine Bild- oder Textdatei manipuliert wurde.

cc) Befundtatsachen
Die 3. Kategorie zur Beantwortung von Beweisfragen ist umstritten und schwierig zu bewerten. Darunter fallen Befundtatsachen, die vom IT-Sachverständigen festgestellt werden, wenn dafür besondere Sachkunde erforderlich ist. In dieser Beweiskategorie hilft der Sachverständige bei der Generierung des Beweisstoffes, zum Beispiel durch das Auffinden von unüblichem Datenmaterial in nicht unerheblicher Menge auf einem Datenträger. Dabei ist höchst strittig, wann besondere Sachkunde bei der Sicherung und Auswertung der Datenträger erforderlich ist und wann es sich lediglich um ein illegales Outsourcing von Ermittlungstätigkeiten handelt. Weitere Probleme dieser Kategorie ergeben sich dadurch, dass die Wahrnehmungen des Forensikers in dieser Kategorie einen gewissen Grad an Schlussfolgerungen enthalten und dadurch eine strikte Grenzziehung zur 2. Kategorie schwierig ist. Darüber hinaus ist auch die Abgrenzung zwischen Sachverständigen und sachverständigen Zeugen nicht trivial.

dd) Anregungen der Referentin
Nach der Erläuterung dieser drei Kategorien, regt die Referentin an, eine weitere Kategorie zu etablieren. Unter diese vierte Kategorie soll die Vornahme bloßer Verrichtungen zur Tätigkeit des Sachverständigen, z.B. die Sicherung und Entschlüsselung von Datenmaterial, fallen.

5. Würdigung der Zuverlässigkeit der Ergebnisse

Im weiteren Verlauf ihres Vortrages präsentiert *Frau Dr. Scheler* ein eigens entwickeltes Prüfungsschema, welches das Spannungsfeld zwischen freier Beweiswürdigung gem. § 261 StPO und den Grundsatz der Nachvollziehbarkeit und Transparenz bei der Beweiswürdigung in Einklang bringt. Im ersten Schritt wird die Beweisfrage analysiert und in einem zweiten Schritt die Antworten des Sachverständigen bewertet. Diese Bewertung der Sachverständigen-Ergebnisse setzt sich aus einer Nachvollziehbarkeitsprüfung und einer Transparenzkontrolle, sowie der Kategorisierung der angewandten Methoden nach deterministisch, statistisch und selbstlernend zusammen.

a) Kategorisierung der Methoden

Eine Datenverarbeitung, die auf deterministischen Methoden beruht, generiert nur solche Informationen aus den Daten, die in diesen Datensätzen unzweifelhaft vorhanden sind. Dabei handelt es sich um Programme, die digitale Daten in eine menschenlesbare Form übersetzen, wie die Anzeige von Bildern.

Statistische Methoden hingegen sind komplexer und errechnen Informationen aus Datensätzen. Diese Informationen lassen sich nicht ohne weiteres aus diesen Daten entnehmen und sind nur mit einem gewissen Grad an Wahrscheinlichkeit zutreffend. Die Richtigkeitswahrscheinlichkeit der Ergebnisse hängt dann von der zugrundliegenden Heuristik und Annahme ab. Unter solche Methoden fallen u.a. Ähnlichkeitsanalysen beim Data Mining.

Noch komplexer sind dann selbstlernende Methoden. Diese Methoden entwickeln Annahmen und Heuristiken aufgrund der ihnen zugrundeliegenden Trainingsdaten. Häufiger Kritikpunkt dieser Methoden ist der Mangel an Nachvollziehbarkeit, aufgrund der selbstentwickelten Heuristiken und Annahmen.

Um die Methoden in eine Richtigkeits- und Zuverlässigkeitsskala einordnen zu können, muss man sich mit der genauen Arbeitsweise des Sachverständigen auseinandersetzen. Nur durch diesen nächsten Schritt können die weiteren Prüfungs- und Darstellungsanforderungen im Urteil ermittelt werden.

Neben der Würdigung und Bewertung der angewendeten Methoden, sollte auch die Person des Sachverständigen beurteilt werden, um einen möglichen Bias ausschließen zu können. Ein solcher ist anzunehmen, wenn der Sach-

verständige in seiner Interpretation und Analyse naheliegende Alternativhypothesen außer Acht lässt.

b) Einordnung der Methoden und Erfahrungssätze in eine Zuverlässigkeitsskala

Durch die Entwicklung einer Zuverlässigkeitsskala könnte man eine potenzielle Bindungswirkung an die Ergebnisse ableiten. Die Referentin definiert hierfür vier Abstufungen: (1) gesicherte, wissenschaftliche Erkenntnisse, (2) wissenschaftliche Erkenntnisse mit Richtigkeitswahrscheinlichkeit, (3) einfache Erfahrungssätze und (4) ungeeignete Methoden.

(1) Gesicherte, wissenschaftliche Erkenntnisse liegen immer dann vor, wenn die Erkenntnisse nach dem aktuellen Stand der Wissenschaft unangefochten sind. Es handelt sich dabei um Erkenntnisse, die auf deterministischen Methoden beruhen.

Der zweiten Stufe werden (2) wissenschaftliche Erkenntnisse mit wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit zugeordnet. Diese basieren in der Regel auf statistischen Methoden und es liegt keine Bindung der Ergebnisse für das Gericht vor. Dieses muss jedoch die gewonnenen Erkenntnisse einbeziehen und zusätzlich die Richtigkeit der Aussage im jeweiligen Einzelfall anhand weiterer Indizien bestätigen und widerlegen.

Ergebnissen, die sich aufgrund (3) einfacher Erfahrungssätze ergeben, kann nur eine Indizwirkung zugesprochen werden.

Schließlich und zuletzt existieren (4) Methoden, die zu völlig ungeeigneten Ergebnissen führen. Zwar gilt im Grundsatz die freie Beweiswürdigung, jedoch regelt § 244 Abs. 3 S. 3 Nr. 4 StPO eine Ausnahme davon. Demnach sind Beweismittel wertlos, wenn feststeht, dass jede Möglichkeit ausgeschlossen ist, dass das Beweismittel Sachdienliches ergeben kann. Beispielsweise wären Blackbox-Tools unter diese vierte Stufe zu subsumieren, denn diese sind nicht nachvollziehbar und intransparent.

6. Endgültige Einordnung und Endergebnis

Die meisten Methoden der forensischen Informatik sind nicht standardisiert und Erfahrungssätze nicht wissenschaftlich gesichert. Dementsprechend muss das Gericht bei der Würdigung solcher Beweise umfangreichen Prüfungs- und Darstellungsanforderungen gerecht werden und Erfahrungssätze, Methodiken und zugrundeliegende Prämissen zum Tatsachenstoff machen, was wiederum Auswirkungen auf das Recht auf Akteneinsicht gem. § 147 StPO, das Recht auf ein faires Verfahren, das Fragerecht der Beteiligten und das prozessuale Gleichgewicht hat. Zudem ermöglicht dies den Weg zu den Rechtsmittelverfahren und dadurch auch die mögliche Entwicklung von antizipierten Sachverständigengutachten, die dann letztlich eine Beweiswürdigung abkürzen und vereinfachen.

Grundsätzlich ist und soll der Sachverständige weisungsfrei arbeiten. Eine Prämisse könnte dahingehend formuliert werden, dass die zuverlässigste Methode angewendet werden muss.

Als abschließendes Resümee hält *Frau Dr. Scheler* fest, dass die Hürden, die sie im Rahmen ihres Vortrags aufgezeigt hat, sehr gut mit unserer Strafprozessordnung lösbar sind.

7. Q&A-Session

Abschließend bot der erste Vortrag Raum für Fragen der Teilnehmenden, die zu einer zusätzlichen Vertiefung des Themas beitrugen. Und so wurde darüber diskutiert, wo konkret die Grenze von Allgemeinwissen und Fachwissen gezogen werden kann. Als Faustformel lässt sich festhalten, soweit Richter:innen das Wissen gut und nachvollziehbar eigenständig erklären können, bewegen sie sich im Rahmen des Allgemeinwissens. Ist diesen eine eigenständige Erklärung nicht möglich, spricht dies für eine begrenzte Sachkunde, sodass die Einschaltung von Expert:innen erforderlich wäre. Weiterhin wurde die Frage nach der Abgrenzung zwischen Sachverständigen und sachverständigen Zeugen vertieft. Als erstes sollte auf den Zweck der Befragung abgestellt werden. Lässt sich daraus keine Abgrenzung ziehen, stellt man auf das Vorliegen eines Auftrags ab. Im Austausch über die Entwicklung möglicher Tools und Fragen der Beweiswürdigung zeigte sich, dass der Einfluss der KI-Verordnung und etwaige Zertifizierungen, sowie deren Bewertung einen Diskussionspunkt darstellen kann.

III. Herausforderungen bei der Präsentation von digitalen Beweismitteln, Marion Liegl (Friedrich-Alexander-Universität Erlangen-Nürnberg)

Als nächstes bot die IT-Forensikerin *Marion Liegl* einen humorvollen und aufschlussreichen Einblick in ihre praktischen Erfahrungen als freiberufliche IT-Sachverständige für Strafverfolgungsbehörden. Ihren Vortrag strukturierte sie anhand von drei Fällen aus Ihrer Praxiserfahrung, die die Herausforderungen bei der Präsentation digitaler Beweismittel im gerichtlichen Alltag anschaulich untermalten. Dabei befasste sich jeder Fall mit einem eigenen großen Problempunkt: (1) Auswertung und gerichtsverwertbare Aufbereitung von Big Data, (2) Die Bedeutung des Sachverstandes des IT-Sachverständigen und der Mangel an Zertifizierungsregelungen, (3) Der Umgang mit Eingriffen in den höchstpersönlichen Lebensbereich bei der Präsentation digitaler Beweismittel. Die Referentin hat neben einem Master für Digitale Forensik und elfjähriger Berufserfahrung auch Rechtswissenschaft im Nebenfach studiert, sodass sie besonders geeignet ist, die Probleme mit einer interdisziplinären Perspektive zu beleuchten.

1. Auswertung von Big Data

In der Präsentation des ersten Falles befasste sich die Referentin mit den Problemen, die Big Data aufwerfen. Massendaten die ausgewertet, extrahiert und analysiert werden müssen, obwohl die geeigneten Ressourcen bei den Strafverfolgungsbehörden derzeit noch fehlen.

a) Massendaten

Die erste Herausforderung verdeutlichte *Frau Liegl* im Kontext der Auswertung eines Mobiltelefons, die es der Staatsanwaltschaft ermöglichen sollte, eine relevante Verbindung zwischen Täter und Opfer zu ermitteln. Hierbei bestand die Aufgabe der Sachverständigen zunächst darin, Daten zu extrahieren, zu filtern, nach vorgegebenen Suchmerkmalen entsprechend zu durchsuchen und Fragen der Ermittler zu beantworten. Die Herausforderung im konkreten Fall: Als relevant stellte sich ein über mehrere Monate andauernder und im Schnitt 250 Nachrichten pro Tag umfassender Chatverlauf heraus. So war zwar schnell klar, dass sich Täter und Opfer kannten, jedoch galt es in einem nächsten Schritt, die Frage zu klären, in welchem konkreten Verhältnis die beiden zueinanderstanden. Dabei lässt sich von einer großen Masse an Daten nicht per se ein enges Verhältnis ableiten. Vielmehr muss der Inhalt der Chatnachrichten analysiert werden.

b) Grenzen analoger Präsentation digitaler Beweismittel

Diesen langen Chatverlauf galt es für die Beweiswürdigung „gerichtsverwertbar" zu präsentieren. Dabei entsprach es nach den Erfahrungen der Referentin gerichtlicher Praxis, die extrahierten Daten in analoger Form, das heißt ausgedruckt, bereitzustellen. Dass diese Vorgehensweise angesichts des erheblichen Datenumfangs an ihre Grenzen stößt, führte *Frau Liegl* den Zuhörern anhand einer Berechnung plastisch vor Augen. Rechnet man mit 250 Chatnachrichten pro Tag in einem relevanten Zeitraum von ca. neun Monaten, so kommt man ungefähr auf 67.000 Nachrichten. Möchte man diese gerichtsverwertbar, d.h. auch in lesbarer Schriftgröße auf Papier drucken, ergibt das ca. 1.688 Seiten. Für die Präsentation des Chatverlaufs ergab sich somit eine erforderliche Menge von 4,2 Kilogramm Papier, soweit man doppelseitig drucken würde. Demgegenüber ist die Stelle im eigentlichen Gutachten des Sachverständigen kurz. Man findet lediglich Sätze wie "Das Telefon wurde ausgewertet und es wurde ein mutmaßlich fallrelevanter WhatsApp-Chat gefunden. Siehe Anlagen."

c) Grenzen des Aufgabenbereichs eines IT-Sachverständigen

Die daraufhin erfolgte Anfrage der Ermittler, ob eine Kürzung der Daten möglich sei, bildete einen Anknüpfungspunkt der nächsten Schwierigkeit und einer aktuell viel diskutierten Problematik. Es stellt sich die Frage, wo die Arbeit des Sachverständigen aufhört, und die originären Aufgaben der Strafverfolgungsbehörden anfangen. Das Herausfiltern des für die Beweiswürdigung relevanten Inhalts aus der Masse an Daten stellt dabei eine diffizile Aufgabe dar.

„Kann und darf der Sachverständige, der IT-Sachverständige entscheiden, was relevant ist und was nicht?"

Die Antwort auf die aufgeworfene Frage der Referentin brachte zugleich ihr Unwohlsein bezüglich der Aufgabe zum Ausdruck und machte deutlich, dass die Grenzen der Aufgabenbereiche nicht verschwimmen sollten.

„Ich kann mir nicht anmaßen, als IT-Sachverständige dem Gericht hier in irgendeiner Form was vorwegzunehmen."

Denn das Gericht muss neben der Feststellung der Tatumstände in der Lage sein, alle relevanten be- und entlastenden Begleitumstände zu würdigen. Das können neben offensichtlichen Tatsachen auch solche sein, die mittelbar Relevanz haben. Dabei stellt die Einordnung als relevante Tatsache bereits eine rechtliche Bewertung dar und entzieht sich daher einer vorbereitenden Selektion durch den IT-Sachverständigen. Diesem obliegt es, die digitalen Inhalte zugänglich zu machen, ohne den Beweiswert zu verändern. Das Sachverständigengutachten umfasst die Bestätigung der Auswertung, die Beschreibung der technischen Vorgehensweise und Bedingungen, sowie den Hinweis bezüglich des Funds eines mutmaßlich fallrelevanten Chats.

d) Die notwendige Fortentwicklung des Strafverfahrens

Im Ergebnis lag die pragmatische Lösung in der Aushändigung eines USB-Sticks mit den Chatinhalten, dessen Verteilung durch das Gericht angeordnet wurde. Der mobile Datenträger ermöglichte einen vollständigen und praktikablen Zugang zu den Daten. Der USB-Stick wurde an das Gericht, die Verteidigung und Staatsanwaltschaft verteilt, damit diese die Chatinhalte im Selbstleseverfahren betrachten konnten. Letztlich spiegeln sich hier weitere Herausforderungen, die mit Massendaten hervorgehen und mit denen derzeit an Gerichten gekämpft wird, wider. Daten sollen gestrafft und übersichtlich, trotzdem vollumfänglich, und gerichtsverwertbar als Beweismittel in der Hauptverhandlung präsentiert werden. Die Referentin zeigt anhand Ihres Falles, dass die Lösung des Konflikts mit Mitteln der Strafprozessordnung und einer Offenheit gegenüber bis dato auch unkonventionelle Methoden gelöst werden kann.

2. Anforderungen an den IT-Sachverständigen

In ihrem zweiten Beispielfall befasste sich *Frau Liegl* mit der erforderlichen Expertise des Sachverständigen und dessen Bedeutung für das Strafverfahren. Dabei spricht auch sie die Notwendigkeit einer Qualitätssicherung der Arbeit der IT-Forensiker durch Regulierungen und Standards an.

a) Bedeutung und Aussagekraft von digitalen Beweismitteln

In diesem Fall waren die einzigen Beweismittel die Hauptbelastungszeugin, die auch gleichzeitig das Opfer war und die Referentin in ihrer Rolle als Sachverständige zur Interpretation eines digitalen Beweismittels. Die Verteidigungsstrategie des Angeklagten zielte darauf ab, die Glaubwürdigkeit der Beweismittel in Frage zu stellen. Er versuchte dies insbesondere dadurch zu erreichen, dass er sowohl der Belastungszeugin als auch der Referentin die Intention zuschreiben wollte, dass ihm beide die Tat fälschlicherweise anlasten wollten. Dem Angeklagten gelang es zumindest kurzzeitig, Zweifel bei den Beteiligten hervorzurufen, als er in der Hauptverhandlung Dateninkonsistenzen in den Zeitstempeln des digitalen Beweismittels nachweisen konnte. Diese waren zuvor nicht aufgefallen, da auch dieses Beweismittel aus Massen von Daten und Datensätzen bestand und im Rahmen der Hauptverhandlung mehrbändig ausgedruckt wurde.

b) Spontaner Einsatz der Expertise von Sachverständigen

An dieser Stelle kam es daher für die Sachverständige darauf an, die Unstimmigkeiten aus dem Stehgreif technisch richtig und nachvollziehbar einordnen zu können. Aufgrund der Flüchtigkeit von Daten können Inkonsistenzen schnell gewollt, aber auch ungewollt entstehen. Die Aussagekraft des digitalen Beweismittels spielte eine tragende Rolle, da dieses die Aussagen der Hauptbelastungszeugin bestätigen oder dementieren sollte. *Frau Liegl* bestätigte, dass die Daten tatsächlich Inkonsistenzen aufwiesen. Anhand anderer digitaler Spuren ließ sich jedoch technisch sauber eingeordnet und plausibel erklären, dass es sich dabei nicht um eine gewollte Manipulation der Daten handelte.

Gerade die spontane Interpretation von digitalen Daten und Spuren erfordert umfänglichen technischen Sachverstand, den *Frau Liegl* im konkreten Fall einbringen und dadurch den vollen Beweiswert zur Geltung bringen konnte. Die Herausforderung besteht darin, dass ohne Kenntnis der relevanten Begleitumstände des Verfahrens und insbesondere auch vor dem Hintergrund des jeweiligen Datenmaterials, eine Vorbereitung auf die jeweilige Beweismittelpräsentation vor Gericht schwer möglich ist.

c) Regelungslücke trotz großer Bedeutung

Der Expertise von Sachverständigen kommt im Strafverfahren eine hohe Bedeutung zu.

„Wenn ich was gesagt habe, das hat man nicht hinterfragt. Das wurde einfach hingenommen“

– so beschreibt die Rednerin ihre tragende Rolle und kritisiert vor diesem Hintergrund die derzeit nicht bestehenden Anforderungen an die Qualifikation der IT-Sachverständigen. Zwar soll § 73 Abs. 2 StPO bestimmen, dass öffentlich bestellte und vereidigte Sachverständige bevorzugt ausgewählt werden sollen, jedoch ist dies in der Praxis nicht immer gegeben. Eine bestimmte Ausbildung ist für IT-Sachverständige nicht notwendigerweise vorgesehen. Zwar stehen den IT-Sachverständigen zertifizierte Tools zur Verfügung, allerdings geht die Arbeit über die bloße Tool-Anwendung hinaus. Es kommt auf das Verständnis und Hinterfragen der Tools und den daraus resultierenden Ergebnissen an, um sich über die Anwenderebene hinausheben zu können. *„Dafür ist eine gute Ausbildung erforderlich“*, die nach eigener akademischer Erfahrung der Rednerin auch von der Zusammenarbeit mit Juristen und interdisziplinärer Arbeit sowie Sichtweise profitiert.

Die aktuellen Umstände bezeichnet sie als Regelungslücke, die es gerade zur Gewährleistung eines fairen Verfahrens und der Wahrung der Menschenrechte, insbesondere auch im Interesse des Angeklagten, dringend zu hinterfragen gelte.

3. Eingriffe in den höchstpersönlichen Lebensbereich durch die Präsentation (digitaler) Beweismittel

Im letzten Fall, der von der Referentin vorgetragen wurde, wurde sich mit der möglichen Verletzung höherrangiger Rechtsgüter auseinandergesetzt.

a) Schutz des Persönlichkeitsrechts in Großverfahren

Hierbei schildert die Referentin eine Situation, durch welche der höchstpersönliche Lebensbereich einiger Beteiligten des Strafprozesses durch die Präsentation (digitaler) Beweismittel berührt wurde. Konkret ging es um die Einführung von Videomaterial in einer Gerichtsverhandlung, welches aufgrund des hohen Interesses der Öffentlichkeit, einer großen Masse an Menschen zugänglich gemacht wurde. Das Abspielen der Videobeweismittel diente dem Zweck, den Angeklagten hierdurch zu identifizieren. Im Hintergrund dieses Videomaterials waren aber auch unbeteiligte Personen in den Aufnahmen zu sehen. Es wurden Szenen aufgezeichnet, die teilweise den Kernbereich privater Lebensführung berührten. Diese sowieso schon heikle Situation wurde durch das erhöhte Öffentlichkeitsinteresse verschärft. Denn das Gerichtsverfahren fand nicht in einem üblichen Gerichtssaal statt, sondern wurde in einen größeren Raum verlagert, um den Andrang der Öffentlichkeit, Presse, aber auch vermehrten Nebenanklagenden, Strafverteidigern usw. gerecht zu werden. Dies führte auch dazu, dass das Videomaterial, um es für alle Beteiligten sichtbar zu machen, auf einer großen Leinwand abgespielt wurde.

b) Beweispräsentation vs. Persönlichkeitsrechte

Dies rief nicht nur bei der Referentin ein besonderes Unwohlsein und Unverständnis hervor. Der unangemessene Umgang dieser sensiblen Inhalte wurde auch von einem Beteiligten gerügt und der weiteren Beweisaufnahme wi-

dersprochen, sodass die Inaugenscheinnahme mittels eines kleineren Monitors fortgeführt wurde. Die Rednerin weist an dieser Stelle auf ein Spannungsfeld zwischen vollumfänglicher Beweispräsentation und dem Schutz der Persönlichkeitsrechte hin, welches durch digitale Beweismittel, insbesondere bildliche Aufnahmen, intensiviert wird. *Frau Liegl* fordert einen sensibleren Umgang und hofft, dass dieser Fall auch die Interessierten im Publikum, ob vor Ort oder vor den Monitoren, zum Nachdenken anregt.

4. Q&A-Session

In der abrundenden Q&A-Session wurde die Frage nach der Verwendung von KI für die Kürzung von Daten aufgeworfen. Doch auch der Einsatz von KI knüpft an die Problematik der Möglichkeit einer vorweggenommenen Selektion des für die Beweiserhebung Relevanten an. Zudem spielen datenschutzrechtliche Fragen eine Rolle. Daraufhin folgte eine spannende Frage zur Vorgehensweise bei der Auswertung und Sicherung des Mobiltelefonasservats. Ob ein komplettes Image des Handys vorgenommen wird, ist abhängig vom konkreten Fall und Ermittlungsauftrag. Je enger die Ermittlungsfrage gestellt wird, desto selektiver kann gesichert und ausgewertet werden.

IV. Using digital evidence to prove international crimes: a view from international courts (englischer Vortrag ins Deutsche übersetzt) von Matthew Cross (Internationaler Strafgerichtshof in Den Haag)

Nach der Mittagspause durften die Teilnehmenden und alle Interessierten über den Tellerrand blicken und *Matthew Cross*, Appeals Counsel der Anklagebehörde am *Internationalen Strafgerichtshof*, auf der Bühne begrüßen. In seinem Vortrag gewährte er dem Publikum einen Einblick in den Umgang mit digitalen Beweismitteln vor den internationalen Strafgerichtshöfen und die damit verbundenen Herausforderungen. Der Vergleich zu nationalen Problemen und Hindernissen, sowie die Erfahrungen auf internationaler Ebene stellen einen lehrreichen Austausch und eine Inspiration dar.

1. Wesentliche Merkmale internationaler Strafgerichte

Zum Einstieg erläutert der Referent die Grundzüge der internationalen Strafgerichtsbarkeit. Auf transnationaler Ebene existiert keine einheitliche Institution. Vielmehr setzt sich die internationale Strafgerichtsbarkeit aus einer Reihe von verschiedenen Gerichten und ad-hoc Tribunalen zusammen, welche jeweils ihren eigenen Verfahrens- und Beweisregeln unterliegen. Dabei nimmt der *Internationale Strafgerichtshof* in Den Haag (*IStGH*) eine zentrale Rolle ein, da er ein permanenter Spruchkörper ist. Es liegt jedoch keine Bindung der verschiedenen Gerichte und Spruchkörper untereinander vor. Diese sind unabhängig voneinander.

a) Zuständigkeiten

Internationale Strafgerichtshöfe sind auf die Ahndung schwerster internationaler Verbrechen ausgerichtet. Dazu gehören Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen und das Verbrechen der Aggression sowie weitere Handlungen, die die Rechtspflege beeinträchtigen können. Unter dem letzten Punkt versteht man Straftaten wie Zeugenbeeinflussung oder Vergeltungsmaßnahmen gegen Mitarbeiter des Gerichts.

b) Besonderheiten der Verfahren

Aufgrund der starken Begrenzung der Zuständigkeiten und limitierten Ressourcen der Ermittlungsbehörden wird nur eine geringe Zahl von Fällen verfolgt und zur Anklage gebracht. Hinzu kommt, dass es sich um besonders komplexe und umfangreiche Sachverhalte handelt, was dazu führt, dass sich die Verfahren über Jahre hinziehen und hunderte Zeugen und zahlreiche Anklagepunkte umfassen. Zudem sind die Ermittlungen mit erheblichen praktischen Schwierigkeiten verbunden. So beginnen die Verfahren meist mehrere Jahre nach den strafrechtlichen Ereignissen.

c) Mangelnder Zugang zum Tatort

Eine bedeutende Schwierigkeit, die auch die hohe Relevanz der digitalen Beweismittel in diesen Strafverfahren beeinflusst, ist, dass den Ermittlern oft der Zugang zum Tatort oder der Zugang zum entsprechenden Staat verwehrt wird. Die Ermittler können sich kein Bild vor Ort von der Situation machen. Auch die Akquirierung von Zeugen und persönliche Gespräche werden dadurch erschwert. Aufgrund der zeitlichen Dauer, bis die Ermittlungen beginnen, sind Zeugen aufgrund des Alters, Krankheiten, oder Todesfällen meist schwer oder gar nicht mehr erreichbar.

Der Referent weist darauf hin, dass die geschilderten Herausforderungen internationale Gerichte dazu veranlassen, innovative und kreative Ansätze zur Untersuchung von Verbrechen zu entwickeln. Dadurch gewinnen digitale Ermittlungsmaßnahmen und die Nutzung bereits verfügbarer digitaler Daten neben den traditionellen Beweismitteln zunehmend an Bedeutung.

2. Allgemeine Beweisregeln

Die Beweisregeln vor internationalen Strafgerichtshöfen orientieren sich in ihren Grundzügen an Prinzipien, die aus dem nationalen Recht bekannt sind. Diese Grundgedanken entwickeln die internationalen Gerichte dann fort und verknüpfen diese mit sog. „hybriden" Ansätzen. Eine derartige Kombination spiegelt zum einen die bewährte Praxis der internationalen Gemeinschaft wider, während zum anderen der Umstand berücksichtigt wird, dass internationale Strafverfahren besondere Herausforderungen mit sich bringen.

Wie auch vor den nationalen Gerichten müssen Beweismittel vor dem *IStGH* relevant, beweiskräftig und nicht unangemessen vorurteilsbehaftet sein. Im Unterschied zu traditionellen *common-law*-Verfahren verschiebt sich die Praxis vor dem *IStGH* jedoch zunehmend dahin, Fragen

der Beweiszulässigkeit erst am Ende des Prozesses zu klären. Dies erlaubt es den Richtern, den Beweiswert im Kontext des gesamten Beweismaterials zu bestimmen. Vor allem mit Blick auf die Praxis stellt dies eine verfahrensökonomische Entwicklung dar, weil dadurch der Umgang mit umfangreichen Beweismitteln erleichtert wird.

Zuletzt hebt der Referent hervor, dass vor dem *IStGH* grundsätzlich alle Beweisarten zugelassen sind und kein Verbot der Aussagen von Hörensagen besteht. Trotz der Vielfalt an Möglichkeiten sind Zeugenaussagen auch weiterhin das bevorzugte Beweismittel. Im Zuge des Fortschritts muss sich jedoch mit der Frage auseinandergesetzt werden, ob die zwingende Erforderlichkeit von Zeugenaussagen besteht und falls dies bejaht wird, in welchem Umfang sie heranzuziehen sind. Es ist zu hinterfragen, ob Zeugenaussagen der alleinige "Goldstandard" sind, oder auch andere Beweismittel einen Sachverhalt belastbar und substantiiert darstellen können.

3. Steigende Relevanz digitaler Beweismittel

Der Begriff der digitalen Beweise umfasst ein breites Spektrum an elektronischen Daten. Diese reichen von audiovisuellen Materialien in Form von Videos, Fotos und Tonaufnahmen über Satelliten- und Luftbilder bis hin zu Kommunikations- und Gerätedaten aus Mobiltelefonen oder Computern.

a) Chancen und Vorteile digitaler Beweismittel

Zur Veranschaulichung geht *Cross* beispielhaft auf zwei Verfahren ein, bei welchen vor allem Social Media Beiträge eine bedeutende Rolle spielten.

Der erste Fall ist das MH17 Verfahren aus den Niederlanden.[3] Durch die Beweiserhebung öffentlich verfügbarer Fotos und Social-Media-Beiträge gelang es den Ermittlern anhand einer Zusammenstellung des Beweismaterials eine Zeitachse der Geschehensabläufe zu rekonstruieren, um so die Nachverfolgung der Ereignisse zu ermöglichen. Im Fall des Haftbefehls gegen *Al-Werfalli*[4] stützten sich die Ermittlungen maßgeblich auf Fotos und Videos, die angeblich vom Verdächtigen selbst oder in seinem Auftrag erstellt und auf verschiedenen Social-Media-Plattformen geteilt wurden. Durch diese digitalen Beweismittel war der Fall relativ eindeutig und dadurch gut nachvollziehbar. Als diskutabel erwies sich insbesondere, ob eine Anklage im Wesentlichen auf öffentlich zugänglichen digitalen Daten aus Sozialen Netzwerken beruhen kann. Da der Beschuldigte mittlerweile verstorben ist, wird offenbleiben, ob diese Beweisergebnisse ausreichend waren, um das Strafverfahren weiterzuführen.

b) Risiken und Nachteile von digitalen Beweismitteln

Gleichzeitig weist der Referent auf die neuen Herausforderungen hin, die sich aus der zunehmenden Nutzung digitaler Beweismittel ergeben. Insbesondere sinkt mit der Entwicklung Künstlicher Intelligenz das Vertrauen in die Authentizität und Manipulationssicherheit solcher Beweismittel. Es liegt ein fortwährendes „Katz-und-Maus-Spiel“ zwischen Fälschungstechniken durch Kriminelle und den Methoden der Echtheitsprüfung durch die Gerichte vor. Hier kommen dann IT-Sachverständige ins Spiel, die die Ermittlungen und Beweisanalyse unterstützen.

4. Anwendung digitaler Beweismittel

In der Theorie, so *Cross*, bieten internationale Gerichte grundsätzlich geeignete Rahmenbedingungen, um den Umgang mit digitalen Beweismitteln zu erproben. Sie sind mit professionellen Richtern besetzt, verfügen über stabile Ressourcen und bearbeiten fast ausschließlich komplizierte sowie langwierige Verfahren.

a) Digitale Beweismittel: Eine Beweisform im Frühstadium?

Bislang gab es jedoch noch kein Verfahren vor dem *IStGH*, welches digitale Beweismittel hauptsächlich problematisierte. Dies ist vor allem der Tatsache geschuldet, dass viele der aktuellen Verfahren Ereignisse vor 2014 betreffen. Sie stammen also aus einer Zeit, in der die Digitalisierung noch nicht den Umfang erreicht hatte, den wir heute beobachten können.

Daneben führen Digitale Beweismittel nicht immer, wie oft angenommen, zu simpleren, effizienteren oder schnelleren Verfahren. Zur Veranschaulichung verweist der Referent auf das *Ayyash*-Verfahren[5] vor dem Special Tribunal for Lebanon. Dieses Verfahren stützte sich zwar hauptsächlich auf Mobilfunkdaten, dennoch wies das Urteil am Ende 2.227 Seiten, fast 300 Zeugen, zahlreiche Experten und mehrere tausend Beweisstücke auf. Dieses Beispiel verdeutlicht auch, dass der Umgang mit neuen Beweismitteln naturgemäß besonders aufwendig ist. Mit zunehmender Erfahrung dürfte sich jedoch eine effizientere und routiniertere Anwendung durch die Gerichte entwickeln.

b) Guidelines und Dokumente, insbesondere die Leiden Guidelines

Angesichts einer bislang fehlenden umfangreichen internationalen Rechtsprechung verweist der Referent zur Orientierung bei der Verwendung digitaler Beweise vor Ge-

[3] vgl. Tagesschau, Prozess um MH17-Abschuss, 17.11.2022, https://bit.ly/4tcnlzw.

[4] The Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli, ICC-01/11-01/17.

[5] The Prosecutor v. Salim Jamil Ayyash, Hassan Habib Merhi, Hussein Hassan Oneissi, Assad Hassan Sabra, STL-11-01/T/TC.

richt auf zwei Projekte hin, die von internationalen Expert:innen entwickelt wurden. Dabei handelt es sich zum einen um das *Berkeley Protocol on Digital Open Source Investigations*[6], welches sich mit Ermittlungstechniken befasst und sich dabei insbesondere auf die Möglichkeit von OSINT-Beweisen konzentriert. Daneben können die *Leiden Guidelines*[7] als Ergänzung dieses Dokuments angesehen werden. Letzteres beschäftigt sich im Gegensatz zum *Berkeley Protokoll* weniger mit den Ermittlungen, sondern setzt seinen Fokus auf den bislang bestehenden Umgang, um daraus Erkenntnisse abzuleiten.

Nach *Cross* lassen sich aus den *Leiden Guidelines* diese sechs Kernprinzipien entnehmen:

aa) Einreichung des gesamten Beweismittels
Beweismittel sollen möglichst in ihrer Gesamtheit und nicht nur teil- oder auszugsweise verwendet werden. Nur so kann sichergestellt werden, dass der Kontext des Beweises richtig verstanden wird. Will man beispielsweise einen Videoclip in seiner Gesamtheit verstehen, sollte man sich auch den Ausschnitt davor und danach anschauen. Bei besonders umfangreichen digitalen Beweisen, beispielsweise bei einem WhatsApp-Chat mit mehreren tausenden Einträgen, kann dies auch eine Herausforderung darstellen.

bb) Einwilligung
Will das Gericht Bildmaterial, auf welchem eine Person zu erkennen ist, verwenden, so ist, sofern möglich, die Einwilligung der abgebildeten Person einzuholen. Damit soll garantiert werden, dass sich keiner als Subjekt eines internationalen Verfahrens wiederfindet, ohne davon in Kenntnis gesetzt worden zu sein. Dies gilt insbesondere dann, wenn es sich um sensibles Bildmaterial, wie die Darstellungen von geschlechtsspezifischer Gewalt, handelt. Damit sind weitere Schwierigkeiten verknüpft. Der Vorteil öffentlich zugänglicher Daten und Informationen für Ermittler ist, dass diese schnell und einfach auffindbar sind. Diese unkomplizierte Beweiserhebung geht verloren, wenn man in einem zweiten Schritt die Identitäten von Personen feststellen muss. Zum anderen möchte man sensibles Bildmaterial nur einem kleinen Kreis zugänglich machen. Bei der Identifizierung von Personen stehen Ermittler jedoch vor dem Dilemma, dass Material unter Umständen auch Dritten zugänglich gemacht und vorgelegt werden muss.

cc) Authentifizierung
Im Rahmen der Authentifizierung digitaler Beweismittel wird betont, dass es sich dabei um ein immer relevanteres und zunehmend komplexes Themengebiet handelt. Einzelne digitale Beweismittel können als sich „selbstauthentifizierende Beweismittel" bewertet werden, sofern keine augenscheinlichen Bedenken hinsichtlich einer Manipulation (z.B. in Form von Deepfakes) bestehen. Sie bestätigen ihre Authentizität selbst, so beispielsweise Bilddateien, die alle zugehörigen Metadaten enthalten und mit Zeitstempeln versehen sind. Um die Echtheit eines Beweismittels zu bestimmen, wird es immer öfter erforderlich, zusätzliches Beweismaterial heranzuziehen, wie den Sachverständigenbeweises. Daneben können auch Zeugen, die in dem Beweismaterial zu sehen sind, im Rahmen ihrer Aussage die Echtheit des Beweismittels bestätigen.

dd) Kontext der Beweiserhebung
Der Kontext und die Umstände der Beweiserhebung spielen eine wichtige Rolle, auch im Rahmen der Überprüfung der Authentizität. Dies gilt insbesondere bei Abhörmaßnahmen oder in Situationen, in denen das Gericht Bedenken hinsichtlich der Rechtmäßigkeit der Erhebungsmaßnahme oder der Originalität des Beweismaterials haben könnte. Dann muss, wie im *Ayyash*-Fall, nachvollziehbar dargelegt werden wie das Beweismaterial erhoben wurde. Hierzu können sowohl Sachverständige als auch Zeugen angehört werden.

ee) Interpretation und Expertise
Soweit dem Referenten bekannt ist, existiert zur Frage, wann Richter selbst genügend Sachverstand besitzen, um digitale Beweise zu interpretieren, keine internationale Rechtsprechung. Nichtsdestotrotz ist diese Fragestellung indirekt in Verfahren aufgetaucht. Meist in Fällen, wo das Alter von Kindern untersucht werden musste bzw. festgestellt werden musste, ob diese jünger als 15 Jahre sind. Daran knüpft auch die nächste und letzte Kernaussage der *Leiden Guidelines* an.

ff) Schlussfolgerungen
Es ist grundsätzlich für Richter:innen möglich, aus digitalen Beweismitteln Schlussfolgerungen zu ziehen, jedoch nur insofern das Material eine „eindeutige Feststellung" erlaubt. Diese Formulierung ist unbestimmt und schwammig, wobei die Anforderungen für eine entsprechende Feststellung besonders hoch sind, so dass diese in der Praxis zusätzlich mit weiteren Beweisen und Indizien untermauert werden sollten.

5. Fazit

Insgesamt zeigt sich, dass der Einsatz digitaler Beweismittel im internationalen Strafrecht weiterhin mit zahlreichen offenen Fragen verbunden ist, da sich bislang in keinem Fall vor dem *IStGH* zentral mit der Problematik auseinandergesetzt werden musste. Dabei stellt *Cross* die Vermutung auf, dass nationale Gerichte voraussichtlich früher Antworten auf diese offenen Fragen herausarbeiten werden, an denen sich internationale Gerichte später orientieren könnten.

Zum Abschluss arbeitete der Referent zwei wichtige Problematiken heraus, die neben digitalen Beweismitteln die (internationalen) Strafverfahren verändern werden: Zum einen der Einsatz digitaler Ermittlungsmethoden in Kombination mit Dritten, die dem *IStGH* bei der Beweiserhebung helfen. Zum anderen muss sich neben der Digitalisierung von Ermittlungsmethoden auch mit digitalen Straftaten befasst werden.

[6] Berkeley Protocol on Digital Open Source Investigations, https://bit.ly/4t5r2H8.

[7] Leiden Guidelines on the Use of Digitally Derived Evidence https://bit.ly/3PP15gF.

6. Q&A

In der sich anschließenden Q&A-Session konnten einige offene Fragen und Probleme vertieft diskutiert werden. Dabei interessierte sich das Publikum für datenschutzrechtliche Aspekte und das Herausfiltern relevanter Informationen für den Ermittlungsfall im Falle von Big Data. Der Referent erörtert an dieser Stelle, dass digitale Ermittlungen aufgrund der geforderten Objektivität häufig breit angelegt sind und daher umfangreiche digitale Informationen gesammelt werden müssen, so auch in den sozialen Medien. Auch die Anklagebehörde des *IStGH* sammelt belastende, aber auch entlastende Beweise und Indizien. Zugleich wird hervorgehoben, dass die beim *IStGH* gespeicherten (persönlichen) Daten angemessen aufbewahrt werden. Die Institution unterliegt zwar nicht Europäischen Vorgaben und Vorschriften, wie der DSVGO, entwickelt jedoch eigene, ähnliche Richtlinien.

V. Verteidigung gegen und mit digitalen Beweismitteln von RA Dr. Eren Basar (Wessing & Partner)

Von einem wiederkehrenden Gast und regelmäßigen Teilnehmer, *Dr. Eren Basar*, wurde der vierte und vorletzte Vortrag präsentiert. Der Anwalt gab Einblicke in die praktischen Fragen und Probleme eines Strafverteidigers, wobei aufgrund seiner Spezialisierung insoweit auch immer die Bezüge zum Wirtschaftsstraf- und Unternehmensrecht zu erkennen waren.

1. Status Quo

Der Referent weist darauf hin, dass die Beweisführung von digitalen Spuren äußerst problematisch ist.

a) Allgemeines

Im Grunde dreht sich die heutige Diskussion um die Frage, ob das strenge Beweisrecht, welches im Kern seit dem 19. Jahrhundert unverändert besteht, tatsächlich für das 21. Jahrhundert geeignet ist. Die Erhebung digitaler Daten als Beweismittel und die Digitalisierung spielen dabei eine alltägliche Rolle in den Strafverfahren, wie die Analyse von Smartphones, wodurch Ermittler Zugang zu nahezu tagebuchähnlichen Informationen erlangen können. Neben diesen Beweisdaten können auch Metadaten und Zeitstempel wichtige digitale Spurenelemente sein. Über diese lassen sich beispielsweise der Versendungszeitpunkt oder der Ersteller einer E-Mail ermitteln. Besonders praxisrelevant ist § 23 Geschäftsgeheimnisgesetz.

b) Dritte als Datenquellen

Neben dem Beschuldigten und Strafverfolgungsorgan können mittlerweile auch Dienstanbieter als Dritte eine wichtige Rolle in einem Strafverfahren spielen. Diese sind eine weitere Quelle für Daten. Anfragen bei Telekommunikationsanbietern können jedoch problematisch sein. Im Standardfall wollen Ermittler sog. Bestandsdaten ermitteln, um die Person hinter einem Accountnamen zu identifizieren. Problematisch sind dann sog. Reverse-Ermittlungen im Sinne einer nachträglichen Reverse-Local-History. Dabei handelt es sich um Anfragen bei Providern zur Übertragung von Verkehrsdaten aus einer bestimmten Zelle, um die Identität der Anwesenden in dieser Zelle zu erschließen.

c) Durchsicht und Beschlagnahme von Daten

§ 94 StPO lässt umfassende Ermittlungen im Rahmen der Sicherstellung und Durchsuchung zu. Der Gesetzeswortlaut spricht von "Gegenständen", wobei die Rechtsprechung den Inhalt des Begriffes konturiert. Die Ermittlungsmaßnahmen werden durch § 110 StPO erweitert. Nach der Rechtsprechung des *BVerfG* ist die Durchsicht nämlich ein eigenständiger Teil der Durchsuchungsmaßnahme.

2. Herausforderungen und Probleme

a) Sicherung und Beschlagnahme

Ein gängiges Problem der Sicherung und Beschlagnahme der Datensätze ist die ordnungsgemäße Trennung nach beweisrelevant und irrelevant. Das *BVerfG* gab bereits im Jahre 2005 eine Richtung vor und appellierte, dass der Zugriff auf verfahrensirrelevante Daten aufs Vertretbare zu reduzieren ist. Offen bleibt jedoch, wie die konkrete Umsetzung dieser Vorgaben bei der vollständigen Beschlagnahme eines E-Mail-Accounts zu erfolgen hat.

b) Spannungsfeld des prozessualen Gleichgewichts

Ein weiteres Problem ist der Wettlauf der technischen Möglichkeiten. Die Richtung des Verfahrens kann davon abhängig sein, welche Verfahrensbeteiligten die Daten schneller auswerten können. *Dr. Basar* weist darauf hin, dass Regelungen diesen Konflikt lösen könnten. Weiterhin könnte dadurch auch sichergestellt werden, dass die Datenqualität im Ermittlungsverfahren bereits der Wahrheit so nahe wie möglich kommt.

c) Aktuelle Rechtsprechung - Zwangsentsperrung des Smartphones durch Fingerabdruck

Letzes Jahr hat das *OLG Bremen*[8] eine Entscheidung gefällt, die eine wichtige strafprozessuale Frage diskutiert. Denn bei einer Durchsuchung eines Unternehmens ist der Umgang mit den persönlichen Smartphones der Betroffenen rechtlich umstritten. Kern des Streits ist eine Diskussion um den Grundsatz der Selbstbelastungsfreiheit des Beschuldigten. Anknüpfungspunkt ist, ob die Polizei, um das Smartphone zu entsperren, im Rahmen des § 81b StPO die Fingerabdrücke des Beschuldigten zwangsweise abnehme darf. Und neben der Frage, ob der nemo-tenetur-Grundsatz betroffen ist, eröffnet sich noch

[8] Mittlerweile wurde diese Entscheidung vom *BGH* bestätigt, vgl. *BGH,* NStZ 2025, 560 ff.

ein weiteres rechtlich-dogmatisches Problemfeld, denn auch der Zweck der Vorschrift ist umstritten. Dahingehend wird debattiert, ob die Maßnahme nur einen "Zugang" zum Smartphone und dem Datensatz ermöglicht oder, ob sie eher als Vorfeldmaßnahme von § 94 und 110 StPO einzuordnen ist. Diese Auseinandersetzung ist streng von der einfachen Eingabe des Passworts zu unterscheiden, denn hierbei handelt es sich um die biometrische Erfassung von Fingern und Gesicht.

d) Grenzüberschreitende Ermittlungen bei Datensätzen

Neben dem Smartphone ist auch die Cloud eine wachsende Datenquelle für Ermittler und ein viel diskutiertes Thema. Problematisch ist vor allem die territoriale Zuordnung der gespeicherten Datensätze. Vor einigen Jahren galt die Auffassung, dass Durchsuchungen nach § 110 StPO oder Zugriffe an den deutschen Grenzen enden. Nach aktueller Rechtsprechung ist eine staatliche Eingrenzung richtigerweise nicht möglich, da die Daten durch die Cloud potenziell überall liegen können. Demnach ist es ungewiss, ob Daten in Deutschland oder in einem anderen Hoheitsgebiet liegen. Konsequenterweise ist die Durchsicht in der Cloud zulässig, auch wenn die Daten in einem anderen Staat als Deutschland liegen. Dies wird durch die e-Evidence Verordnung verschärft. Durch die Regelung ist es möglich, dass Ermittler europaweit auf Daten zugreifen können. Das hat Auswirkungen auf die Verteidigung, da der Rechtschutz im Bereich dieser Internationalisierung noch ausgebaut werden muss. Dies hat wiederum zur Folge, dass vermehrt Datenlieferungsvereinbarungen getroffen werden. Die Möglichkeit einer solchen Ermittlungsmaßnahme wird normativ über §§ 94, 95 StPO begründet.

3. Geschäftsgeheimnisgesetz

Besonders praxisrelevant ist das bereits angesprochene Geschäftsgeheimnisgesetz. Typischerweise drehen sich die Fälle um Kündigungen eines Arbeitsverhältnisses. Betroffene möchten bestimmte Daten(sätze) aus ihrer Arbeitszeit mitnehmen, wie selbst erstellte Präsentationen usw. Aufgrund von § 23 GeschGehG ist dies nicht ohne weiteres möglich. Voraussetzung der Norm ist ein materielles Geschäftsgeheimnis, also ein wichtiges Betriebsgeheimnis, welches zugleich von angemessenen Geheimhaltungsmaßnahmen geschützt wird. Diese Voraussetzung ist äußerst umstritten und die Ausgestaltung dieser Maßnahmen ist unklar. Unter anderem kann dies von der Unternehmensgröße abhängig sein.

4. Anforderungen an eine angemessene Verteidigung

a) Herausforderungen und Probleme

Der Referent fordert, dass auch für die Verteidigung in einem Strafverfahren die Möglichkeit bestehen sollte, sich alle Daten und Datenspuren anzuschauen. Um dies umfassend zu ermöglichen, braucht es einen Zugriff auf die Rohdatensätze. Dies gilt umso mehr, da die Polizei die Datensätze zur Durchsicht oder Analyse an Spezialisten, auch an externe Forensiker, delegiert. Es ist jedoch äußert diskutabel, ob ein Forensiker den entsprechenden juristischen und ermittlungstaktischen Blick hat, um alle wichtigen Indizien zu erkennen und zu erheben. *Dr. Basar* sieht hier die Gefahr, dass entlastende Beweise und Indizien übersehen werden. Jedoch vermutet der Referent die zukünftige Lösung darin, dass solche Dokumentanalysen von Künstlicher Intelligenz übernommen werden.

b) Lösungen und Reformvorschläge

Wie auch in vorherigen Vorträgen angesprochen, ergeben sich zwischen der freien richterlichen Beweiswürdigung gem. § 261 StPO und digitalen Spuren Spannungen. Um diesen Konflikt aufzulösen, bietet der Referent Lösungsvorschläge an, wie die Verankerung von best-practice Lösungen in der RiStBV oder die Heranziehung des Leitfadens des BSI zur IT-Forensik zusammen mit englischsprachiger Literatur. Aus diesen Quellen lassen sich einige Eckpunkte für mögliche rechtliche Regulierungen ableiten und herauslesen.

Vor allem bei der Beschlagnahme einer Festplatte sieht der Referent Reformierungs- und Regulierungsbedarf. Gegenwärtig wird diese bei der Beschlagnahme erst bezeichnet, dann übergeben und danach werden Ausdrucke und auswertungsentsprechende Vermerke hergestellt, teilweise auch kurze Übersichten. Das empfindet *Dr. Basar* als ungenügend und fordert den Zugriff auf die Rohdaten auch für Verteidiger, sodass diese die Daten eigenständig analysieren können. Für die notwendigen Ressourcen ist jeder Strafverteidiger selbst zuständig.

Die Integrität kann dann durch die Dokumentation von Gewinnungs- und Verarbeitungsprozessen, die Reproduzierbarkeit und Methodenverlässlichkeit gewahrt werden. Eine erfreuliche Entwicklung zeigt sich in der tendenziell vermehrten Besprechung und Erörterung der Beweiswürdigung und Authentizität von der Rechtsprechung in ihren Urteilen.

Abschließend möchte *Dr. Basar* folgende Reformanregungen mit auf den Weg geben: Der Schutzbereich der Beschuldigten muss gestärkt werden und die Beschlagnahme und Durchsuchung sollten nicht in jedem Verfahren zugelassen werden, v.a. wenn es um Smartphones oder tagebuchähnliche Einträge geht. Zudem sollten Basiskenntnisse der IT-Forensik auch für Juristen gefordert werden, unter anderem im Wirtschaftsstrafrecht.

5. Q&A Session

Im Rahmen der Q&A Session erörtert der Referent ausführlich Datenlieferungsvereinbarungen und die damit einhergehenden Berührungspunkte mit der Datenschutz-Grundverordnung. §§ 45, 48 DSVGO sind diesbezüglich die maßgeblichen Vorschriften. Der Beschuldigte hat keine Mitwirkungspflicht bei Strafverfahren, auch nicht bei Wirtschaftsstrafverfahren und muss der Staatsanwaltschaft nicht entgegenkommen. Der Abschluss einer Datenlieferungsvereinbarung kann aber für beide Seiten eine Win-Win-Situation darstellen. Weiterhin betont der Referent die Bedeutung der Rolle des Sachverständigen und

die Schwierigkeit, ein einmal im Raum stehendes Gutachten anzugreifen, selbst wenn dieses den strafprozessualen Ansprüchen nicht genügt und Mängel aufweist.

VI. IT-Forensik aus Sicht der Polizei, Gregory Kochneff (Bayerisches Landeskriminalamt)

Zum Abschluss der Tagung berichtete *Gregory Kochneff*, Sachverständiger für Mobilfunkforensik beim Landeskriminalamt, über IT-Forensik aus Sicht der Polizei. Neben einem praktischen Einblick in die Mobilfunkforensik als solche und deren Herausforderungen, gewährte er den Zuschauern einen Einblick in die Welt der Ergebnisdaten, also die Probleme und Hindernisse bei der Aufbereitung der Daten für den Auftraggeber und das Leistungsspektrum eines Mobilfunkforensikers. Einige amüsante Filmausschnitte und die Bezugnahme auf praktische Beispiele trugen zu einer informativen und anschaulichen Darstellung des Themengebiets und der Unterhaltung der Zuschauer bei. Frau Liegl bestätigend erläuterte er, dass der Begriff des Sachverständigen weder geschützt ist noch zwangsläufig eine Ausbildung voraussetzt, um vor Gericht als Expert:in stehen zu dürfen.

1. Mobilfunkforensik

Der Referent begann damit, den Bereich der Mobilfunkforensik näher zu erläutern. In der Regel beschäftigt sich ein solcher Forensiker *post mortem* mit den Gegenständen, sprich: er analysiert in der Regel nicht an Live-Systemen.

a) Allgemeines

Die Arbeit des Sachverständigen beginnt durch Zusendung eines Mobiltelefons inklusive des Untersuchungsauftrags durch den Ermittler, das Gerät auszulesen. In der Regel wird der Auftrag nicht weiter konkretisiert, sodass eine Vollsicherung des Gerätes und keine selektive Sicherung vorzunehmen ist. Überwiegend stammen die Daten aus dem Gerätespeicher, vereinzelt wird eine Sicherung des Speichers von Cloud-Anbietern und Telekommunikationsanbietern erforderlich. Während die Daten solcher Provider im Grunde bereits aufbereitet sind, was sich beispielsweise anhand der Abfrage einer SIM-Karte zeigt, wobei man Informationen zum Anschlussinhaber, PIN-Nummer, Rufnummer usw. erlangen kann, werden die Daten direkt aus dem Speicher des Mobilfunkgeräts vom Forensiker entsprechend selbst aufbereitet.

b) Tools

Die Auswertung der Daten erfolgt sodann manuell oder automatisiert durch kommerzielle, zugekaufte Tools. In manchen Fällen wird auf selbstentwickelte Tools zurückgegriffen. In bestimmten Fällen werden sog. Teststellungen durchgeführt, um das technische Verhalten des Geräts nachzustellen und Abläufe und Hypothesen diesbezüglich zu verifizieren. Auch hier liegen Grenzen in der technischen Weiterentwicklung der Mobilfunkgeräte, da man ein altes Handy mit altem Betriebssystem nicht bzw. schwer nachahmen kann.

c) Weitere Speicherquellen

Ferner können die Daten auch direkt aus dem physischen Speicherort extrahiert werden. In Smartphones und Tablets sind unter anderem Speicherbausteine, wie etwa UFS-Chips, microSD-Karten, SIM-Karten und eMMC-Chips, eingebaut bzw. eingelegt. An dieser Stelle sind handwerkliche und elektrotechnische Fertigkeiten gefragt.

2. Ergebnisdaten

Neben der Aufbereitung der Daten ist auch die Bereitstellung für den Auftraggeber ein wichtiger Aufgabenbereich eines Mobilfunkforensikers.

a) Extrahieren der Daten

Ergebnisdaten werden in der Mobilfunkforensik selbst aus den Geräten extrahiert. Dabei erklärt *Herr Kochneff*, dass manchmal Chips ausgelötet oder Speicherkarten aus den Geräten montiert werden, wobei darauf zu achten ist, diese forensisch in möglichst unveränderter Form zu sichern. Zum Teil bedarf es auch invasiverer Maßnahmen, die ein Öffnen und Zerstören der Geräte bedingen. Hierfür muss eine Zerstörungsgenehmigung der Staatsanwaltschaft eingeholt werden, da das Gerät dadurch irreversibel beschädigt wird bzw. werden kann.

b) Aufbereitung der Daten

Für die Recherche der Ermittler werden interaktive Berichtsdateien, wie z.B. der Cellebrite Reader, benutzt. Diese Programme ermöglichen es den Forensikern, Daten aus dem Labor in einer Weise bereitzustellen, die eine ermittlungsfreundliche Datenanalyse ermöglicht. Zudem wird eine automatische Interpretation der Daten durch sog. Enrichments unterstützt, die eine Kategorisierung und Vorabfilterung der Daten gewährleisten. Nach Auffassung des Referenten zeichnet sich ein Trend bezüglich des Einsatzes von Enrichments und KI-gestützten Zusammenfassungen ab. Der Vorteil dieser Funktionen liegt darin, dass sie die Bewältigung großer Datenmassen erleichtern. Gleichzeitig haben diese Funktionen hohe Hardware-Anforderungen, sodass man für eine optimierte Auswertung leistungsstarke Computer braucht. Die Bewältigung der Big Data für Justiz und Ermittler wird darauf hinauslaufen, Technik durch Technik zu regulieren.

c) Bereitstellung

Die Bereitstellung der Ergebnisdaten erfolgt über CD, Festplatten, und/oder Netzwerk. Letztere können den Ermittlungsprozess beschleunigen, indem sie die Möglichkeit eines schnelleren Zugriffs auf die Daten ermöglichen; teilweise noch während der Gutachtenerstellung. Ein Faktor, der die Effizienz bei dieser Vorgehensweise limitiert,

besteht aber im Erfordernis einer funktionierenden Netzwerk-Anbindung und einer bayernweiten Zugriffsverbindung einzelner Behörden. Derzeit stehen die schleppende Digitalisierung und Kostenpunkte einer effizienten Nutzung entgegen.

3. Leistungsspektrum

Herr Kochneff präsentiert seine abwechslungsreichen Aufgabenbereiche, die von der technischen Analyse und Handwerkszeug, über die Gutachtenerstellung und auch in der Weiterbildung von Kolleg:innen und Praktikant:innen bestehen.

a) Vorfeldaufgaben

Das Leistungsspektrum beginnt bereits mit der einfachen Identifikation von Geräten und dem Modell. Ferner werden Zugriffsmöglichkeiten auf relevante Gerätedaten durch Exploits, von den kommerziellen Tools ausgenutzt. Der Rahmen des Möglichen variiert diesbezüglich aber vor dem Hintergrund der vielen Betriebssystem-Updates, neuen Geräte- und Chip-Generationen. Daneben wird der Referent auch tätig, um Geräte wieder Instand zu setzen, um so die Sicherung dieser zu gewährleisten – etwa für den Fall mutmaßlicher Schädigung der Geräte durch Beschuldigte. Je nach Fall und Umständen kann es dann zur bereits erwähnten Auslötung von Chips kommen.[9] Grundsätzliche nachfolgende Aufgaben bestehen in der technischen Untersuchung, Verfügbarkeit zur Beantwortung von Fragen und Gutachtenerstellung. In Großverfahren können die Ergebnisdaten in speziellen Recherche-tools gemeinsam, asservatenübergreifend, analysiert werden.

b) Herausforderungen - technischer Fortschritt

Der technische Fortschritt bietet zum einen neue Möglichkeiten, zum anderen führt dies im Rahmen der Mobilfunkforensik dazu, dass Forensiker ständig neu interpretieren oder einordnen müssen. Die Schwierigkeit besteht demnach vor allem darin, mit der hohen Datenmenge, Asservatenaufkommen, Applikationsvielfalt und Massen an Apps, Betriebssysteme und Sicherheitspatches[10] umzugehen, diese neu zu interpretieren, einzuordnen bzw. zu berücksichtigen. Das kann in der Implementation von neuen Funktionen der Messenger, wie einem Gelesen-Button bestehen, der dann neu interpretiert werden muss. Der Referent veranschaulichte diese Dimensionen, indem er den Blick auf die Identifizierung und Umgang mit kleinsten Details warf, da diese wichtige Kontextinformationen hergeben können. Beispielsweise kann es bei einer Textnachricht, die eine Drohung enthält, einen Unterschied machen, ob dahinter ein schwarzes oder ein rotes Herz gesetzt wird. In diesem Zusammenhang berichtete er von einem offiziellen Standard für die richtige Benennung der Emojis. Eine weitere spannende Neuerung von Smartphones ist die Diebstahlerkennung auf den Geräten, deren genaue Funktion und Möglichkeiten es noch genauer zu erforschen gilt.

c) Präsentation vor Gericht

Gewonnene Erkenntnisse müssen vor Gericht präsentiert werden.

aa) wiederkehrende Aufgaben
Den Vortrag von Frau Liegl bestätigend, berichtet der Referent, dass eine spezifische Vorbereitung kaum möglich und teilweise eine „Live-Interpretation" der Daten vorzunehmen ist. Vor diesem Hintergrund können konkrete Fragestellungen der Ermittler die Arbeit vereinfachen. Trotzdem kann es zu Folgefragen kommen, je nachdem wie vertieft auch das Grund IT-Verständnis der Beteiligten ist, und im Zweifel muss ein Folgegutachten erstellt werden.

Neben der Vorstellung des Gutachtens vor Gericht, bereiten (Mobilfunk)forensiker in Großverfahren auch die Daten auf, damit man über ein Tool Zugriff auf alle dazugehörigen Asservate - PCs, Handys usw. - hat und in diesen recherchieren kann.

Dasselbe gilt für eine zuverlässige IT im Gerichtssaal – etwa im Sinne von funktionierenden Anschlüssen –, die eine anschauliche Visualisierung der digitalen Beweismittel fördert. Eine reibungslose Beweismittelpräsentation gewinnt vor allem dann an Relevanz, wenn den digitalen Beweismitteln im konkreten Verfahren eine tragende Rolle zukommt.

bb) Beispielfälle
Wie wichtig die digitalen Spuren sein können, die wir auf unseren Mobiltelefonen hinterlassen, unterstreicht der Referent in zwei Fällen aus seiner Praxis. Im ersten Fall verhalfen Standortdaten auf den Smartphones der Angeklagten dazu, eine Verwechselung auszuräumen. Dadurch konnte dann der Unschuldsbeweis geführt werden, der die Angeklagten vor einer mehrjährigen Haftstrafe gerettet hatte. In einem anderen Verfahren konnte mittels Datenextraktion aus einem zerstörten Mobiltelefon der relevante Geschehensablauf anhand einer Temperaturkurve rekonstruiert werden. Dabei wurde das Mobiltelefon des Opfers Monate später völlig zerstört im Wasser gefunden. Die Aufgabe des Forensikers bestand nun darin, die Platine aus dem kaputten Mobilgerät heraus zu montieren und zu reinigen. So konnte diese dann in ein baugleiches Gerät implementiert und auf die Funktionen zugegriffen werden. Die daraus gewonnenen Daten konnten den relevanten Moment in der Tatnacht sehr genau wiedergeben.

4. Die Übersetzungsproblematik

Zudem betont der Referent, dass das Schaffen von Verständnis eine wichtige Rolle spielt. Solches kann etwa durch Übersetzung der IT-Sachverhalte in Laiensprache und Bildung von verständlichen Analogien erreicht werden.

[9] Vor allem ältere TSOP-Chips (*thin small-outline package*) lassen sich in Fest-Einbau-Navigationsgeräten oder Skimmern finden.

[10] „Sicherheitspatches" sind kleine Updates für das Betriebssystem, die eine Sicherheitslücke in einem Smartphone-Betriebssystem schließen.

a) Anforderungen an den Sachverständigen

Dabei kommt es auch auf die korrekte Ausdrucksweise im technischen Sinne an, ohne das Gericht mit zu vernachlässigendem Hintergrundwissen zu überfrachten und rechtliche Wertungen oder Mutmaßungen in die verbale Präsentation einfließen zu lassen. Während des Auftrittes vor Gericht gilt es, sich nicht aus der Ruhe bringen zu lassen. Fragen, die spontan nicht beantwortet werden können, sollten im Zweifel zunächst unbeantwortet bleiben und auf ein Nachreichen verwiesen werden. Manchmal kann es sich auch anbieten, eine kurze Pause einzufordern. Aufgrund der extremen Fluktuation der Mobilfunkforensik, bietet sich zur Bewältigung dieser ein stetiger Austausch der Mobilfunkforensiker untereinander an.

b) Analogie zum Verständnis der Datensicherung eines gesperrten Mobiltelefons

Gegenseitiges Verständnis und Kommunikation sind wichtig. Dadurch können die Strafverfolger besser nachvollziehen, wieso unter anderem die Sicherung eines entsperrten Handys lange dauern kann. Der Referent zieht dabei einen Vergleich mit einem Banküberfall, wobei ein Tunnel von einem Gebäude zum nächsten gegraben werden muss. Der Tunnel stellt dabei die Sicherheitslücken dar, die inoffizielle Kanäle zur Nutzung sind. Der Tunnel ist instabil und kann jederzeit beim Einleiten von Daten einstürzen. Kommt man nun am "Datentresor" an, kann man nicht einfach alles markieren und kopieren. Auch hier bedarf es Fingerspitzengefühl. Ist der Tresor offen, kann nur Barren für Barren transportiert werden. Auch die Sicherung der riesigen Datenmengen, die sich auf einem solchen Gerät befinden, dauert.

5. Q&A Session

In Rahmen der letzten Fragerunde wurde zunächst die Funktionsweise der Enrichments genauer geklärt. Es handelt sich dabei um eine Offline-Software, die sich aktuell auf eine Analyse von Bilder- und Videodateien beschränkt und auf Deep-Learning beruht. Eine hundertprozentige Verlässlichkeit der Interpretation durch Enrichments kann aufgrund der schieren Menge an Daten und Updates nicht garantiert werden. Dennoch sei gerade eine Offline-Software geeignetes Mittel zur ersten Interpretation von Rohdaten. Zuletzt wurde über die Relevanz von Standortdaten diskutiert, welche nach Ansicht des Referenten insbesondere auch als entlastendes Beweismittel von Bedeutung sein können und damit das Einschalten der Standortverfolgung nicht nur Nachteile mit sich bringt. Insoweit rät der Referent zu einer selektiven Auswahl, wann wie wo es sinnvoll ist, dass persönliche Daten abgegriffen werden und wann unter Umständen auch nicht.

VII. Schlussworte

Prof. Dr. Christoph Safferling, LL.M. (LSE) und sein ICLU-Team danken allen Teilnehmenden für die rege Beteiligung und die lebhafte, interdisziplinäre Diskussion. Zugleich freuen sie sich auf die Fortsetzung der Veranstaltungsreihe auch im Jahr 2026, dann zum Thema „*Legal Tech im Strafprozess - Chancen, Risiken, Perspektiven*“. Angesichts des zehnjährigen Bestehens des Erlanger Cybercrime Tages in diesem Jahr, erhält die Veranstaltung einen besonderen Charakter.