Schriften zum Strafrecht

Band 450

Die Tätigkeit der IT-Sachverständigen im deutschen Strafverfahren

Von

Nicole Scheler

Duncker & Humblot · Berlin

NICOLE SCHELER

Die Tätigkeit der IT-Sachverständigen im deutschen Strafverfahren

Schriften zum Strafrecht

Band 450

Die Tätigkeit der IT-Sachverständigen im deutschen Strafverfahren

Von

Nicole Scheler

Duncker & Humblot · Berlin

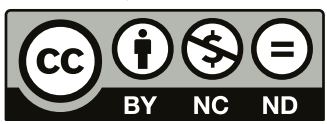
Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) –
Projektnummer 393541319

Der Fachbereich Rechtswissenschaft
der Friedrich-Alexander-Universität Erlangen-Nürnberg hat diese Arbeit
im Jahre 2024 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über http://dnb.d-nb.de abrufbar.

D29



Erschienen bei: Duncker & Humblot GmbH, Berlin
Satz: L101 Mediengestaltung, Fürstenwalde
Druck: Beltz Grafische Betriebe GmbH, Bad Langensalza
Printed in Germany

ISSN 0558-9126
ISBN 978-3-428-19431-5 (Print)
ISBN 978-3-428-59431-3 (E-Book)
DOI 10.3790/978-3-428-59431-3

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

Verlagsanschrift: Duncker & Humblot GmbH, Carl-Heinrich-Becker-Weg 9,
12165 Berlin, Germany | E-Mail: info@duncker-humblot.de
Internet: https://www.duncker-humblot.de

Meinen Söhnen

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2023/2024 vom Fachbereich Rechtswissenschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg als Dissertationsschrift angenommen. Für die Drucklegung konnten Rechtsänderungen, Rechtsprechung und Literatur bis Ende 2024 berücksichtigt werden.

Mein besonderer Dank gilt zunächst meinem Doktorvater, Professor Dr. Christoph Safferling LL.M. (LSE). Seine Hingabe und sein unermüdlicher (internationaler) Einsatz für Forschung, Lehre und Rechtspolitik haben mich zutiefst beeindruckt. Sein stetes Verständnis als Ansprechpartner sowie seine wegweisende Begleitung haben die Fertigstellung dieser Arbeit erst ermöglicht. Ein großer Dank gebührt außerdem meinem Zweitbetreuer Professor Dr. Hans Kudlich, nicht nur für die zügige Erstellung des Zweitgutachtens, sondern auch und vor allem für seine wertvollen Ratschläge, seine warmherzige Art und das stets offene Ohr. Ein „rhino-großes“ Dankeschön auch an Professor Dr.-Ing. Felix Freiling für die Betreuung, seine Unterstützung und den inspirierenden interdisziplinären Austausch. Seine Leidenschaft für die Wissenschaft und seine Visionen für die forensische Informatik waren ansteckend und seine Hilfsbereitschaft unendlich.

Zudem möchte ich auch Professor Dr. Christian Rückert tiefen Dank aussprechen, ohne den ich diese Arbeit gar nicht hätte erstellen können – angefangen mit der Vorgabe des Themas, über den strukturierten und regelmäßigen Austausch im Rahmen der Arbeitsgruppe, bis hin zu den wertvollen Anknüpfungspunkten aus seiner Habilitationsschrift für diese Arbeit. Ebenso herzlich danke ich Dr. Marlene Wüst, meiner Partnerin in Cybercrime, die mich als Kollegin und Freundin großartig, kreativ und humorvoll durch die gemeinsame Zeit am Lehrstuhl begleitet hat! Großen Einfluss auf die Forschung, die diesem Buch zugrunde liegt, hatten außerdem alle Mitglieder:innen des DFG-Graduiertenkollegs 2475 Cyberkriminalität und Forensische Informatik, insbesondere Dr.-Ing. Dominic Deuber, Dr.-Ing. Jan Gruber, Merlin Humml, Dr.-Ing. Benedikt Lorch, Dr. Florian Nicolai, Jenny Ottmann und Dr. Janine Schneider.

Dankbar bin ich auch für den wertvollen Input aus der Praxis der Strafverfolgung. Dank der Zusammenarbeit mit der Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg, namentlich vertreten durch LOStA Thomas Goger, und der Betreuung durch OStA Marc Heusinger und

den dort angesiedelten IT-Forensiker:innen Carina Cedl und Johannes Pollach M. Sc. konnte ich Einsicht in Akten nehmen und am bundesweiten Erfahrungsaustausch von IT-Forensiker:innen teilnehmen und so wertvolle Einblicke in die Praxis erhalten.

Großen Dank schulde ich zudem Dr. Viktor Herlitz für seine spannenden Anregungen aus der Perspektive der forensischen Psychiatrie sowie seine wertvollen Kommentare und sein zügiges Korrekturlesen.

Von Herzen danken möchte ich meiner Mutter, Lydia Eschbach, deren orthographische Hinweise mindestens genauso sehr zum Erfolg dieser Arbeit beigetragen haben wie ihre hingebungsvolle Unterstützung in allen Belangen und die Betreuung der Enkelkinder. Außerdem meinem Vater, Jürgen Eschbach, der mich überhaupt zu diesem Schritt ermutigt hat. Meinem Mann, Max Scheler, und meiner Schwester, Sarah Newrzella, die mich nicht die Nerven und die Leichtigkeit haben verlieren lassen. Und meinen beiden Söhnen, Sven und Karl, denen ich diese Arbeit auch widmen möchte. Jeden Tag aufs Neue beweisen sie, wie wichtig es ist, die richtigen und wichtigen Fragen zu stellen.

Schließlich möchte ich mich bei der Deutschen Forschungsgemeinschaft (DFG) bedanken, die im Rahmen ihres Graduiertenkollegs 2475 Cyberkriminalität und Forensische Informatik sowohl die Erstellung als auch die Veröffentlichung dieser Arbeit – insbesondere auch als Open Access-Veröffentlichung – so großzügig gefördert und damit ermöglicht hat.

Fürth, im April 2025 *Nicole Scheler*

Inhaltsübersicht

Inhaltsverzeichnis

3. Teil

Die Beschaffung des Tatsachenstoffes: Die forensische Informatik 221

Abbildungsverzeichnis

1. Teil

Einführung

IT ruft bei den Menschen[1] ganz unterschiedliche Gefühle hervor, wie sie zuletzt nur bei der Erfindung der Eisenbahn im 19. Jahrhundert und der Entdeckung der Kernspaltung im 20. Jahrhundert zu erleben waren: euphorische Segens- und Heilsempfindungen auf der einen Seite und existenzielle Ängste auf der anderen.

Einerseits beruhigen wir uns damit, dass wir denken, unsere Kinder und Jugendlichen werden sicher wie selbstverständlich in die Welt der IT hinein sozialisiert, andererseits ist zu beobachten, dass unsere Gesellschaft in eine interessenbestimmte neue Welt hineingeworfen wird, ohne Mitsprache, geschweige denn Kontrolle darüber zu haben. In unserer demokratischen Welt schreit das nach Kontrolle (wie das Bemühen um den „Al Act" in der EU zeigt)[2], da sowohl ethische, wirtschaftliche und soziale Risiken bestehen.

Alltag ist eben inzwischen, dass die Möglichkeiten der IT auch eine völlig neue Variante krimineller Aktivitäten hervorgebracht hat oder vorhandene so verändert hat, dass ihnen mit den bisherigen polizeilichen Kompetenzen nicht mehr zu begegnen ist. Das bedarf deshalb auf Seite der Strafverfolgungsbehörden spezieller Fachleute und dann auf der juristischen Seite aber auch einer speziellen Schulung der Beteiligten: Richter, Staatsanwältinnen und Rechtsanwälte sowie spezielle Sachverständige, die diese unterstützen, wenn ihre Sachkenntnisse nicht ausreichend sind.

Wenn nun Sachverständige aus einer „neuen", populär werdenden, forensischen Disziplin in einem Strafprozess anfangen, immer häufiger in Erscheinung zu treten, kommen Fragezeichen auf – manchmal sind es immer wieder die gleichen; und manchmal sind es, den Besonderheiten der bestimmten Wissenschaft geschuldet, neue Fragen – und es wird eine rechtswissenschaftliche Diskussion des Sachverständigenbeweises erforderlich. So auch in Bezug auf den IT-Sachverständigenbeweis. Zum Teil sind (wieder) grundlegende Strukturprinzipien der StPO tangiert (etwa die Waffengleichheit der Prozessbeteilig-

---

[1] Um geschlechtersensible Sprache zu gewährleisten, wird eine abwechslungsreiche Verwendung von männlichen, weiblichen und neutralen Bezeichnungen verwendet. Diese schließen stets alle Geschlechter ein.

[2] Vgl. https://www.zeit.de/2024/33/ki-gesetz-eu-regulierung-ai-act-innovation [7.11.2024].

ten oder die Abgrenzung zu anderen Prozessrollen), aber auch neue Fragen werden gestellt, die speziell die forensische Informatik und den Umgang mit digitalen Beweismitteln betreffen, so bspw., wie sich die Besonderheiten der analysierten Beweisdaten und die Richtigkeitswahrscheinlichkeiten der verwendeten Datenverarbeitungsmethoden auf die Bestimmung der Beweiskraft im Rahmen der tatrichterlichen Überzeugung nach § 261 StPO auswirken.

Immer wieder ist dann von einer „Entmachtung des Richters“[3] die Rede und man sorgt sich um eine immer größer werdende Sachverständigengläubigkeit der Justiz.[4] So hat aber nicht (nur) die zunehmende Komplexität der Lebenssachverhalte und das Ausmaß der Fortentwicklung der Wissenschaften und der damit einhergehenden Vergrößerung des Abstandes zwischen dem Fachwissen einer Sachverständigen und der allgemeinen Bildung einer Richterin oder etwa ihre Bequemlichkeit oder Gleichgültigkeit dazu geführt, dass die Sachverständigen eine immer wichtigere und präsentere Rolle in deutschen Strafverfahren spielen, sondern auch die höchstrichterliche Rspr., von der zunehmend die Beteiligung von Sachverständigen für notwendig gehalten worden ist, hat ganz entscheidend dazu beigetragen.[5]

Wer aber sind diese „heimlichen Richter“[6], die sich so unheimlich gut mit IT auskennen, und den Prozessbeteiligten Sorge bereiten?

Aus Filmen und Büchern kennt man sie aus früherer „analoger“ Zeit noch als Sherlock Holmes, der im London des späten 19. und frühen 20. Jahrhunderts Straftäter mit Beobachtungsgabe und einem Vergrößerungsglas überführt, wobei lediglich eine geringe Menge an Blut, ein latenter Fingerabdruck oder Fußspuren im Moor ausreichten. Die modernen IT-Experten im digitalen Zeitalter kennt man wohl eher aus Serien wie „CSI: Crime Scene Investigation“ oder „Person of Interest“, die 0’er und 1’er vor großen Screens analysieren und denen es gelingt, in nur wenigen Sekunden – per „Mausklick“ – die Täter ausfindig zu machen. Ganz so einfach und v. a. schnell sind IT-forensische Untersuchungen nicht. Allerdings haben die Methoden der forensischen Informatik ein unbeschreiblich großes Potential für die Strafverfolgung. Denn *digitales* Verhalten hinterlässt einen *digitalen* Fußabdruck, der nur schwer zu verwischen ist. Die in Satellitenbildern, abgefangener Kommunikation, Fotos und Videos enthaltenen Metadaten können es Ermittlerinnen ermöglichen,

---

[3] So formulierte es bspw. *Weber*, Gesammelte politische Schriften, S. 344 f.

[4] Vgl. etwa *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 55 m. w. N., wonach sich dieses Abhängigkeitsverhältnis der Strafjustiz zu bestimmten Wissenschaftsgruppen vllt. auch aus übertriebenem Respekt in die moderne Medizin oder Psychologie und mangelndem Vertrauen auf die eigene Urteilskraft ergibt.

[5] Vgl. auch *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 55 m. w. N.

[6] Vgl. *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, V (Vorwort).

den Inhalt bis hin zu Datum, Uhrzeit, Standort und Urheberschaft des digitalen Materials zurückzuverfolgen. So kommen IT-Sachverständige in den verschiedensten Fällen zum Einsatz: Vom „einfachen" Handy, das entschlüsselt und ausgewertet wird, Analysen einer kompletten Infrastruktur von großen KRITIS Unternehmen, bis hin zur internationalen Ebene, um Kriegsverbrecher mithilfe von Anrufdatenaufzeichnungen[7], E-Mails und Social-Media Beiträgen[8] oder Bildern von Google Earth und YouTube-Videos[9] zu „überführen".[10] Am Ende der Arbeit sitzt dieser Sherlock Holmes des digitalen Zeitalters (eine Art „Sheldon Cooper" vllt.) im Gerichtssaal und versucht, sich und sein Handwerk „Fachfremden" zu erklären und diese von der Richtigkeit seiner Ergebnisse zu überzeugen. Seine Aussage beeinflusst dabei nachhaltig die Urteilsfindung des Gerichts.

Was man sich wirklich unter der Arbeit einer IT-Sachverständigen vorstellen kann, welche verfahrensrechtlichen Regeln dabei nach der deutschen StPO gelten und ob dabei wirklich Anlass zur Sorge besteht, soll Gegenstand dieser Arbeit sein.

A. Skizzierung der Forschungsfragen

Für die Bearbeitung der Untersuchung wurden drei Forschungsfragen formuliert:

1. Passt die tatsächlich ausgeführte Praxis der IT-Sachverständigen (noch) unter die Strafverfahrensvorschriften?

---

[7] Im Fall *Pros. v. Ayyash et al.*, Urt. v. 18.8.2020 vor dem Sondertribunal für den Libanon (STL) stützte sich die Staatsanwaltschaft in hohem Maße auf Mobilfunk- und Geolokalisierungsdaten, um zu beweisen, dass die Mitangeklagten den Anschlag in Beirut am 14.2.2005, bei dem der ehemalige libanesische Premierminister Hariri und 21 weitere Personen getötet wurden, verfolgt und geplant hatten. Das erforderte die Beschaffung großer Mengen von Gesprächsdaten. Außerdem ging es um eine computergestützte Analyse einer Explosion („digitaler Sprengstoffbeweis").

[8] *Pros. v. Bemba et al.*, Urt. v. 8.3.2018.

[9] Im Jahr 2016 bekannte sich Al Mahdi vor dem IStGH aufgrund der überwältigenden Beweise, die gegen ihn wegen des Kriegsverbrechens der Zerstörung von Kulturgütern in Timbuktu (Mali) vorgelegt wurden, schuldig. Zu den vorgelegten Beweisen gehörten Satellitenbilder und Videoaufzeichnungen aus dem Internet, die ihn in Verbindung mit Geolokalisierungsberichten mit der Zerstörung bestimmter Mausoleen in Verbindung brachten, vgl. *Pros. v. Al Mahdi*, Urt. v. 27.9.2016.

[10] Vgl. *Freeman*, Fordham International Law Journal Vol. 41, Issue 2 (2018), S. 307 ff.; *De Arcos Tejerizo*, Leiden Journal of International Law (2023), S. 1 f.; vertiefend zur Verifizierung von OSINT-Recherchen auch *Dubberley/Koenig/Murray*, Digital witness, S. 185; *Rückert*, Mit künstlicher Intelligenz auf Verbrecherjagd: Einsatz von Gesichtserkennungstechnologie zur Aufklärung der „Kapitolverbrechen", Verfassungsblog, 22.1.2021, https://verfassungsblog.de/ki-verbrecherjagd/ [26.6.2023].

2. Wie kann eine möglichst (hochwertige) objektive Tatsachengrundlage für die tatrichterliche Überzeugungsbildung i. S. d. § 261 StPO in Bezug auf den IT-Sachverständigenbeweis in einem Strafverfahren geschaffen werden?
3. Wie sieht eine revisionssichere Beweiswürdigung des IT-Sachverständigenbeweises aus?

Ziel bei der Beantwortung dieser Fragen ist es, zunächst auf die Grundstrukturen des IT-Sachverständigenbeweises anhand der deutschen StPO, der begleitenden Rechtsprechung und dazugehöriger Literatur einzugehen. Im Rahmen der Einführung digitaler Beweismittel in das Strafverfahren spielt der IT-Sachverständigenbeweis als bestmögliches und sachnächstes Beweismittel eine entscheidende Rolle.[11] Das zugrundegelegt, soll weiter erörtert werden, wann die eigene Sachkunde der zur Entscheidung berufenen Richter bzw. Staatsanwältinnen erreicht ist und sie zu einer Beauftragung von IT-Sachverständigen i. S. d. Wahrheitserforschungspflicht nach § 244 Abs. 2 StPO verpflichtet sind. Wie stellt sich der „Sachverständigenpool" dar, aus dem die Auftraggeberinnen ihren IT-Experten wählen können? Wie sind die Beweisfragen im Untersuchungsauftrag zu formulieren? Welche Pflichten und Grenzen haben die IT-Forensiker bei der Ausübung ihrer Tätigkeit zu beachten? Wie sehen die verschiedenen Aussagekategorien der IT-Sachverständigen aus? Was ist unter der Leitungspflicht nach § 78 StPO zu verstehen? Wie gestalten sich die Einflussmöglichkeiten der Verfahrensbeteiligten in Bezug auf den IT-Sachverständigenbeweis? Vertieft soll im Zusammenhang mit der Abgrenzung der verschiedenen Verfahrensrollen bzw. Beweispersonen v. a. auch der aktuelle Rechtsstreit in Bezug auf die Anforderungen an die Qualität der Sachkunde des IT-Sachverständigenbeweises in Strafverfahren dargestellt werden. An dieser Stelle soll auch auf die verfahrensrechtlichen Besonderheiten der im Ermittlungsverfahren bestellten und bei den Strafverfolgungsbehörden angesiedelten IT-Forensikern eingegangen werden.

Hier sollen keine – wie in vielen anderen vorangegangenen Werken[12] – Reformvorschläge der Strafverfahrensvorschriften in Bezug auf den Sachverständigenbeweis gegeben werden, sondern vielmehr das Sachverständigenrecht auf den gesetzgeberischen und praxisrelevanten Prüfstand gestellt wer-

---

[11] Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 661 ff.; *Mysegades*, Software als Beweiswerkzeug, S. 56 ff., S. 169 und hier im 2. Teil, A. IV.

[12] Vgl. bspw. *Zwiehoff*, Das Recht auf einen Sachverständigen; *Wellmann*, Der Sachverständige in der Praxis; *Plewig*, Funktion und Rolle des Sachverständigen; *Hepner*, Richter und Sachverständiger; *Pawlak*, Ablehnung des Sachverständigen; *Ley*, Die Pflicht des Strafrichters zur Anhörung weiterer Sachverständiger; *Dippel*, Die Stellung des Sachverständigen im Strafprozess; *Walter*, Sachverständigenbeweis; *Dölp*, Zeitschrift für Rechtspolitik (2004) Vol. 7, S. 235 ff.

den. Auf der Grundlage des geltenden Beweisrechts der StPO soll erarbeitet und gezeigt werden, dass diese Normen grds. geeignet sind, bei entsprechender Auslegung die spezifischen Problemlagen sowohl bei der forensischen Tätigkeit der Sachverständigen als auch bei der Bewertung und Würdigung als Beweis im Strafverfahren zu lösen und letztlich den Richtern dabei zu helfen, die „forensische Wahrheit" zu finden.

Die Betrachtung der verfahrensrechtlichen Vorschriften im Zusammenhang mit der forensischen Tätigkeit, dem Beweiswert und der Würdigung des IT-Sachverständigenbeweises beinhaltet anspruchsvolle Problemstellungen. Nicht nur die bei Sachverständigen im Allgemeinen auftretenden Probleme werden (in Kürze) dargestellt, sondern insb. die mit der IT verbundenen Fragestellungen und Herausforderungen aufgezeigt und analysiert. Der Schwerpunkt der folgenden Betrachtungen liegt dabei auf neuen Erkenntnissen und Gedanken, bei denen bestehende Thesen konkretisiert oder aktualisiert werden, um den neuartigen Anforderungen durch die „digitale Strafverfolgung" gerecht zu werden,

Dafür werden die Grundzüge sowie die Besonderheiten der forensischen Informatik erläutert und Beispiele von forensischen Sicherungs- und Analysemethoden aus der Praxis und dem universitären Raum (sowohl aus juristischer als auch IT-Perspektive) beschrieben, wobei der Anspruch dieser Arbeit nicht auf einer Vollständigkeit der Methoden der forensischen Informatik liegt, sondern vielmehr nur einen Einblick in die Vielseitigkeit geben soll. Der Fokus soll dabei auf der Datenträgerforensik liegen.[13] Die praktischen Einblicke und universitären Diskussionsbeiträge stammen aus verschiedenen Vorträgen, Workshops und dem interdisziplinären Austausch mit Kolleginnen und Kollegen eines Arbeitskreises des DFG-Graduiertenkollegs „Cyberkriminalität und Forensische Informatik"[14], dem „Planspiel" im Rahmen der StPO-Vorlesung von Prof. Safferling,[15] dem Austausch und den Vorträgen von Praktikern (bspw. bei DFRWS EU[16], dem „ECCT"[17], einem bundesweiten Erfahrungsaustausch von bei Staatsanwaltschaften angesiedelten IT-Forensikerinnen und

---

13 Digitale Spuren auf Datenträgern sind nach wie vor am verbreitetsten. Nicht zuletzt deshalb handelt es sich bei der Datenträgerforensik um ein sehr gut erforschtes und weitgehend standardisiertes Gebiet und soll „einfach genug" sein, um als einführendes Beispiel für methodische Fragen der forensischen Informatik zu dienen, so jedenfalls *Dewald/Freiling*, Forensische Informatik, S. 268.

14 https://www.cybercrime.fau.de/ [26.6.2023].

15 *Trapp/Gallmetzer/Safferling*, Erfahrungsbericht JA 10/2020, StPO-Planspiel: Strafprozessrecht für Studierende und Lehrende zum Anfassen.

16 https://dfrws.org/conferences/dfrws-eu-2022/ [26.6.2023].

17 https://www.str1.rw.fau.de/forschung/cybercrime-2/erlanger-cybercrime-tag/ [7.11.2024].

-Forensikern am Veranstaltungsort der ZCB[18] im Jahre 2021) und einer Akteneinsicht[19]. Damit sollen die Herausforderungen für die Strafjustiz im Kontakt mit dem IT-Sachverständigenbeweis im Vergleich zu anderen Disziplinen erklärt werden.

Im Umgang mit digitalen Spuren und den damit einhergehenden Besonderheiten für die Strafverfolgungspraxis haben sich in der (internationalen) forensischen Informatik mittlerweile Mindeststandards etabliert (Maßnahmen zur Sicherstellung der Integrität und Authentizität, korrekten Verwendung wissenschaftlich verifizierter Methoden, Sachkunde des Sachbearbeiters, Wiederholbarkeit und Reproduzierbarkeit der Ergebnisse, Mitteilung über mögliche und nicht mögliche Schlussfolgerungen und Fehlerquellen, die Dokumentation sowie die Einhaltung der verfahrensrechtlichen Grenzen). Nachdem im Rahmen des IT-Sachverständigenbeweises die digitalen Spuren bzw. Ergebnisse von Datenverarbeitungsmethoden als Befundtatsachen (i. V. m. Schlussfolgerungen und Erfahrungssätzen) präsentiert werden, sollen die Arbeiten von Mysegades[20] und insbesondere Rückert[21] als Grundlage und Anknüpfungspunkt dienen. Denn sowohl die ermittelten Beweisdaten, als auch die dabei angewendeten Erfahrungssätze und Schlussfolgerungen sowie Methodiken (wie Tools) werden Grundlage des sachverständigen Gutachtens, womit sie das Tatgericht über den Sachverständigenbeweis in die Tatsachenermittlung mit einbeziehen muss.[22] Rückert hat sich der Erarbeitung grundlegender Regeln für den Umgang mit digitalen Spuren im Beweisrecht der StPO angenommen und die forensischen Mindeststandards in die relevanten Vorschriften der Strafverfahrensordnung, insb. §§ 244 Abs. 2, 261 StPO, „integriert". Dabei berücksichtigte er v. a. die unterschiedlichen Grade der Richtigkeitswahrscheinlichkeit und Probleme der Nachvollziehbarkeit (besonders problematisch bei „Blackbox-Tools").[23] Diese Regeln sollen hier im Speziellen auf die drei Aussagekategorien des IT-Sachverständigenbeweises übertragen und fortgeschrieben werden – von der Befundermittlung bzw. des zugrundeliegenden Datenverarbeitungsvorganges (Dritte Aussagekategorie), über den Vorgang der Befundbewertung bzw. dem Ziehen von Schlussfolgerungen

18 Die in Bamberg ansässige Zentralstelle Cybercrime Bayern (ZCB).

19 Diese konnte dankenswerterweise im Rahmen der Kooperation zwischen der FAU und der ZCB, insb. durch den Einsatz von LOStA Thomas Goger und der Betreuung durch OStA Marc Heusinger und die dort angesiedelte IT-Forensikerin Carina Cedl durchgeführt werden. Insgesamt wurden elf Gutachten mit dazugehörigen Urteilen bzw. Strafbefehlen gesichtet.

20 Software als Beweiswerkzeug.

21 Digitale Daten als Beweismittel im Strafverfahren.

22 Siehe zu dieser Einschätzung auch *Mysegades*, Software als Beweiswerkzeug, S. 53 ff.

23 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 673 ff.

(Zweite Aussagekategorie) sowie der Erstattung von Erfahrungssätzen (Erste Aussagekategorie). Weil diese Datenverarbeitungs- und -analysemethoden der forensischen Informatik – anders als andere forensische Methoden wie etwa die Daktyloskopie, die DNA-Analyse oder die automatisierte Geschwindigkeitsmessung im Ordnungswidrigkeitenverfahren – (bisher) nicht standardisiert sind, müssen sich die Tatgerichte mit der Zuverlässigkeit der Methoden in der Beweiswürdigung intensiv auseinandersetzen. Im Zusammenhang mit der Standardisierung der sachverständigen Methodik soll die Monographie von Mysegades[24] Berücksichtigung finden.

Als Beitrag zur Erleichterung dieses Umstandes – zumindest im Hinblick auf einzelne Kriminalitätsbereiche wie bspw. der §§ 184b ff. StGB – werden Vorschläge aus Praxis und Wissenschaft zusammengebracht, die bei der Kommunikation zwischen den Verfahrensbeteiligten und dem IT-Sachverständigen und der Überprüfung der jeweiligen beweisrechtlichen Anforderungen weiterhelfen könn(t)en.

Denn nicht nur die Übersetzungstätigkeit in eine menschenlesbare Form durch Software stellt die beteiligten Strafjuristinnen bei der Verwendung digitaler Spuren vor eine Herausforderung, sondern gerade auch die (tiefgehende) Erläuterung der Ergebnisse von Datenverarbeitungsvorgängen durch menschliche IT-Sachverständige zu verstehen, nachzuvollziehen und zu bewerten, ist für die Verfahrensbeteiligten oft schwierig. Zentrale Herausforderung ist dabei das Schaffen eines gemeinsamen „Spurenverständnisses“[25] sowie eine einheitliche „Kommunikationsbasis“ zu finden. Dafür sind ein gewisses Grundverständnis und eine Offenheit gegenüber der jeweils anderen Disziplin erforderlich. Das Problem beginnt schon mit der Erkenntnis, wann die eigene Sachkunde in Bezug auf digitale Spuren nicht mehr ausreicht. Weiter geht es damit, dass es dem Auftraggeber gelingen muss, die richtigen und für den IT-Sachverständigen verständlichen Beweisfragen zu formulieren, wofür bereits ein gewisses Basiswissen der IT erforderlich ist („Was kannst du mir geben?“). Das gleiche gilt für die Leitungspflicht und eine authentischen Richterrolle nach §§ 78, 261 StPO. Die Richterinnen dürfen die Verantwortung über die Entscheidung von Rechtsfragen nicht einfach auf die IT-Sachverständigen übertragen (bspw. die Subsumtion unter die einzelnen Tatbestände des § 184b StGB), sondern sie müssen – so wie es auch das Gesetz vorschreibt – die Beantwortung der Rechtsfrage unter Zuhilfenahme des Gutachtens und ggf. durch weitere Fragen eigenverantwortlich herleiten. Dafür ist eine verständliche Form und Sprache (des schriftlichen und mündlichen Gut-

[24] Software als Beweiswerkzeug, S. 231 ff.

[25] Bspw. in Bezug auf die Natur und Eigenschaften digitaler Spuren und wie sie sich verhalten („browser behavior“, „file sharing“, Übertragung von Kommunikationsdaten, etc.).

achtens) erforderlich, so dass die Strafjuristen sowohl die zugrundeliegenden forensischen Methodiken, Schlussfolgerungen und Erfahrungssätze als auch die zugrundeliegenden Ausgangshypothesen, Anfangswahrscheinlichkeiten sowie Unsicherheiten nachvollziehen und eigenverantwortlich auf ihre Plausibilität prüfen sowie unter die normativen Konzepte der StPO subsumieren können.[26] Dagegen ist für die Durchführung des Auftrags ein gewisses juristisches Grundverständnis erforderlich, um gerichtsverwertbare Befunde zu erarbeiten („Was brauchst du?"). Daher soll diese Arbeit ein Beitrag zur Kultivierung dieses „Ping-Pongs"[27] zwischen Strafjustiz und IT sein; d. h. ein interdisziplinäres Grundverständnis der beiden Disziplinen zu schaffen und bei der gegenseitigen Translation in die jeweiligen Sprachsysteme zu helfen.

B. Gang der Untersuchung

Nach der Einführung im vorangegangen 1. Teil ist diese Arbeit weiterhin wie folgt strukturiert:

Der Zweite Teil erläutert zunächst „Grundlegendes zum IT-Sachverständigenbeweis im Strafverfahren". Angeknüpft wird dabei an der von Rückert[28] und Mysegades[29] herausgearbeiteten wichtigen Rolle der IT-Sachverständigen für jegliche Art von aktuellen Strafverfahren, da er in den meisten Fällen das bestmögliche und sachnächste Beweismittel für die Einführung von digitalen Spuren darstellt. Für die Erläuterung der geltenden Prinzipien des Sachverständigenbeweises werden die entsprechenden Verfahrensvorschriften und ihre Auslegung sowie die aktuelle Rechtsprechung herangezogen. Diese werden insb. von den von Toepel[30] erarbeiteten Thesen zu den Grundstrukturen des Sachverständigenbeweises im Strafprozess und die aktuellen Betrachtungen, insb. in Abgrenzung zu anderen Prozessrollen, von Stinshoff[31] ergänzt. Für eine praxisnahe Einschätzung helfen auch Kommentare von Praktikerinnen und Praktikern und erste Eindrücke der Verfasserin, die durch eine Akteneinsicht gewonnen werden konnten. In diesem Kapitel wird insbesondere auf die Besonderheit der Bestellungspraxis der (häufig bei den Strafverfolgungsbehörden angesiedelten) IT-Sachverständigen durch die Staatsanwaltschaft

---

26 Vgl. auch *Ottmann et al.*, DuD 2021, 546 (549).

27 So lautet auch das Ziel von Professor Dr. Christoph Safferling, LL.M. (LSE) und Prof. Dr.-Ing. Felix Freiling, das häufig zu Beginn der gemeinsamen Vorlesung der Professoren im Rahmen des o. g. Planspiels Erwähnung findet.

28 Digitale Daten als Beweismittel im Strafverfahren, S. 661 ff.; *Mysegades*, Software als Beweiswerkzeug, S. 56 ff., S. 169.

29 Software als Beweiswerkzeug, S. 56 ff., S. 169.

30 Grundstrukturen des Sachverständigenbeweises.

31 Operative Fallanalyse.

bzw. ihrer Ermittlungspersonen bereits im Ermittlungsverfahren, die Abgrenzung der Sachverständigentätigkeit von der Verfahrensrolle der (sachverständigen) Zeugen (insb. von Ermittlungspersonen), auf die Anforderungen an die Objektivität („bias“) und die erforderliche besondere Sachkunde sowie gleichzeitig auf die Schwierigkeiten der fehlenden Sachkunde auf Seiten der Auftraggeber eingegangen. Weiter sollen die Pflichten und Grenzen der Sachverständigentätigkeit sowie die drei verschiedenen Aussagekategorien erläutert und die dabei auftretenden Schwierigkeiten der Formulierung des Beweisthemas durch den Auftraggeber (insb. die Trennung zwischen Rechts- und sonstigen Tatsachen) dargestellt werden. Daneben sollen die Einflussmöglichkeiten der Verfahrensbeteiligten auf den mithilfe des IT-Sachverständigen gesammelten Tatsachenstoff hauptsächlich mit Blick auf die prozessuale Waffengleichheit aufgezeigt werden. Letztlich soll herausgearbeitet werden, dass wohl die wichtigste Aufgabe der Auftraggeber und der zur Entscheidung berufenen Richterinnen in der Leitungspflicht nach § 78 StPO besteht; auch diese soll deshalb ausführlichere Erwähnung finden.

Im 3. Teil wird daran anschließend „Die Beschaffung des Tatsachenstoffes: Die forensische Informatik“ betrachtet. Denn, um die Frage beantworten zu können, wie IT-Sachverständigengutachten in Strafverfahren richtig bewertet und gewürdigt werden können, bedarf es zunächst einer Darstellung des Prozesses der forensischen Informatik und seiner Herausforderungen und Besonderheiten – v. a. in Abgrenzung zu anderen forensischen Bereichen. Dabei wird zunächst ein Blick auf die einzelnen Schritte des forensischen Prozesses am Beispiel der Datenträgerforensik geworfen. Hierbei werden die Ausführungen von Freiling und Dewald[32] zugrunde gelegt. Auch sollen die Besonderheiten von digitalen Spuren und Daten sowie die Standards der forensischen Informatik und deren Auswirkungen auf das Beweisrecht näher aufgezeigt werden. Dabei helfen sowohl die erarbeiteten Ergebnisse von Rückert[33], die teilweise auch in der Arbeitsgruppe und dem interdisziplinären Austausch unter Kolleginnen und Kollegen im Rahmen des o. g. Graduiertenkollegs entstanden sind, als auch die Ausführungen von Mysegades zu standardisierten Verfahren im Strafprozess[34]. Besonders wegweisend waren in diesem Zusammenhang auch die Ideen von Freiling, die in einem (inspirierenden) Gespräch aufgekommen sind im Hinblick auf die Besonderheit der Technologie: Die Abgekoppeltheit von der physischen Welt und die dadurch bedingte Universalität.

Im 4. Teil „Die Beweiswürdigung des IT-Sachverständigenbeweises“ soll es schließlich um die Beweiswürdigung von IT-Sachverständigenaussagen

32 Forensische Informatik.

33 Digitale Daten als Beweismittel im Strafverfahren, S. 665 ff., S. 673 ff.

34 Software als Beweiswerkzeug, S. 231 ff.

durch die zur freien Entscheidung berufenen Richterinnen i. S. d. § 261 StPO gehen. Hierbei kann wieder an die Untersuchungsergebnisse von Rückert angeknüpft werden, der die Datenverarbeitungs- und -analysemethoden kategorisiert und in eine Zuverlässigkeitsskala einordnet, die Methoden als nicht „standardisiert" und eine Pflicht zur Berücksichtigung der IT-forensischen Standards bzgl. des § 261 StPO herausgearbeitet hat.[35] Zur Verdeutlichung des Einschätzungsprozesses der Beweiskraft von Indizientatsachen, wie sie auch durch den IT-Sachverständigen ermittelt werden, soll v. a. am Beispiel der Ausführungen von Bender, Nack und Treuer[36] erfolgen.

Für eine schnelle Orientierung über den Inhalt der Arbeit eignen sich die einzelnen Abschnitte der abschließenden Zusammenfassungen sowie die Darstellung der Ergebnisse der Forschungsfragen als zusammenfassender Überblick im 5. Teil.

[35] Digitale Daten als Beweismittel im Strafverfahren, S. 673 ff.; unterstützt werden diese Ergebnisse auch durch die Thesen von *Mysegades*, Software als Beweiswerkzeug, S. 60 ff., S. 118, S. 231 ff.

[36] Tatsachenfeststellung vor Gericht.

2. Teil

Grundlegendes zum IT-Sachverständigenbeweis im deutschen Strafverfahren

Wie in der Einleitung beschrieben, soll es im Folgenden um die Tätigkeit des IT-Sachverständigen im deutschen Strafverfahren gehen. Die Tätigkeit des Sachverständigen ist entsprechend der sich immer weiter verzweigenden Gesellschaft und der sich immer stärker differenzierenden und rasant entwickelnden Technik äußerst mannigfaltig.[1] Wenn der eigene technische Sachverstand für eine Beurteilung nicht ausreicht oder wenn ein Gutachten Dritten gegenüber als glaubwürdiger Nachweis dienen soll, können weder Richterinnen, noch Politiker, Gewerbetreibende oder Privatpersonen auf die Mitwirkung Sachkundiger verzichten.

Wer sich im Gesetz im Einzelnen mit den Aufgaben und Pflichten des Sachverständigen befassen will, sieht sich weitestgehend enttäuscht: Denn wo der Gesetzgeber den Begriff verwendet (vgl. §§ 402 ff. ZPO, § 72 StPO), setzt er seinen Bedeutungsinhalt voraus. Hilft das Gesetz nicht weiter, lässt sich die Frage, wer Sachverständige ist und wie ihre Pflichten zu bestimmen sind, aus dem Begriff selbst und aus der Zweckbestimmung ableiten.[2]

Das – und v. a. warum es dringend notwendig ist, sich mit dem IT-Sachverständigenbeweis im deutschen Strafverfahren auseinanderzusetzen – soll in diesem Kapitel dargestellt werden.

A. Die Dringlichkeit der Diskussion um das Thema des IT-Sachverständigenbeweises

Ziel des Strafprozesses ist die bestmögliche Ermittlung der materiellen Wahrheit.[3] Dabei nehmen neben den klassischen Beweismitteln wie toxikologische Gutachten, Bilder oder Waffen digitale Beweismittel einen immer

---

[1] Vgl. auch *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 1.

[2] Vgl. auch *Wellmann*, Der Sachverständige in der Praxis, S. 1.

[3] *Kudlich/Nicolai*, JA 2020, 881 (886); vgl. u. a. aus der Rspr. des BVerfG zur Pflicht der Wahrheitsermittlung im Strafverfahren: BVerfGE 57, 250 (275); 118, 212 (231); 122, 249 (270); 130, 1 (26); 133, 168 (199 und 226) sowie *Landau*, NStZ 2015, 665 (669). Zur Wahrheitsfindung im Strafverfahren siehe in diesem Teil, B. I.

größeren Raum in Ermittlungsverfahren ein und werden in fast jedem Strafverfahren relevant.[4] Mehr und mehr Kriminalitätsformen sind heutzutage mit digitalen Spuren verbunden. Dies beruht im Wesentlichen auf verschiedenen Entwicklungstendenzen: Zunächst hat Cyberkriminalität i. e. S.[5] an Bedeutung gewonnen. Darüber hinaus verlagert sich die Tatbegehung bei herkömmlicher Kriminalität zunehmend in das Internet (Cyberkriminalität i. w. S.[6]).[7] In nahezu allen Bereichen des täglichen Lebens, sei es der private oder auch der professionelle Bereich, ist die digitale Unterstützung nicht mehr wegzudenken. Von der Smartwatch über den Laptop bis hin zu Auto und mittels Google Street View auch auf den öffentlichen Straßen[8] finden wir (ob gewollt oder ungewollt) Eintritt in die digitale Welt. Banken, Industriezweige, Krankenhäuser, Versorgungsunternehmen, Polizei und Bundeswehr, Feuerwehr, Wissenschaft und vieles mehr sind mittels Computer vernetzt. Das führt dazu, dass mit diesen Geräten bewusst oder unbewusst von Tätern, Opfern oder unbeteiligten Dritten erzeugte Daten wertvolle Anhaltspunkte für die Strafverfolgung liefern können.[9] Wie andere Beweismittel auch, dienen sie der Wahrheitserforschung, und geben Aufschluss über die Identität, den Modus Operandi oder die Absicht der Verdächtigen.[10]

In diesem Zusammenhang ist häufig eine Fragestellung der forensischen Informatik Kern der Ermittlungstätigkeit, bspw. die Deanonymisierung bestimmter IP-/Nutzer-Adressen.[11] Auch in anderen Prozessen, wie in Wirtschaftsstrafverfahren, sind die Anwendungsfälle der forensischen Informatik sehr vielseitig und umfassen Fragen zum Betrug im Online-Handel ebenso wie die Nachverfolgung von Geldflüssen bei Korruptionsdelikten.[12] Daneben

---

4 *Sunde*, Non-technical Sources of Errors, S. 2.

5 Im engeren Sinne geht es dabei um den Schutz und die Integrität informationsverarbeitender Systeme, vgl. *Kochheim*, Cybercrime und Strafrecht in der IuK-Technik, S. 16, Rn. 37.

6 Im weiteren Sinne sind die Straftaten umfasst, die unter der Nutzung informationsverarbeitender Systeme und ihrer großräumigen Vernetzung begangen werden, vgl. *Kochheim*, Cybercrime und Strafrecht in der IuK-Technik, S. 16 Rn. 37.

7 Vgl. dazu auch *Rückert/Wüst*, KriPoZ 2021, S. 65.

8 So laueteten erst kürzlich die Schlagzeilen, dass Google Street View bei Mordermittlungen in Spanien hilft, vgl. https://www1.wdr.de/nachrichten/spanien-mord-google-maps-aufklaerung-100.html [19.12.2024].

9 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/IT-Forensik/it_forensik_node.html [12.4.2023].

10 Vgl. auch *Sunde*, Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation, S. 68.

11 Laut dem Sirius-Report von Europol aus 2020 das relevanteste digitale Beweismittel, vgl. S. 40. https://www.europol.europa.eu/cms/sites/default/files/documents/sirius_desr_2020.pdf [26.6.2023].

12 *Farthofer*, HRRS 2021, 313 (314).

kann es in Massenverfahren wie der §§ 184b ff. StGB[13] oder in Verfahren zu Tatvorwürfen nach dem BtMG notwendig werden, Daten bis hin zu Terabytes an Festplattenspeichern auszuwerten. Dafür ist – mangels gerichts- oder staatsanwaltsseitiger IT-forensischer Expertise – die Sachverständigenbestellung nach §§ 73 Abs. 1, 161a Abs. 1 S. 2 StPO regelmäßig das Mittel der Wahl. Selbst innerhalb des „Pools" der IT-Expertinnen wird oftmals ein sehr unterschiedliches und weiter spezialisiertes Fachwissen gefordert. Die Bedeutung von Sachverständigengutachten kann in diesen Verfahren kaum überschätzt werden, weil sich die erstatteten Gutachten für Staatsanwaltschaften und Gerichte weit überwiegend als handlungsleitend, für die Beschuldigten jedoch prima facie als schicksalshaft darstellen. Dem IT-Sachverständigengutachten kommt in diesen Verfahren eine essenzielle, faktisch streitentscheidende Bedeutung zu.[14]

I. Digitale Beweismittel

Zunächst soll knapp[15] dargestellt werden, was digitale Spuren sind. Gemeinhin werden diese als Spuren definiert, die auf Daten[16] basieren, welche auf informationstechnischen Systemen[17] gespeichert oder übertragen worden sind.[18] Sie stellen den tatsächlichen Ausgangspunkt in der Außenwelt dar, bedürfen aber einer digitalforensischen, kunstgerechten Erhebung, Auswertung und Interpretation, um aus ihnen strafverfolgungsrelevante Erkenntnisse zu gewinnen. Soweit solche digitalen Spuren als Beweismittel in einem Strafverfahren Verwendung finden sollen, spricht man auch von digitalen Be-

---

13 Hier verzeichnet man einen Anstieg von 272, 3 %, vgl. PKS 2022, https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2022/pks2022_node.html [26.6.2023]; auch aktuelle Meldungen in den Medien berichten von diesem Phänomen, vgl. FAZ-Artikel „Darstellungen von Kindesmissbrauch nehmen weiter zu" v. 23.5.2023: https://www.faz.net/aktuell/politik/inland/bka-darstellungen-von-kindesmissbrauch-nehmen-weiter-zu-18913112.html [26.6.2023].

14 Vgl. so ähnlich auch *Vogel/Volkmann*, GesR 2021, 753 f. in Bezug auf medizinische Gutachten in Arzthaftungs- und Arztstrafsachen.

15 Im 3. Teil erfolgt eine vertieftere Auseinandersetzung mit digitalen.

16 Daten sind solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (§ 202a Abs. 2 StGB). Zu den Datenkategorien in der StPO und ihre Zuordnung zum strafprozessualen Begriff der Telekommunikation vgl. MüKo-StPO/*Rückert*, 2. Aufl., § 100a, Rn. 69.

17 Ein informationstechnisches System ist eine Einheit aus technischen Anlagen und Bauelementen, denen eine gemeinsame Funktion zukommt und die der Verarbeitung oder Übertragung von Daten und/oder Informationen dient, vgl. MüKo-StPO/*Rückert*, 2. Aufl., § 100b, Rn. 22.

18 *Dewald/Freiling*, Forensische Informatik, S. 55; *Casey*, Digital Evidence and Computer Crime, S. 12 f.

weismitteln (auch elektronisches Beweismittel).[19] Das können elektronische Dokumente, digitale Bilder, Mails, Chatprotokolle sein genauso wie verschlüsselte Informationen oder Spuren von Angriffen auf Netzwerke.[20] Laut dem aktuellsten Sirius-Report von Europol sind die Verbindungsprotokolle, die IP-Adressen und der Username die wichtigsten digitalen Daten in Ermittlungsverfahren;[21] daraus lässt sich schließen, dass es bei der digitalen Strafverfolgung hauptsächlich um die Identifizierung von Personen geht.

II. Zahlen und Praxisbeispiele

Für rund 85 Prozent der strafrechtlichen Ermittlungen werden elektronische Beweismittel benötigt[22] und in den kommenden Jahrzehnten wird sich kaum mehr ein Strafverfahren finden lassen, in dem digitale Daten nicht in irgendeiner Weise – und sei es nur als erster Spurenansatz – zur Aufklärung beigetragen.[23] Tools der forensischen Informatik werden mittlerweile täglich von Ermittlerinnen der Strafverfolgungsbehörden auf kommunaler, Landes- und Bundesebene, aber auch in der Cyberstrafverteidigung eingesetzt, sowie beim Militär, Menschenrechtsorganisationen und der privaten „e-Discovery"-Industrie.[24]

Aus einer kleinen Anfrage der Fraktion der CDU an den Senat im Land Bremen,[25] hat sich ergeben, dass die dortige KTU im Jahr 2022 294 Fälle im Bereich der Computerforensik und 1003 Fälle im Bereich der Mobilfunkforensik bearbeitete.[26] Eine durchschnittliche Bearbeitungsdauer konnte mit Blick auf die Diversität der Asservate und eine fehlende statistische Erhebung der Bearbeitung nicht valide dargestellt werden. Jedenfalls konnten zu priori-

---

19 Vgl. *Rückert/Wüst*, KriPoZ 2021, S. 65.

20 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/IT-Forensik/it_forensik_node.html [12.4.2023]; einen guten Überblick über mögliche digitale Beweismittel bietet auch *Mason/Seng*, Electronic Evidence, S. 7 ff.

21 Sirius-Report von Europol 2023. https://www.europol.europa.eu/cms/sites/default/files/documents/Factsheet-prespective-of-EU-law-enforcement.pdf [7.11.2024].

22 *Ewald*, Digitale Beweismittel und neue Wege der Strafverteidigung, S. 267 (269).

23 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 2; *Momsen/Hercher*, Digitale Beweismittel im Strafprozess, S. 173 (175); *Momsen*, in: FS Beulke, S. 871 (873 ff.).

24 *Garfinkel*, Digital Investigation (2010) Vol. 7, S. 64.

25 Vgl. https://www.bremische-buergerschaft.de/drs_abo/2023-02-08_Drs-20-1766_b85d6.pdf [12.4.2023].

26 Im Vergleich: Bei der DNA-Analytik waren es 953; bei der Chemie 1941 und der Daktyloskopie 509.

sierende Verfahren (grds.[27] in Fällen laufender Untersuchungshaft, kinderpornografischer Delikte, Kapitalverbrechen und Staatsschutzverfahren) in einem Zeitraum von weniger als 180 Tagen beendet werden (durch den sukzessiven Zulauf von neuen Mitarbeitern).[28] Zu der Frage nach einer Fremdvergabe an externe IT-Sachverständigenbüros äußerten sie, dass durch die Staatsanwaltschaft i. d. R. keine Vergabe von Untersuchungen an private Anbieter von Untersuchungsdienstleistungen erfolge. Soweit es einer inhaltlichen Auswertung der auf den sichergestellten Datenträgern gespeicherten Daten bedarf (z. B. von Chatverläufen), scheide eine Fremdvergabe von vornherein aus.[29]

Die hohen Fallzahlen und die große Bandbreite[30] von Cybercrime i. e. S. und i. w. S.,[31] das Stimmungsbild der überlasteten Strafverfolgungsbehörden im Hinblick auf die Auswertung von IT-Asservaten,[32] die immer größer werdenden Datenmengen, die auf ihre Ermittlungsrelevanz hin gesichtet und danach ausgewertet werden müssen,[33] die langen Verfahrensdauern, die nicht

---

27 Weitere Priorisierungen werden im Einzelfall mit den Ermittlungsdienststellen oder der Staatsanwaltschaft individuell abgestimmt.

28 https://www.bremische-buergerschaft.de/drs_abo/2023-02-08_Drs-20-1766_b85d6.pdf [12.4.2023], S. 7 f.

29 https://www.bremische-buergerschaft.de/drs_abo/2023-02-08_Drs-20-1766_b85d6.pdf [12.4.2023], S. 9.

30 Die Vielfalt reicht von der Beleidigung, über das Sexualdelikt, bis hin zum Waffen- und Drogenkauf sowie zu Verbrechen des Völkerstrafrechts.

31 Vgl. PKS 2023: Die Fallzahlen des Deliktsbereichs Cybercrime belaufen sich im Jahr 2023 auf 134.407 Fälle und nehmen damit nach einem kontinuierlichen Anstieg seit 2016 nun im zweiten Jahr in Folge ab (-1,8 Prozent; 2022: -16.282 Fälle – 3,0 Prozent). Berücksichtigt werden müssen in diesem Zusammenhang jedoch das große Dunkelfeld und, dass viele Tatverdächtige aus dem Ausland heraus agieren; https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2023/Polizeiliche_Kriminalstatistik_2023/Polizeiliche_Kriminalstatistik_2023_node.html [19.11.2024]. Auch bietet ein Blick in das „Bundeslagebild 2020 – Cybercrime“ eine Auflistung relevanter Cyberangriffe in Deutschland, die das Ausmaß verdeutlichen, vgl. Cybercrime – Bundeslagebild Cybercrime 2020, S. 5 f., vgl. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html [26.6.2023].

32 Nach einem Bericht von „SPIEGEL-ONLINE“ lagern deutsche Strafverfolgungsbehörden die Auswertung beschlagnahmter Speichermedien immer häufiger an private IT-Dienstleister aus. Anfragen hätten ergeben, dass zunehmend auch sensible Daten nicht mehr von Behörden, sondern von gewerblichen Anbietern ausgewertet würden, „Privatermittler sichten Beweise bei Kinderporno-Anklagen“, https://www.spiegel.de/netzwelt/web/outsourcing-privatermittler-sichten-beweise-bei-kinderporno-anklagen-a-533078.html [26.6.2023].

33 Insbesondere im Bereich der Strafverfahren wegen Wirtschaftsstraftaten und Kinder- und Jugendpornographie stehen die Ermittlungsbehörden bei Durchsuchungen (vgl. § 110 StPO) mit zunehmender Digitalisierung regelmäßig vor dem Problem, im-

zuletzt auf die Auswertung digitaler Spuren zurückzuführen sind,[34] und darüber hinaus das facettenreiche Angebot privater IT-Sachverständigenbüros[35] legen jedoch nahe, dass neben IT-Forensikerinnen der Strafverfolgungsbehörden auch (und das nicht zu selten) externe IT-Expertinnen als IT-Sachverständige in Strafverfahren beauftragt werden.[36]

Dabei herrscht nach wie vor viel Unsicherheit unter den Prozessbeteiligten im Umgang mit digitalen Beweismitteln und dem IT-Sachverständigenbeweis. Die Zustände und Auswirkungen dieser digitalen Kluft zeigen bspw. die folgenden Fälle und gängigen Praktiken: Der dänische Funkzellen-Daten-Skandal, in dem durch Software-Fehler der Polizei und falsche Daten der Telekommunikationsanbieter bis zu einem Drittel der dort relevanten Standortdaten fehlerhaft in den Prozess eingebracht worden sind;[37] das fehlerhafte Computersystem „Horizon" im Fall der sog. Sub-Postmaster der Britischen Post;[38] die Anwendung fehlerhafter Software wie Cellebrite in deutschen Strafverfolgungsbehörden;[39] misslungene Beweiswürdigungen wie im Kemptener

---

mer größere Datenmengen auf ihre Ermittlungsrelevanz hin sichten und diese danach auswerten zu müssen.

34 Verfahren werden immer langsamer: Die Verfahrenslänge in erstinstanzlichen Strafgerichten in Deutschland verlängern sich. Mittlerweile beträgt die Verfahrensdauer durchschnittlich ca. 8 Monate; vor 10 Jahren waren es noch 6 Monate. Gerechnet ab Eingang bei der Staatsanwaltschaft laufen die erstinstanzlichen Verfahren beim Landgericht im Schnitt sogar mehr als 20 Monate. Das soll u. a. auch an immer mehr Auslandsbezug und immer größer werdenden Datenmengen liegen (so deutscher Richterbund, September 2021), vgl. https://www.drb.de/newsroom/presse-mediencenter/nachrichten-auf-einen-blick/nachricht/news/strafjustiz-am-limit-1 [26.6.2023].

35 Vgl. hierzu die Ausführungen und Beispiele bei B. II. 2. c) aa).

36 So zeichnet sich auch eine weiter steigende Nachfrage nach Expertise und Tools auf dem Gebiet der forensischen Informatik ab, vgl. https://www.mordorintelligence.com/de/industry-reports/digital-forensics-market [26.6.2023].

37 Die Mängel bei der Funkzellen-Datenanalyse führten in Dänemark zur Überprüfung von 10.700 Urteilen und am Ende zur Freilassung von 32 Gefangenen; siehe dazu auch vertiefter *Wacher Lentz/Sunde*, Digital Evidence and Electronic Signature Law Review (2021) Vol 18, S. 1 ff.; https://netzpolitik.org/2019/vorratsdatenspeicherung-in-daenemark-ein-it-fehler-koennte-zu-falschen-urteilen-gefuehrt-haben/ [12.1.2024]; https://www.fr.de/politik/vorratsdatenspeicherung-wurden-daenemark-unschuldige-wegen-falscher-telefondaten-verurteilt-12776492.html [12.1.2024].

38 Zwischen 2000 und 2019 wurden sog. Sub-Postmaster der Britischen Post im Wege der „privat prosecutions" verfolgt, weil ihnen unterstellt wurde, Geld in Größenordnungen veruntreut zu haben. Durch die Untersuchungen von CCRC (criminal cases review commission) wurden massenhafte Wiederaufnahmen wegen Fehlurteils aufgrund ungeprüfter digitaler Beweise aus einem komplexen Computersystem namens „Horizon" erwirkt, vgl. https://www.sueddeutsche.de/politik/horizon-post-office-skandal-justiz-grossbritannien-1.6330303 [23.1.2024].

39 https://www.deutschlandfunk.de/probleme-bei-digitalen-ermittlungen-wenn-forensik-software-100.html [27.6.2023].

Bitcoin Fall;[40] die beweisrechtlichen Schwierigkeiten in den Fällen „EnchroChat“ und „Sky-ECC“;[41] die nicht angepassten zugrundeliegenden Annahmen bei Kryptowährungstransaktionen (Coinjoin/Bitcoin);[42] die tagtäglichen Fehler, die schon bei der Sicherung am Tatort passieren und mögliche Beweise vernichten (z. B. durch Antiforensik-Maßnahmen);[43] oder wenn Lichtbildaufnahmen von Chatprotokollen als Urkundenbeweis in die Hauptverhandlung eingeführt werden, wodurch mögliche Manipulationen ganz einfach übersehen werden (können).[44]

III. Die Besonderheit der forensischen Informatik[45]

Um die Herausforderungen des IT-Sachverständigenbeweises und der digitalen Spuren für das Strafverfahren wissenschaftlich herausarbeiten und untersuchen zu können, ist zunächst auf die Besonderheit der forensischen Informatik einzugehen. Denn obwohl diese eine „ganz normale“ forensische Wissenschaft ist (siehe dazu im 3. Teil, B.), ergeben sich für digitale Spuren und damit auch für die IT-Sachverständigen einige Besonderheiten im Vergleich zu physischen Spuren.[46]

Die IT (Informationstechnologie) gibt es seit dem Aufkommen der ersten Rechenmaschinen und elektronischen Datenverarbeitungssysteme in den

---

40 LG Kempten, 29.10.2014 – 6 KLs 223 Js 7897/13; BGH, 21.07.2015 – 1 StR 16/15; LG Kempten, 13.04.2016 – 13 Ss 360/16; BGH, 27.07.2017 – 1 StR 412/16. Vgl. dazu auch *Brodowski*, StV 2019, S. 385 (S. 386). Schon auf tatrichterlicher Ebene wurden im Rahmen einer Akteneinsicht durch die Verfasserin erhebliche Mängel bzgl. der Beweiswürdigung von IT-Sachverständigengutachten festgestellt (dazu später im 4. Teil dieser Arbeit).

41 Vgl. bspw. *Gebhard/Michalke*, NJW 2022, 655.

42 *Deuber/Ronge/Rückert*, Proceedings on Privacy Enhancing Technologies (2022), Vol. 3, S. 670 ff.

43 So das Beispiel aus der Praxis von Johannes Pollach M. Sc., IT-Forensiker bei der ZCB: Durch Antiforensik-Maßnahmen werden in der täglichen Strafverfolgungspraxis beim Booten des verdächtigen Laptops am Tatort durch technisch nicht versierte Polizeibeamte alle Beweisdaten gelöscht/verschlüsselt und damit unbrauchbar als Beweismittel.

44 Beispiel aus *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 658; *Rückert/Meyer-Wegener/Safferling/Freiling*, Juristische Rundschau (2023), S. 1 ff.: Verwertung von Messengerchats (am Beispiel von WhatsApp-Chats) als Beweismittel im Strafverfahren durch Ausdrucke im Wege des Urkundenbeweises bzw. werden zum Teil sogar nur die Chatinhalte von den Bildschirmen eines Smartphones abfotografiert oder abgefilmt und später die Fotografien oder das Video als Urkunden (bei verlesbarer Fotografie) oder Augenscheinsobjekte (bei Videos oder, wenn es auf nicht verlesbare Informationen in der Fotografie ankommt) in die Hauptverhandlung eingebracht.

45 Zum Begriff siehe unten Dritter Teil, B. I.

46 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 14, S. 55 ff.

1940er Jahren. Seitdem hat sie sich rapide weiterentwickelt und umfasst heute eine Vielzahl von Technologien und Anwendungen, einschließlich Computerhardware, Software, Netzwerke, Internet und Cloud Computing. Sie hat die Art und Weise, wie Menschen und Unternehmen arbeiten, kommunizieren, lernen und leben, grundlegend verändert; wobei die KI (Künstliche Intelligenz) noch einmal einen dramatischen Wandel bewirken wird. Die forensische Informatik gibt es etwa seit den 1980er Jahren, als Computer und digitale Technologie alltäglich wurden und damit auch die Möglichkeiten zur Ausführung, aber auch zur Aufklärung von Straftaten durch die Auswertung digitaler Spuren.[47] Seitdem hat sich die forensische Informatik als eines der wichtigsten Arbeitsfelder der Strafverfolgung etabliert.

Aber was ist – von der immerzu gepriesenen und gleichwohl verteufelten „Schnelllebigkeit" abgesehen – das Besondere an dieser forensischen Wissenschaft?

Die vielen spezifischen Eigenschaften digitaler Spuren finden ihren Ursprung in zwei Besonderheiten: Der Abgekoppeltheit von der physischen Welt und der dadurch bedingten Universalität.

1. Die Abgekoppeltheit von der physischen Welt

Die Besonderheit der digitalen Technologie liegt darin, dass sie auf der Verarbeitung von Informationen basiert, die in binärer Form (Nullen und Einsen) codiert ist. Intuitiv kann die digitale Welt als Zustandsautomat beschrieben werden. Auch wenn dieser Automat in die reale Welt eingebettet ist, bleiben dessen Zustände „diskret"[48]. In diesem Sinne gibt es in der digitalen Welt auch keine Materie. Alle dort manipulierten Artefakte sind schlussendlich Daten, die in diskreter Kodierung im Speicher eines Rechners liegen.[49] Die Daten müssen zwar irgendwo auf einem physischen Datenspeicher vorgehalten werden (magnetisiert), aber wo sich dieser letztlich befindet, ist egal. Man verlässt also die physische Ebene und betritt das Binärsystem; die virtuelle Realität. Mithilfe des Binärsystems können digitale Geräte jegliche Art von Daten verarbeiten, speichern oder übertragen. Damit können alle Arten von

---

47 Die statistische Erfassung von Cybercrime begann 2007, vgl. *Kochheim*, Cybercrime und Strafrecht in der IuK-Technik, S. 1. Siehe zum historischen Überblick digitaler Forensik auch *Meseke*, Digitale Forensik, S. 7 ff.

48 Siehe zur Wortbedeutung „diskreter Zustand" *Dewald/Freiling*, Forensische Informatik, S. 70 f.: Diese Bezeichnung betont, dass es zwischen zwei binären Werten keine Zwischenwerte gibt, d. h. der Computer befindet sich zu jedem Zeitpunkt in einem klar definierten Zustand. In der analogen Welt ist Materie im Gegensatz dazu (nahezu) beliebig zerteilbar, d. h. der analoge Zustand ist gerade nicht „diskret" i. S. d. Informatik.

49 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 61.

Informationen aus der physischen Welt und unserer Phantasie in die virtuelle übertragen und bspw. in Text, Bild, Video oder Audio dargestellt, verbreitet und gespeichert werden.

Und genau hier wird der Unterschied und das Ausmaß der IT im Vergleich zu anderen forensischen Wissenschaften deutlich: Die Daten können auf einem beliebigen Datenspeicher gespeichert sein, um weltweit auf sie zugreifen zu können, und es ist von außen völlig unklar, was auf einem Datenspeicher, wie etwa einem USB-Stick, tatsächlich für Informationen gespeichert sind – das können Ordner von Urlaubsbildern, Steuerunterlagen, Krypto-Wallets oder virtuelle Maschinen sein. In der IT können Datenspeicher und Inhalt einfach voneinander getrennt werden.[50] Menschliche Zellen dagegen sind zwar auch ein Speichermedium, aber eben „nur" für DNA und RNA. Das gleiche gilt für Fingerabdrücke. Manche dieser Speichermedien und die darauf enthaltenen Informationen können auch nicht beliebig oft kopiert bzw. vervielfältigt werden (wie bspw. Blutspuren o. ä.).

Diese Besonderheit wird hier als „Abgekoppeltheit von der physischen Welt" bezeichnet.

Für Cyberermittlungen bedeutet diese Abgekoppeltheit von der physischen Welt, dass es Unmengen an möglichen (auch weit entfernten grenzüberschreitenden) Speicherorten für die ermittlungsrelevanten Daten gibt, die durchsucht werden müssen. Ermittlerinnen müssen sich im Zusammenhang mit der Frage, wo Daten physisch überall gespeichert sein können, einen Netzwerkplan über die ganze Systemlandschaft kabelgebundener oder drahtlos angebundener Geräte erstellen.[51] Vor allem das Auffinden kleiner Speichermedien stellt eine große Herausforderung dar: So gibt es bspw. USB-Sticks oder Speicherkarten in jeder nur erdenklichen Form: Autoschlüssel, Taschenmesser, Schmuck oder Büromaterial und noch dazu können sie überall versteckt werden.[52] Das Ausmaß nimmt unter Berücksichtigung von IoT weiter zu. So müssen zukünftig nicht mehr nur Smartphones, Laptops und Spielekonsolen ausgewertet werden, sondern auch Kühlschränke, Autos und Staubsauger.

Die Abgekoppeltheit der Spureninformation birgt außerdem die Problematik für Cyberermittlungen, dass man durch die Abkehr vom Spurenträger unendlich viele Blickrichtungen ausschließt, die weitere Spureninformationen tragen könnten. Das kann fatale Folgen haben.[53] Oft wird angenommen, dass

---

[50] Das wird noch wichtig im 3. Teil bzgl. digitaler Spuren.

[51] Vgl. dazu vertiefend auch *Dewald/Freiling*, Forensische Informatik, S. 346.

[52] Vgl. dazu vertiefend auch *Dewald/Freiling*, Forensische Informatik, S. 346.

[53] Hätte man bspw. schon in den 1960er Jahren alle Spuren „digitalisiert" und die Spurenträger vernichtet, dann wären alle DNA-Spuren verloren gegangen, weil die Bedeutung dieser Spurenart zu der Zeit noch unbekannt war.

der Austausch zwischen digitaler Welt und nicht-digitaler Welt nur über wohldefinierte Schnittstellen geschieht, wie etwa die Tastatur des Computers. Dadurch wird der Blick auf digitale Spuren stark eingeschränkt. So gibt es physische Phänomene, die sich direkt in digitalen Spuren niederschlagen und mit entsprechenden Techniken ausgewertet werden können, z. B.:[54] Wie ordnet jemand seine Dateien an? Gibt es Sprachkommunikation, z. B. mit Robotern oder „Alexa"[55]? Gibt es Maschinenfingerabdrücke auf den Daten (Kamerasensor)[56]? Gibt es Maschinenartefakte[57]?

Für das Beweisrecht bedeutet die Abgekoppeltheit von der physischen Welt mithilfe des Binärsystems in einem ersten Schritt ein Übersetzungsproblem (was wiederum Folgen für das Unmittelbarkeitsprinzip hat). Nachdem digitale Daten auf der physikalischen Ebene aus Bits („binäre Einheit für die Anzahl möglicher alternativer Entscheidungen in einem binären System")[58] bestehen, sind sie in dieser Speicherform für den Menschen nicht les- und verstehbar. Damit sie von Menschen wahrgenommen werden können und ihr Informationsgehalt zugänglich wird, müssen die Daten von Computerprogrammen in eine menschenwahrnehmbare Form „übersetzt" werden.[59] Der Weg der Information von den physikalischen Bits bis hin zu einer Anzeige auf einem Bildschirm (z. B. als Text, Grafik oder Video) ist, je nach Datenmenge, Informationskomplexität und verwendeter Computerprogramme, unterschiedlich „lang" und komplex. Gemeinsam ist all diesen Vorgängen jedoch, dass die Richter bei der Verwendung von Daten als Beweismittel am Ende dieses Weges nur diejenigen Informationen wahrnehmen und würdigen können, welche ihnen in menschenwahrnehmbarer Form vorliegen.[60]

---

54 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 63; vertiefend dazu Dritter Teil.

55 I. S. v. wie wird kommuniziert, gibt es Auffälligkeiten beim verwendeten Vokabular u. ä.

56 Siehe auch das Beispiel zu Metadaten über Bild- und Videodateien aus *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 655.

57 So verhält sich bspw. ein Mikroprozessor bzw. USB-Stick anders, wenn er altert und oft benutzt worden ist (z. B. Bit-Fehler).

58 https://www.duden.de/rechtschreibung/Bit_Einheit_in_der_EDV [6.12.2021].

59 *Fährmann*, MMR2020, 228 (229); *Warken*, NZWiSt 2017, 329. Dies gilt analog z. B. auch für die Visualisierung eines DNA-Vergleichs. Hierbei spielen standardisierte Methoden der Aufbereitung und Präsentation eine wesentliche Rolle.

60 Zu den Folgen hieraus für das Unmittelbarkeitsprinzip, das hier nicht vertieft werden soll, siehe *Brodowski*, in: Buschmann u. a. (Hrsg.), Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, S. 83; vertiefend zum Übersetzungsproblem siehe auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 653 ff.

2. Die Universalität

Die zweite Besonderheit baut auf der eben angesprochenen Abgekoppeltheit von der physischen Welt auf: die Universalität. Wie oben angedeutet, lassen sich mithilfe dieser Technologie alle beliebigen Informationen kodieren in Bilder, Texte, Töne, Programme oder virtuelle Maschinen; eine neue Schicht des Datenträgers kann wieder anders kodiert sein. Der Informationsgehalt eines Datenträgers kann hoch komplex und eben „universell" sein.[61]

Auch auf die Gefahr hin, das Offensichtliche zu sagen: Elektronische Geräte und digitale Medien sind in unserer modernen Welt – eben deswegen – allgegenwärtig. Es können sowohl die belebten als auch die unbelebten Objekte um uns herum auf digitalisierte Einsen und Nullen reduziert werden: von E-Books über Filme, Tabellenkalkulationen bis hin zu GPS-Geräten, Musik, Familienfotos, von Partnersuche bis hin zur Arbeitssuche, sowie Tagebücher und Rezepte, Auktionen, Bildung und Aktienhandel. Die Menschen stolpern durch Flure und Gehwege, starren auf digitale Geräte, schreiben auf „Whats-App", schauen nach dem Wetter, hören Musik, und scheinen die physische Welt um sie herum nicht wahrzunehmen.[62] Für die Forensik bringt die Technologie mit sich, dass man jedes Beweismittel digitalisieren und digital abspeichern kann. Im Vergleich zu einer menschlichen Zelle, die eine DNA gespeichert hat, kann ein Datenträger Millionen an DNA und Fingerabdruck- oder Waffenscans gespeichert haben.[63]

Für Cyberermittlungen und das Beweisrecht bedeutet die Universalität der IT zunächst, dass man es nicht nur mit einem bestimmten Beweisthema (Identität; berauscht oder alkoholisiert; krank; zu schnell; unglaubwürdig) oder einem bestimmten Deliktsfeld (wie bspw. dem Wirtschafts- oder Verkehrsstrafrecht) zu tun hat, wenn es um digitale Spuren geht. Digitale Spuren fallen sowohl in Spezialbereichen an, wie Datendiebstahl, Cyberspionage etc. (Cybercrime i. e. S.), aber eben auch in allen anderen Lebens- und damit Kriminalitätsbereichen, sobald informationsverarbeitende Systeme als Tatmittel in Betracht kommen (Cybercrime i. w. S.).

---

61 So zeigt bspw. eine ARD-Doku, dass mithilfe der Auswertung des Browserverlaufs ein „Digitaler Zwilling" der Versuchsperson erstellt werden konnte, vgl. https://programm.ard.de/TV/Themenschwerpunkte/Dokus--Reportagen/Wissenschaft/Startseite/?sendung=284874000196530 [27.6.2023].

62 *Harrington*, William Mitchell Law Review (2011) Vol. 38, S. 353 (354).

63 Nur zur Verdeutlichung von „Informationseinheiten": eine DNA hat ca. 100.000 Gene und etwa 3 Milliarden Basenpaare. Der Datenträger bei der DNA-Analyse speichert bei Weitem nicht alles, sondern nur den sequentierten Ausschnitt der DNA, der eine ausreichende Wahrscheinlichkeit für eine Übereinstimmung ergibt.

Auf der einen Seite kämpft man mit dem Phänomen „big data“, auf der anderen Seite hat man die Möglichkeit, Einblicke in das Abbild der analogen Welt mit vielen Ermittlungsansätzen zu bekommen. Mit der richtigen „Expertenbrille“ (und eingegrenzten Untersuchungsaufträgen) kann man in dem „Datenwust“ auch schnell in einen eingegrenzten Bereich kommen und Zugriff auf die ermittlungsrelevanten Daten bekommen. Dafür ist es jedoch notwendig, die Beweisfrage möglichst präzise zu formulieren[64].

Dieses digitale Abbild und die darauf enthaltenen digitalen Spuren sind auch nicht so einfach zu fälschen, was Auswirkungen auf den Beweiswert und die Würdigung hat.[65]

Allerdings erreicht man durch diese Universalität nie eine abgeschlossene Einheit von wissenschaftlichen Erkenntnissen. In abgeschwächter Form gilt das ebenso für die anderen forensischen Disziplinen, denn Wissenschaft ist ein ständiger Prozess, für die IT gilt das jedoch besonders ausgeprägt. So ergeben sich v. a. im Zusammenhang mit der Ermittlung des Beweiswerts und im Rahmen der Beweiswürdigung Schwierigkeiten bei der Beantwortung der Frage, was wissenschaftlich „gesichert“ ist. Es gibt wohl etabliertere Bereiche (z. B. die Datenträgerforensik), und noch ziemlich unerforschte bzw. neuere Kategorien (wie etwa KI oder Cloud-Forensik), bei denen man kaum von „wissenschaftlich gesichert“ sprechen kann.[66]

IV. Der IT-Sachverständige als bestmögliches und sachnächstes Beweismittel

Im Zusammenhang mit dem oben bereits angedeuteten „Übersetzungsproblem“, aufgrund der Abgekoppeltheit von der physischen Welt (siehe A. III. 1.), stellen sich die Fragen, in welcher Form digitale Daten als Beweismittel in die Hauptverhandlung eingeführt werden können und, ob das Tatgericht verpflichtet ist, das qualitativ bessere bzw. sachnähere Beweismittel zu verwenden, wenn dies zur Verfügung steht.[67]

Den sogleich beschriebenen Arten der Beweismitteleinführung ist gemeinsam, dass nicht die Daten selbst Gegenstand der Hauptverhandlung werden, sondern nur diejenigen in den Daten enthaltenen Informationen, welche im Rahmen der gewählten Einbringungsart für das Gericht unmittelbar wahrnehmbar sind. Bedeutsam ist das insbesondere deshalb, weil bestimmte For-

---

64 Dazu sogleich unter B. II. 3. c).

65 Vgl. bspw. *Schneider/Wolf/Freiling*, Forensic Science International: Digital Investigation (2020) Vol. 32, S. 1 ff. Siehe dazu vertiefter im 3. Teil, B. II. 3. c).

66 Siehe hierzu im 4. Teil, A. III. 4. b).

67 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 656 ff.

men der Daten (etwa Ausdrucke oder Visualisierungen der in den Daten enthaltenen Informationen) Manipulationen und unbeabsichtigte Veränderungen an den Daten nicht erkennen lassen und außerdem die Gefahr bergen, dass weitere in den Daten enthaltene Informationen verloren gehen.[68]

Digitale Beweismittel können i. S. d. vier Strengbeweismittel in das Strafverfahren eingeführt werden.[69]

Die Inaugenscheinnahme (§ 86 StPO) gestattet die sinnliche Wahrnehmung des Beweismittels: sehen, hören, riechen, schmecken, fühlen. Digitale Daten bedürfen jedoch einer „Aufbereitung", um deren Informationsgehalt, bspw. als Ausdruck oder durch Abspielen auf einem Bildschirm[70], in Augenschein zu nehmen, z. B. als Bild-[71] und Videodateien[72].

Bei einem Urkundenbeweis wird ein Schriftstück verlesen und damit über die in der Urkunde enthaltene Gedankenerklärung Beweis erhoben (vgl. § 249 StPO). Seit dem 1.1.2018 kann man auch elektronische Dokumente wie eine verkörperte Urkunde verlesen. In diesem Sinne können die Informationen der Daten also zunächst in Form des Ausdrucks in Textform durch Verlesung nach § 249 Abs. 1 StPO oder durch das sog. Selbstleseverfahren nach § 249 Abs. 2 StPO eingeführt werden.[73] Hierbei spielt die sichere und sachgerechte Transformation eine wesentliche Rolle.

---

68 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 655 ff.; dazu auch *Mysegades*, Software als Beweiswerkzeug, S. 56 ff.

69 *Sieber/Brodowski*, in: Hoeren/Sieber/Holznagel (Hrsg.), HdB Multmedia-Recht, Teil 19.3. Rn. 163 ff.

70 *Jahn/Brodowski*, FS Rengier, 409 (410); *dies.* in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 67 (84).

71 In diesem Zusammenhang ist der Beschluss des BVerwG (2. Senat), Beschl. v. 18.6.2020 – 2 B 24.20, v. a. Rn. 9 interessant: Die Beschwerde beanstandet, das Gericht habe die auf den Speichermedien des Beklagten sichergestellten Fotos nicht selbst in Augenschein genommen und damit nicht selbst bewertet, sondern habe sich Zahl und Inhalt der Dateien lediglich durch den Sachverständigen mitteilen lassen (Verstoß gegen den Grundsatz der Unmittelbarkeit der Beweisaufnahme). Im Gegensatz dazu findet sich bspw. auch eine erst kürzlich ergangene Entscheidung des VGH Baden-Württemberg, Beschl. v. 22.8.2023 – DL 16 S 2467/21. Hier haben die Richterinnen entschieden, dass der Grundsatz der Unmittelbarkeit der Beweisaufnahme nicht verletzt ist, wenn sich die Strafverfolgungsbehörden und Sachverständigen nicht auf die originalen asservierten Datenträger stützen, sondern lediglich mit durch die Ermittlungsbehörden erstellten Ergebnisdatenträgern „arbeiten", wenn keinerlei Anhaltspunkte für eine Verfälschung, ergebnisrelevante Unvollständigkeit oder sonstige Manipulation der auf den Datenträgern enthaltenen Daten vorliegen.

72 *Momsen/Hercher*, Digitale Beweismittel im Strafprozess, S. 173 (186).

73 KK/*Diemer*, § 249 Rn. 1; *Momsen/Hercher*, Digitale Beweismittel im Strafprozess, S. 173 (186); siehe bereits *Schäfer*, wistra 1989, 8 (10 f.); *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 654 ff.

Der Zeugenbeweis bezieht sich auf Wahrnehmungen einer Person (bspw. einer ermittelnden „Cyberkriminalistin") und damit auch nur indirekt auf digitale Spuren. Gleiches gilt für Sachverständige, die über ihr Gutachten berichten.[74] Auch hier geht es um eine Transformation der ursprünglichen digitalen Spuren.[75] Hierbei spielt die besondere Sachkunde der Sachverständigen die wesentliche Rolle.

Es geht also in einem ersten Schritt darum, die Daten in eine wahrnehmbare Form zu übersetzen (sowohl beim Augenscheins- als auch beim Urkundenbeweis). Die Personalbeweise (Zeuge und Sachverständige) können dem Gericht in einem weiteren Übersetzungsvorgang dabei helfen, die jetzt wahrnehmbaren Informationen richtig zu interpretieren und zu verstehen.

Bei dem ersten Übersetzungsvorgang in die für das Gericht oft in ihrem Aussagegehalt überschätzten[76] wahrnehmbaren Informationen (Bilder, Videos, Texte, etc.) können viele der für das Strafverfahren relevante Tatsachen, welche in den Daten enthalten sind oder „am" Datensatz erkennbar sind, verloren gehen.[77] Das betrifft v. a. Metadaten über die dargestellten Informationen[78]

---

74 Kommt es nur auf Teile der in den Daten enthaltenen Informationen an (wie z. B. einzelne Textpassagen eines längeren Austauschs von Chatnachrichten) und dabei auch nicht notwendigerweise auf den genauen Wortlaut der Text-Informationen, können die Teil-Informationen auch bei der Vernehmung von Zeugen oder Sachverständigen im Wege eines sog. Vorhalts als Vernehmungsbehelfs in die Hauptverhandlung eingebracht werden, MüKoStPO/*Kreiker*, § 249 Rn. 6; KK/*Diemer*, § 249 Rn. 2, 41; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 654.

75 Vgl. auch *Rückert/Wüst*, KriPoZ 2021, S. 66; vertiefend dazu *Jahn/Brodowski*, in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 67 (84 f.); *Savic*, in: Buschmann u. a. (Hrsg.), Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, S. 71 (80 f.); *Brodowski*, in: Buschmann u. a. (Hrsg.), Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, S. 83 (84).

76 Vgl. dazu v. a. *Marshall*, Digital Evidence and Electronic Signature Law Review (2020) Vol. 17, S. 25; *Mason/Seng*, Electronic Evidence, S. 101 ff.

77 Die gewählte „Übersetzungsart" (das Computerprogramm, das zur sinnlich wahrnehmbaren Darstellung der Informationen verwendet wird) der Daten stellt jeweils nur die aus Sicht der Programmierer des verwendeten Computerprogramms für einen durchschnittlichen Nutzer relevanten Informationen dar.

78 Beispiel aus *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 655 f.: Metadaten über Bild- und Videodateien wie die Serien- und Modellnummer der jeweils aufnehmenden Kamera, die Geolokationsdaten des Bildes oder Datums- und Zeitstempel. Dasselbe gilt auch etwa für E-Mails oder Chatnachrichten, wie die IP-Adresse der verwendeten Computer, Informationen über die am Chat beteiligten Accounts oder weitere Verkehrsdaten wie bspw. Standortdaten. Diese Informationen sind in aller Regel im Datensatz, der das Bild bzw. die Nachricht repräsentiert, enthalten, gehen jedoch bei der sinnlichen Wahrnehmung als Bild oder Verlesung als Urkunde in der Hauptverhandlung verloren. Diese Informationen können für ein Strafverfahren jedoch von großer Relevanz sein – so können der Zeitstempel und die Geo-

bzw. Hinweise auf Manipulationen.[79] Das ist besonders deshalb misslich, weil es einerseits teilweise trivial ist, eine sinnlich nicht wahrnehmbare Manipulation an den darstellbaren Informationen eines Datensatzes vorzunehmen (wie bspw. die Manipulation von WhatsApp-Chatverläufen mithilfe von „Fake-Whats"), andererseits es jedoch technisch äußerst schwierig ist, eine Manipulation so vorzunehmen, dass diese mit technischen Mitteln am Datensatz selbst nicht erkennbar ist.[80] So besagt eine ausgedruckte WhatsApp-Nachricht, die im Urkundenbeweis verlesen wird, noch nichts über den Urheber.[81] Das in Augenschein genommene Bild, das den mutmaßlichen Angeklagten am Tatort zeigt, muss nicht auch tatsächlich eine „originale" Aufnahme vom Tatort sein.[82] Der Mitschnitt einer TKÜ belegt für sich genommen noch nicht, welche Personen miteinander gesprochen haben.[83] Auch das Auffinden eines USB-Sticks mit kinderpornografischen Bilddateien in einer Wohnung beweist noch nicht, dass es der Wohnungsinhaber, geschweige denn der registrierte Compu-

---

lokation eines Bildes oder einer Nachricht den Beschuldigten entlasten, wenn dieser nachweisbar zu dem bestimmten Zeitpunkt an einem anderen Ort war.

79 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 655.

80 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 370, S. 532, S. 655 f. jew. m. w. N. Vertiefter zur Manipulation digitaler Daten hier im 3. Teil, B. II. 3. c).

81 So berichtet *Rückert* von Fällen, in denen Messengerchats in höchstrichterlichen Entscheidungen eine Rolle gespielt haben, und dabei wenig Problembewusstsein deutlich wurde: Ein Beispiel hierfür wäre BGH BeckRS 2019, 2677, wo eine Prüfung des dringenden Tatverdachts nach §§ 129a, 129b, 131 StGB im Rahmen einer Haftprüfungsbeschwerde vorgenommen wurde. Der Tatverdacht wurde im Wesentlichen auf die den Ermittlungsbehörden vorliegende WhatsApp-Kommunikation gestützt. In der Begründung finden sich auch wörtliche Zitate aus den relevanten Chatverläufen. Nicht entnehmen ließ sich den Entscheidungen allerdings, in welcher Form die Chat-Verläufe dem entscheidenden Gericht vorgelegt wurden. Zur Frage, aus welchen Tatsachen das Gericht schließt, dass die verfahrensgegenständlichen Nachrichten tatsächlich vom Beschuldigten stammten, ließ der BGH lediglich verlauten, dass der „Anschluss" durch eine Bestandsdatenabfrage dem Beschuldigten zugeordnet werden konnte und eine anschließende Telekommunikationsüberwachung auch eine tatsächliche Nutzung durch den Beschuldigten ergab (BGH BeckRS 2019, 2677, Rn. 28). Ein Nachweis dafür, dass die WhatsApp-Nachrichten tatsächlich vom Beschuldigten verfasst und abgeschickt wurden, fanden sich nicht. Ebenso wenig war ersichtlich, wie sichergestellt wurde, dass die Nachrichten nicht manipuliert wurden, z. B. einzelne Nachrichten gelöscht oder sogar gefälschte Nachrichtenteile hinzugefügt wurden, vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 370, S. 532, S. 655 f. jew. m. w. N.

82 https://www.zeit.de/digital/2023-04/ki-risiken-angst-umfrage-forschung-kira [27.6.2023].

83 Vgl. auch die Beispiele von *Thiel/Thiel/Fiedler*, DuD 2021, S. 462 f. wie bereits auf internationaler Ebene Politiker über die Identität mittels KI getäuscht wurden (vermeintlicher Nawalny-Mitarbeiter).

ternutzer, war, der diese Bilder vorsätzlich besitzt.[84] Darüber hinaus wird im Laufe dieser Arbeit gezeigt, dass die Interpretation und Überprüfung der Ergebnisse von Datenverarbeitungs- und analysmethoden oft von Experten vorgenommen werden muss und selten Techniklaien überlassen werden kann.[85]

Für eine erschöpfende Beweiswürdigung (siehe dazu im 4. Teil) sollte deshalb unbedingt versucht werden, das bestmögliche und sachnächste Beweismittel zu erheben, zu analysieren und gerichtlich zu verwerten und fehlende Feststellungen durch weitere Beweise zu treffen. Außerdem muss versucht werden, Fehlerquellen bei der Erhebung, Auswertung und Analyse digitaler Spuren weitgehend zu unterbinden.

So führt Rückert[86] treffend aus, dass der IT-Sachverständige in Bezug auf die Verwendung digitaler Spuren das bestmögliche und sachnächste Beweismittel ist.[87] Die qualitativ beste Beweismittelart zur Einführung von aus Daten gewonnenen Informationen ist stets die Untersuchung der Daten (bzw. einer 1:1-Kopie der Daten zur Wahrung der Integrität des Originaldatensatzes, siehe dazu auch später im 3. Teil) selbst. Nur in Ausnahmefällen[88] kann das durch ein entsprechend qualifiziertes Tatgericht mit Hilfe von hierfür geeigneten Computerprogrammen (vergleichbar mit dem Abspielen eines Tonträgers in der Hauptverhandlung)[89] im Wege des Augenscheinsbeweises[90] nach § 86

---

84 So lauten die Einlassungen häufig, dass das durch Schadsoftware auf den Rechner geladen worden wäre; oder sich diese (unentdeckt) versteckt in einer ZIP-Datei mit pornografischem Material befunden hätten. Die IT-Forensiker müssen dann nach Indizien suchen, die für oder gegen die Einlassungen sprechen: z. B. willentlich gespeichert, systembedingt erzeugte (Cache) oder gelöschte Dateien.

85 So können technikbedingte Fehler bei der Datenverarbeitungsmethode entstehen, z. B. bei Zeitstempeln oder Verlust von Daten, vgl. *Sunde/Dror*, Digital Investigation (2019) Vol. 29, S. 101 (102 f.); vgl. auch *Sunde*, Cogent Social Sciences (2022) Vol. 8, S. 1 ff., die von „evidence elasticity" spricht, um das Phänomen zu beschreiben, das die Wandlungsfähigkeit der Interpretation digitaler Beweismittel widerspiegelt.

86 Digitale Daten als Beweismittel im Strafverfahren, S. 657 f. Ähnlich formuliert es auch *Mysegades*, Software als Beweiswerkzeug, S. 56 ff., S. 169.

87 Vgl. Auch zur internationalen Ebene *De Arcos Tejerizo*, Leiden Journal of International Law (2023), S. 4 m. w. N. Vgl. auch *Mason/Senge*, Electronic Evidence, S. 339 m. w. N.; *Moussa*, Egyptian Journal of Forensic Sciences, 2021, S. 1 ff.: Danach müssen digitale Beweismittel stets von einem „computer science and information technology expert" als valide verifiziert werden, um als Beweismittel Eingang in ein Strafverfahren finden zu können.

88 Vgl. auch die Beispiele aus *Momsen/Hercher*, Digitale Beweismittel im Strafprozess, S. 173 (188); *Savic*, in: Buschmann u. a. (Hrsg.), Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, S. 71 (79 f.).

89 Beispiel aus *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 657.

90 Anmerkung: Zwar sind Daten selbst als nicht sinnlich wahrnehmbare Gegenstände keine tauglichen Augenscheinsobjekte i. S. v. § 86 StPO (anders bei Datenträgern, auf denen sich die Daten befinden). Es ist jedoch anerkannt, dass die auf Infor-

StPO selbst erfolgen.[91] In den meisten Fällen jedoch ist das einzige zur Verfügung stehende Beweismittel, das den Informationsgehalt der Daten möglichst vollständig erfasst und Manipulationen mit hoher Wahrscheinlichkeit ausschließen kann, die Beauftragung eines IT-Sachverständigen nach §§ 72 ff. StPO mit der Auswertung und der Einführung der Daten und der enthaltenen Informationen über das von diesem erstattete Sachverständigengutachten sein. So geht auch Mysegades davon aus, dass eine Softwareauswertung, die nicht durch einen gerichtlichen Sachverständigen bedient und vermittelt wird, einen geringeren Beweiswert hat.[92]

In einem weiteren Schritt leitet Rückert aus § 244 Abs. 2 StPO und § 261 StPO ab, dass die Tatgerichte wohl auch in den allermeisten Fällen im Zusammenhang mit der Verwendung von Daten als Beweismittel dazu verpflichtet sein dürften, einen IT-Sachverständigen als bestmögliches und sachnächstes Beweismittel zu beauftragen.[93] Dem Prinzip der erschöpfenden Beweiswürdigung (und einer objektiven Tatsachengrundlage gem. § 261 StPO) folgend, besteht immer dann Anlass zur Heranziehung und Würdigung weiterer Beweismittel, wenn bekannte oder erkennbare Umstände weitere Nachforschungen nahelegen.[94] Darüber hinaus muss auch jedes bekannte oder erkennbare Beweismittel herangezogen werden, wenn auch nur die Möglichkeit besteht, das Beweismittel könnte die Perspektive des Gerichts auf den aufzuklärenden Sachverhalt beeinflussen.[95] Das zugrunde gelegt bedeutet für die meisten

---

mationsträgern verkörperten Informationen dann Gegenstand einer Inaugenscheinnahme sein können, wenn die Informationen durch ein „Übersetzungswerkzeug" sinnlich wahrnehmbar gemacht werden können, wie bspw. im Falle des Abspielens von Tonträgern, Lichtbildern, Videos oder Filmen. Dem folgend werden Daten ganz allgemein immer dann als Augenscheinsobjekt zu behandeln sein, wenn sie durch entsprechende Software in eine durch Menschen sinnlich wahrnehmbare Form übersetzt und damit in Augenschein genommen werden können, vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 656 m. w. N.

91 Zu den Besonderheiten des Vorgehens, wenn im Rahmen der vom Tatgericht selbst durchgeführten Inaugenscheinnahme zusätzliche Informationen in Textform aufgefunden wurden, siehe *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 657.

92 *Mysegades*, Software als Beweiswerkzeug, S. 169.

93 Das kann aber auch vom Einzelfall abhängen, ob nicht auch sachfernere Beweise ausreichen, vgl. auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 659 ff. Vertiefend zur Pflicht der Beauftragung von IT-Sachverständigen im Zusammenhang mit der Verwendung digitaler Spuren im Strafverfahren siehe später in diesem Teil, B. I. 2. und II. 2. a).

94 BGHSt 3, 169 (175); 10, 116 (119); BGH StV 1981, 165; BGH NStZ 1999, 45; *Eisenberg*, Beweisrecht der StPO, Rn. 11.

95 BGHSt 23, 176 (188); 30, 131 (143); BGH StV 1981, 164 f.; BGH StV 1989, 518 f.; BGH NStZ 1985, 324 (325); BGH NStZ 1990, 384; BGH NStZ 1991, 399; *Eisenberg*, Beweisrecht der StPO, Rn. 11.

Fälle, in denen Daten als Beweismittel verwendet werden sollen, dass sich aus deren forensischer Auswertung – und nicht nur durch ihren Ausdruck oder ihre Visualisierung – weitere Erkenntnisse gewinnen lassen (wie Meta-Daten oder Informationen zu einer möglichen Manipulation).[96]

Für die regelmäßig erforderliche Beauftragung von IT-Sachverständigen und der Einführung der (ausgewerteten) Daten als sog. Befundtatsachen (dazu vertiefter in dem Teil, B. II. 3. b) cc) und d) cc)) spricht auch, dass vom Gericht verlangt wird, dass sich dieses bemüht, das im Verhältnis zum Beweisthema unmittelbarere Beweismittel zu verwenden, wenn dieses erreichbar ist und auch sonst keine (zwingenden) rechtlichen Gründe entgegenstehen.[97] Das unmittelbarste Beweismittel im hier diskutierten Kontext ist zwar die eigene „Übersetzung" der Daten in eine sinnlich wahrnehmbare Form und die Inaugenscheinnahme der visualisierten Daten durch das Gericht. Allerdings dürfte das Gericht in vielen Fällen mangels technischer Ausrüstung und persönlicher Qualifikation hierzu nicht in der Lage sein. Das Sachverständigengutachten ist zwar ebenfalls (wie die bloße Verwendung einfacher Ausdrucke oder Urkunden mit dem – teilweisen – Informationsgehalt der Daten) ein nur mittelbares Beweismittel, weil hier das Beweismittel das erstattete Gutachten und nicht die Daten selbst sind. Allerdings ermöglicht das Sachverständigengutachten sowohl die Erhebung der o. g. zusätzlichen (Meta-)Informationen, die ggf. in den Daten vorhanden sind, Informationen in auf dem Datenträger versteckten oder gelöschten Daten und eine Aussage über die Wahrscheinlichkeit einer Manipulation der Daten. Daher ist das IT-Sachverständigengutachten jedenfalls das bestmögliche Beweismittel im Sinne der o. g. Prinzipien.

In der Rechtspraxis[98] ist die regelmäßige Verwendung qualitativ minderwertigerer (bzw. sachfernerer) Beweismittel wie Ausdrucke, visualisierte Darstellungen auf Bildschirmen oder Fotografien oder Videos des Informationsgehalts als Urkunden- oder Augenscheinsbeweis, der auf einem Bildschirm dargestellt

---

96 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 662.

97 BGH NStZ 2008, 358 zur Einführung eines Videos als Augenscheinsobjekt anstelle der bloßen Verlesung eines Vermerks über den BGHSt 32 122 zur unmittelbaren Vernehmung eines V-Mannes; BVerfGE 57, 250 (277); BGHSt 31, 148 (152); 46, 73 (79); BGH, NJW 1984, 65 (66); KK/*Krehl*, § 244 Rn. 28; *Eisenberg*, Beweisrecht der StPO, Rn. 13; zuletzt BVerwG (2. Senat), Beschl. v. 18.6.2020 – 2 B 24.20, Rn. 8: Der Grundsatz der Unmittelbarkeit der Beweisaufnahme besagt u. a., dass im Interesse der Richtigkeit der gerichtlichen Entscheidung die Feststellung der zentralen rechtserheblichen Tatsachen durch Mittel zu erfolgen hat, die in größtmöglicher Nähe zu der infrage stehenden Tatsache, d. h. in möglichst direkter Beziehung zu ihr stehen. Das lediglich mittelbare Beweismittel kann zulässigerweise nur verwendet werden, wenn die Erhebung des unmittelbaren Beweises unmöglich, unzulässig oder unzumutbar erscheint.

98 Auch in der höchstrichterlichen Rechtsprechung, vgl. BGH BeckRS 2019, 2677; BGH BeckRS 2020, 49703.

war, zu beobachten.[99] Dies allein sollte jedoch nicht dazu führen, dass nun in jedem Prozess, in dem eine digitale Spur als Beweismittel verwendet werden soll, eine IT-Sachverständige beauftragt werden *muss*. Häufig setzt die Verteidigung auf „gängige" Nebelkerzen, um Zweifel an der Authentizität und Integrität digitaler Spuren zu schüren.[100] Auch das sollte nicht in jedem Fall die Einbeziehung von (kosten- und zeitaufwendigen) IT-Sachverständigen erforderlich machen. In diesem Zusammenhang wird häufig kritisiert, dass im Bereich der digitalen Spuren und der forensischen Informatik – möglicherweise nur aufgrund ihrer Neuartigkeit – überzogene Anforderungen an ihre Exaktheit gestellt werden, insbesondere mit dem Verweis darauf, dass Tatgerichte, obwohl man nur wenig über die Genauigkeit oder die Motivation einer Aussage eines etwaigen Belastungszeugen weiß, regelmäßig auf diese zurückgreifen, ohne groß Bauchschmerzen zu haben.

M. E. ist deshalb zu berücksichtigen, welche Tatsache das digitale Beweismittel zu beweisen vermag, welche Wichtigkeit diese Tatsache für den zugrundeliegenden Sachverhalt hat, ob weitere Indizien vorliegen, die für diese Tatsache sprechen und welche Qualität die vorgebrachten Zweifel an der digitalen Spur haben.[101] Der BGH verweist in seiner ständigen Rechtsprechung darauf, dass es für alternative Geschehensabläufe, wie bspw. mutmaßliche Fälschungen von Bildmaterial (mithilfe von KI), tatsächliche Anhaltspunkte geben muss.[102] Die angeklagte Person hat plausibel zu machen, weshalb bspw.

---

[99] Beispiel aus *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 789; *Rückert/Meyer-Wegener/Safferling/Freiling*, JR 2023, S. 366 ff.: Verwertung von Messengerchats (am Beispiel von WhatsApp-Chats) als Beweismittel im Strafverfahren durch Ausdrucke im Wege des Urkundenbeweises bzw. werden zum Teil sogar nur die Chatinhalte von den Bildschirmen eines Smartphones abfotografiert oder abgefilmt und später die Fotografien oder das Video als Urkunden (bei verlesbarer Fotografie) oder Augenscheinsobjekte (bei Videos oder, wenn es auf nicht verlesbare Informationen in der Fotografie ankommt) in die Hauptverhandlung eingebracht.

[100] So lauten die Einlassungen neben dem pauschalen „Ich war das nicht", häufig, dass kinderpornografisches Material nicht durch den Angeklagten, sondern durch Schadsoftware auf den Rechner geladen worden wäre; oder sich diese (unentdeckt) versteckt in einer ZIP-Datei mit pornografischem Material befunden hätten.

[101] In Bereichen, in denen es etwa auf exakte Messungen mittels Methoden der forensischen Informatik ankommt und diese Exaktheit nicht gut rekonstruiert oder erklärt werden kann, mag man das Anzweifeln dieser Ergebnisse gut begründen können. Wenn es aber lediglich um das Auslesen eines Speichers von Textnachrichten geht, kann es im Einzelfall unerheblich erscheinen, dass die Auswertung ggf. mithilfe von nicht exakt nachvollziehbarer technischer Methodik vorgenommen wurde, insbesondere dann, wenn sie weiterhin „Sinn ergeben" und sich in das bisher ermittelte Tatbild einfügen. Dann mag die Beauftragung eines IT-Sachverständigen überflüssig erscheinen. Das haben im Einzelfall die Tatrichter zu entscheiden. Siehe dazu bei B. II. 2.

[102] So bspw. in NStZ 2001, 491: Mit naheliegenden Möglichkeiten eines von den Feststellungen abweichenden Geschehensablaufs hat sich der Tatrichter auseinanderzusetzen. Naheliegend ist eine andere Möglichkeit insbesondere dann, wenn die Be-

ein Bild gefälscht worden sein sollte.[103] Auch werden zunehmend zu „bekannten" digitalen Spuren[104] IT-forensische Standards etabliert[105] und durch die Tatrichterinnen mit zunehmenden Berührungspunkten mit der forensischen Informatik „Erfahrungswissen" erworben, das es dem Gericht möglich macht, sich ein eigenes Urteil zu bilden (ob es also bspw. an der Authentizität oder Integrität Zweifel hegen muss) ohne in jedem Fall auf die Kompetenz eines IT-Sachverständigen zurückgreifen zu müssen.[106]

Sind die Verfahrensbeteiligten jedenfalls in Bezug auf die Schwächen und Stärken digitaler Beweismittel sensibilisiert und besitzen ein gewisses Grundverständnis in Bezug auf die IT, dürfte die Entscheidung, wann eine IT-Sachverständige (als bestmögliches und sachnächstes Beweismittel) beauftragt werden muss, besser beurteilt werden können (dazu später mehr bei B. I. 1., II. 2. a)).

V. Die Lücke im wissenschaftlichen Diskurs zum IT-Sachverständigenbeweis

In der juristischen Literatur findet neuerdings eine vermehrte Auseinandersetzung statt mit den Themen Cybercrime, digitale Spuren, der forensischen Wissenschaft der IT mit Bezügen zum Beweisrecht,[107] die Erhebung und Verarbeitung von Daten im Ermittlungsverfahren[108] sowie deren Transfer als Beweismittel in die Hauptverhandlung, deren „Beweiswert"[109] und die Be-

---

weisanzeichen nach der gegebenen Sachlage mit ihr ebenso zu vereinbaren sind wie mit dem vom Gericht für erwiesenen Sachverhalt. Vgl. auch MüKo-StPO/*Bartel*, 2. Aufl., § 261, Rn. 104 f. m. w. N.; KK/*Tiemann*, 9. Auflage, § 261, Rn. 56 m. w. N.

103 Vgl. https://www.lto.de/recht/hintergruende/h/ki-als-ausrede-elon-musk-kuenstliche-intelligenz-midjourney-huang/ [26.6.2023].

104 Beispielsweise besuchte Websiten, Suchanfragen, App-Nutzungsverhalten und -Kommunikation, Online-Käufe, Dateimetadaten, Standortdaten, Zeitstempel, etc.

105 Dazu vertiefter im 3. Teil, B. III. 5.

106 Siehe zu dieser Thematik auch überblicksartig *Mysegades*, Software als Beweiswerkzeug, S. 134 f. m. w. N.

107 Vgl. z. B. *Jansen*, CR 2018, 334. *Dewald/Freiling*, Forensische Informatik; *Heinson*, IT-Forensik.

108 Z. B. *Warken*, NZWiSt 2017, S. 289, 329; *Blechschmitt*, MMR 2018, 361; *Müller*, NZWiSt 2020, 96; *Jahn/Brodowski*, in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 67 ff.; *Wenzel*, NZWiSt 2016, 85; *Schneider*, ZIS 2020, 79; *Basar/Hiéramente*, NStZ 2018, 681.

109 *Müller*, NZWiSt 2020, 96; *Fährmann*, MMR 2020, 228; *Warken*, NZWiSt 2017, 329; *Sieber/Brodowski*, in: Hoeren/Sieber/Holznagel (Hrsg.), HdB Multmedia-Recht, Teil 19.3. Rn. 163 ff.; *Brodowski*, in: Kipker (Hrsg.), Cybersecurity, Kap. 13 Rn. 55 f.; *Wabnitz/Janovsky/Schmitt/Bär*, Kap. 28 Rn. 58 f.; *Knopp*, ZRP 2008, 156; *Marberth-Kubicki*, Computer- und Internetstrafrecht, Rn. 607 ff.; *Momsen*, in: FS Beulke,

weiswürdigung von digitalen Daten und Datenverarbeitungsmethoden im Strafverfahren.[110]

Es besteht eine große Auswahl an wissenschaftlichen Arbeiten zum Sachverständigenbeweis bzgl. seiner Grundstrukturen[111] und in Bezug auf andere forensische Bereiche[112]. Eine Lücke besteht jedoch im Bereich der forensischen Informatik, die es zu schließen gilt. Die Werke, die v. a. aus den Anfängen der jeweiligen forensischen Disziplinen in der gerichtlichen Praxis stammen, dienen hier als Basis für die Sachverständigenvorschriften, die als Maßstab für die („neue") Praxis der IT-Sachverständigen angelegt werden sollen und deren Einhaltung hier untersucht wird. Zudem helfen die Werke als Vorbild bzw. Vergleich für die Erstellung von forensischen Standards und den Umgang der gerichtlichen Praxis mit „neuen" forensischen Beweisen.

Vereinzelt findet sich auch Literatur zum IT-Sachverständigenbeweis, jedoch nur in Bezug auf Einzelfragen. So gibt es einen Aufsatz, der sich auf die Abgrenzung zwischen der Sachverständigen- und Ermittlungstätigkeit konzentriert[113] und die erst kürzlich erschienene über alle drei prozessrechtlichen Fachsäulen (StPO, ZPO, Verwaltungsverfahren) hinweg angelegte Monographie von Mysegades, die durch die Einordnung von Software als Beweiswerkzeug zum Sachverständigenbeweis auch kurze Ausführungen zum Sachverständigenrecht trifft;[114] die dort herausgearbeiteten Thesen konzentrieren sich auf die Prüfung der sachverständigen Methodik durch das Tatgericht.[115]

S. 871 ff.; *ders.*, in: Beck/Meier/Momsen (Hrsg.), S. 67 ff.; *ders.*, in: Walter (Hrsg.), HdB Industrie 4.0, S. 61 (S. 76 ff.); *Momsen/Hercher*, Digitale Beweismittel im Strafprozess, S. 173; *Jahn/Brodowski*, in: FS Rengier, S. 409 ff.; *dies*., in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 67 ff.; *Rückert*, in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 9 ff.; *Sieber*, Gutachten C zum 69. Deutschen Juristentag 2012, S. 67 ff. und 127; *Savic*, in: Buschmann u. a. (Hrsg.), Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, S. 71; *Brodowski*, in: Buschmann u. a. (Hrsg.), Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, S. 83; *Heinson*, IT-Forensik; *Savic*, Die digitale Dimension des Strafprozessrechts; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, insb. S. 651 ff.

110 Zur KI als Lügendetektor: *Rodenbeck*, StV 2020, 479; zur Bezugnahme nach § 267 Abs. 1 S. 3 StPO auf digitale Daten im Urteil *Gercke/Wollenschläger*, StV 2013, 106; zum „Outsourcing" der Auswertung von Daten auf private Sachverständige *Wackernagel/Graßie*, NStZ 2021, 12 und *Momsen/Rackow/Schwarze*, NStZ 2018, 625; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, insb. S. 651 ff.; *Mysegades*, Software als Beweiswerkzeug; zuletzt *Hess*, Digitale Technologien und freie Beweiswürdigung.

111 V. a. *Toepel*, Grundstrukturen des Sachverständigenbeweises.

112 V. a. die operative Fallanalyse; die psychologische und psychiatrische Forensik; die DNA-Analyse, die Daktyloskopie und die BAK-Analyse.

113 *Wackernagel/Graßie*, NStZ 2021, 12.

114 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 53, S. 134 f.

115 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 118 ff.

Auch geht Hess in ihrer Arbeit auf die Beweiswürdigung des Sachverständigenbeweises ein,[116] der Fokus ihrer Arbeit liegt dabei aber auf dem Einfluss und den Einsatzmöglichkeiten technologiegestützter Beweise und Legal-Tech-Anwendungen in der Sachverhaltsfeststellung im Strafprozess, nämlich Entscheidungsunterstützungssysteme für Tatrichterinnen in Form von KI-gestützten Aussageanalyse- sowie Indizienbewertungssystemen.[117] Weiter reihen sich Werke ein, die sich ausschließelich mit dem IT-Sachverständigenrecht für das Zivilrecht beschäftigen[118] oder andere nationale Rechtsordnungen thematisieren.[119] Eine ganzheitliche Betrachtung und Analyse der aktuellen Fragen in Bezug auf die Tätigkeit von IT-Sachverständigen, ihrem Beweiswert und einer Beweiswürdigung durch das deutsche Tatgericht im Sinne der StPO fehlt.

Für die hiesige Untersuchung wird v. a. die kürzlich erschienene Habilitationsschrift von Rückert[120] relevant. In seiner Forschungsarbeit in Bezug auf die Verwertung und Würdigung von, durch die strafprozessualen Dateneingriffe erlangten, digitalen Daten als Beweismittel in der Hauptverhandlung, knüpft er an die Monographien von Savic[121] und Heinson[122] an und schafft eine dogmatische Anbindung der Erhöhung des Beweiswerts an das Beweisrecht der StPO. Dafür bindet er die Standards der forensischen Informatik in das Beweisrecht ein. Weiter trifft er u. a. spezifische Ausführungen dazu, welche Vorgaben das Recht der Beweiswürdigung für die Verwertung von Daten und Datenverarbeitungsmethoden vorsieht und bespricht dabei eben auch die spezifischen Herausforderungen bei der Würdigung der Ergebnisse komplexer (statistischer und selbstlernender) Datenverarbeitungs- und -analysevorgänge.[123] Für die Analyse des IT-Sachverständigenrechts wird v. a. Kapitel 8 von Rückerts Arbeit relevant. Hier werden Regeln aufgestellt, wie Datenverarbeitungs- und -analyseergebnisse in der Beweiswürdigung zu behandeln sind, insbesondere unter Berücksichtigung der unterschiedlichen Grade der

116 *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 196–212.

117 *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 36 ff.

118 *Hoppen/Streitz*, CR 2007 Heft 4, 270 (271 ff.).

119 Vgl. bspw. *Butler/Choo*, Security Journal (2016) Vol. 29, S. 306 ff.; *Sunde*, Non-technical Sources of Errors. So auch die rechtsvergleichende Betrachtung bzgl. allgemeiner Zulässigkeitsvoraussetzungen des Sachverständigenbeweises und dem Konfrontationsrecht gegenüber Sachverständigen von *Mysegades*, Software als Beweiswerkzeug, S. 185 ff.

120 Digitale Daten als Beweismittel im Strafverfahren.

121 *Savic*, Die digitale Dimension des Strafprozessrechts.

122 *Heinson*, IT-Forensik.

123 Im Übrigen sieht auch er Bedarf an der Aufarbeitung der Rolle des „IT-Forensik-Sachverständigen" in der Hauptverhandlung durch Einzelmonographien, vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 651.

Richtigkeitswahrscheinlichkeit und etwaige Probleme der Nachvollziehbarkeit (besonders problematisch bei „Black Box Tools“).[124] Diese Regeln sollen hier im Speziellen auf die drei Aussagekategorien des Sachverständigenbeweis übertragen und fortgeschrieben werden – also von der Befundermittlung bzw. des zugrundeliegenden Datenverarbeitungs- und -analysevorganges (Dritte Aussagekategorie), über den Vorgang der Befundbewertung bzw. dem Ziehen von Schlussfolgerungen (Zweite Aussagekategorie) sowie der Erstattung von Erfahrungssätzen (Erste Aussagekategorie). Darüberhinaus soll neben den Ausführungen von Mysegades zur Prüfung der sachverständigen Methodik durch das Tatgericht, insbesondere an seinen Thesen zur Standardisierung von Datenverarbeitungsmaßnahmen[125] und an den besonderen Problemen der Beweiswürdigung bei der Verwendung nicht nachvollziehbarer Software angeknüpft werden.[126]

Die Arbeiten dienen daher als Grundlage der in dieser Untersuchung folgenden Ausführungen, die die dort entwickelten Gedanken zum Beweiswert von Daten, zur Standardisierung von Datenverarbeitungs- und -analysemaßnahmen und die Vorgaben der Beweiswürdigung für die Verwertung von Daten und den Verbarbeitungs- und -analysemethoden auf den IT-Sachverständigenbeweis übertragen und ergänzen.

VI. Zusammenfassung „Dringlichkeit der Diskussion um das Thema des IT-Sachverständigenbeweises“

Die Ausführungen sollen verdeutlichen, dass der IT-Sachverständige als bestmögliches und sachnächstes Beweismittel und die Verfahrensbeteiligten in Bezug auf die Bewertung und Würdigung vor besondere Herausforderungen gestellt werden. Das Phänomen „Cybercrime“, der exponentielle Anstieg digitaler Spuren und die damit einhergehenden Besonderheiten der Technologie sowie die Digitalisierung investigativer Methoden bedingt neue und komplexere Anforderungen bzw. Expertisen in Bezug auf die die Ermittlungen und die Forensik. Die massenhaften Daten, die strukturlos, nicht deutlich erkennbar und oft nur temporär (auf Hardware, Software oder im Internet) aufzufinden sind, müssen entdeckt, gesichert, gefiltert und gerichtsverwertbar ausgewertet werden.

Mit zunehmender Bedeutung des IT-Sachverständigenbeweises in der strafprozessualen Praxis wird sich die rechtswissenschaftliche Literatur (optimal

---

124 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 673 ff.; S. 688 ff.

125 Wobei sein Schwerpunkt im Ordnungswidrigkeitenrecht liegt.

126 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 175 ff.

mit Hinzuziehung von IT-Fachleuten) mit dem Thema und den Besonderheiten der forensischen Informatik auseinandersetzen müssen.

B. Die deutsche StPO und der Sachverständigenbeweis

Die Problematik der Grundstruktur des Sachverständigenbeweises ist bestimmt vom Verhältnis der Autorität und Rationalität.[127]

Nach dem deutschen Strafprozessrecht soll die Autorität zur Entscheidung über eine Straftat im Regelfall schwerpunktmäßig beim Gericht konzentriert sein. Durch Einflussmöglichkeiten anderer Verfahrensbeteiligter wird dieses Grundmodell oft in unterschiedlichem Ausmaß verformt. Die Sachverständigen hingegen erhalten gegenüber ihren Auftraggebern als ein bloßes Beweismittel keine eigenen Entscheidungs-Autoritäten. Dennoch sollen sie das Gericht durch ihre Gutachtenerstattung in Bezug auf die Sachverhaltserforschung unterstützen, die das Gericht selbst nicht durchzuführen in der Lage wäre, weil es seinen eigenen Kenntnissen auf dem Gebiet misstrauen muss. Der Weg zu einer eigenen Entscheidung des Gerichts erscheint in solchen Fällen mit vielerlei Hürden versehen, denen Rechnung getragen werden muss, um die unter diesen Umständen bestmögliche Würdigung des Beweismaterials zu erhalten.[128]

Mit der Funktion der Sachverhaltserforschung müssen auch die einzelnen Ausgestaltungen der Sachverständigenvorschriften durch den Gesetzgeber sowie die (höchstrichterliche) Rspr. betrachtet werden. Dabei sollen die Spielräume und die Grenzen der Sachverständigentätigkeit bei ihrem Beitrag zur Wahrheitsermittlung im Strafverfahren verdeutlicht werden.

I. Die Wahrheitsfindung im Strafverfahren

Das BVerfG sieht die Aufgabe des Strafprozesses darin, den Strafanspruch des Staates um des Schutzes der Rechtsgüter Einzelner und der Allgemeinheit willen in einem justizförmigen Verfahren durchzusetzen und dem mit Strafe Bedrohten eine wirksame Sicherung seiner Grundrechte zu gewährleisten. Der Strafprozess hat das aus der Würde des Menschen als eigenverantwortlich handelnder Person und dem Rechtsstaatsprinzip abgeleitete Prinzip, dass keine Strafe ohne Schuld verhängt werden darf, zu sichern und entsprechende verfahrensrechtliche Vorkehrungen bereitzustellen. Zentrales Anliegen[129] des

---

127 Vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 1.

128 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 1.

129 Es wird auch vom „obersten Ziel des Strafverfahrens“ (vgl. BGH NJW 1956, S. 1647) oder auch vom „beherrschenden Prinzip des Strafverfahrens“ (vgl. Löwe/Rosenberg/*Gollwitzer*, § 244 Rn. 38) gesprochen.

Strafprozesses ist die Ermittlung des wahren Sachverhalts[130], ohne den sich das materielle Schuldprinzip nicht verwirklichen lässt.[131]

Das Gericht ist verpflichtet, von Amts wegen selbstständig (§ 155 Abs. 2 StPO), d. h. ohne Bindung an Anträge oder Erklärungen der Prozessbeteiligten, die Tatsachengrundlage des Tatvorwurfs umfassend zu untersuchen und aufzuklären (§ 244 Abs. 2 StPO, der Amtsermittlungsgrundsatz), bevor es eine Entscheidung trifft. Bei dieser Entscheidung ist das Gericht i. S. d. § 261 StPO grundsätzlich „frei", soweit die Richter persönliche Gewissheit haben.[132] Nur mit dem Erstreben, die materielle Wahrheit zu erforschen, kann eine angemessene Tatsachengrundlage geschaffen werden, die Grundrechtseingriffe zu rechtfertigen vermag, die mit den Maßnahmen im Strafverfahren einhergehen (von Ermittlungsmaßnahmen bis hin zur Freiheitsstrafe bei einer Verurteilung).

Wie gelingt es in einem Strafverfahren die materielle Wahrheit zu erforschen? Die wichtigsten Vorschriften in diesem Zusammenhang sind § 244 Abs. 2 StPO und § 261 StPO. Der Amtsermittlungsgrundsatz ist dabei notwendiges Gegenstück zu den Kriterien der Beweiswürdigung, die nur auf der Grundlage einer umfassenden Aufklärung möglich ist.[133]

1. Der Wahrheitsbegriff

Eingang findet der Wahrheitsbegriff in das Strafverfahren und damit in die rechtswissenschaftlichen Diskussionen nicht zuletzt über das Gesetz[134]: So stellt § 244 Abs. 2 StPO mit der Verpflichtung des Gerichts „zur Erforschung der Wahrheit" einen Bezug zu erkenntnistheoretischen Fragestellungen her. Was diese Verpflichtung bedeutet und wie weit sie reicht (siehe dazu gleich in 2.), hängt zunächst einmal davon ab, was unter Wahrheit zu verstehen ist und wie man sie erkennen kann. Auch das Verhältnis der Pflicht zur Wahrheits-

---

130 *Eisenberg*, Beweisrecht der StPO, Rn. 1. Nach *Seel*, Wahrheit im Strafprozess, S. 106 gilt die Erforschung der „materiellen Wahrheit" als „uneingeschränkt anerkannter oberster Grundsatz des Strafverfahrens" – sowohl in Gesetzgebung als auch in Rechtsprechung ab der Phase des Dritten Reichs (davor war es kein allgemein anerkanntes Ziel des Strafprozesses).

131 BVerfG, Urt. v. 19.3.2013 – 2 BvR 2628/10 -, Rn. 1 – 132.

132 *Eisenberg*, Beweisrecht der StPO, Rn. 1; *Kotsoglou*, Forensische Erkenntnistheorie, S. 21.

133 *Eisenberg*, Beweisrecht der StPO; Rn. 2.

134 Auch an anderen Stellen spielt der Wahrheitsbegriff in strafverfahrensrechtlichen Vorschriften eine Rolle. So z. B. in § 66c Abs. 1, 2 StPO, § 38 Abs. 1 DRiG oder §§ 81c Abs. 2 S. 1, 244 Abs. 5 S. 1 StPO. Mehr dazu siehe auch *Stamp*, Die Wahrheit im Strafverfahren, S. 15 f.

erforschung zum Überzeugungsmaßstab des § 261 StPO ist nur dann aufzuklären, wenn man sich zuvor Gedanken über den Wahrheitsbegriff als solchen macht.

So beschäftigt der Wahrheitsbegriff den Strafrechtsdogmatiker, den Rechtstheoretiker und auch die Öffentlichkeit nachhaltig; letztere v. a. dann, wenn Prozesse geführt werden über Geschehnisse, die die Menschen eng berühren, sie aufregen oder ängstigen. Kann die Strafjustiz, so lautet die Frage dann, einen Beitrag leisten zur historischen Aufklärung des Geschehens?[135] Als verlässliches Bild eines Geschehens taugen die Feststellungen der Strafjustiz jedenfalls nicht. Dazu sind sie, um das Wenigste zu sagen, zu selektiv. Ihre Aufklärung folgt einem ganz anderen Drehbuch als die Forschung der Geschichtsschreibung. Die Sonde der Strafjustiz richtet sich nicht auf „das" Geschehen (wenn es das denn überhaupt geben sollte), sondern auf „Sachverhaltsmerkmale": auf diejenigen Partikel des Geschehens, welche den Tatbestandsmerkmalen der strafrechtlichen Tatbestände entsprechen. Der Strafrichter hat, anders als der Historiker und wieder anders als etwa der Klimaforscher, einen allgemeinen Zusammenhang nur ungefähr im Blick, gewissermaßen als Hintergrund oder Umgebung. Unmittelbar vor Augen hat er Einzelheiten, deren Relevanz durch diejenigen Suchprogramme festgelegt wird, die das materielle Strafrecht ihm liefert: Wegnahme, Gewalt, Vermögensschaden. Weil das so ist, sprechen Strafjuristinnen statt von „materieller" lieber von „forensischer" oder „prozessualer" Wahrheit[136] und bringen damit zum Ausdruck, dass die im Strafprozess zutage geförderte Wahrheit relativ ist zu den Suchprogrammen und zu den Grenzen, welche das materielle Strafrecht und das strafprozessuale Verfassungsrecht der Wahrheitssuche im Strafprozess vorgeben. Weiter sind auch die Realbedingungen eines Gerichtsverfahrens zu berücksichtigen mit seinen zeitlichen, örtlichen und wirtschaftlichen Begrenzungen, mit sich streitenden Prozessrollen, nachlassendem Erinnerungsvermögen von Zeugen, nicht eindeutigen Befunden, rechtsstaatlich beschränkten Beweismöglichkeiten und der Unvollkommenheit menschlichen Urteilens. Die genügende Sicherheit über die Erwiesenheit einer Tatsache kann daher nur annäherungsweise erzielt werden.

Wie komplex diese Thematik ist, zeigt die umfassende philosophische Diskussion zu den Wahrheitstheorien, die seit über 2.500 Jahren noch kein Ende

---

135 Beispiele in der Bundesrepublik sind etwa der Auschwitz-Prozess in Frankfurt am Main, der seinen Blick auf die tatsächlichen Umstände dieses Lagers weit schweifen ließ, die Verfahren gegen die „Mauerschützen" und ihre Befehlshaber nach dem Ende der DDR, der NSU-Prozess, aber auch von den Medien breit und eindrücklich berichtete Ermittlungen bspw. in Verfahren wegen Mordes oder gegen „Kinderschänder".

136 Meyer-Goßner/*Schmitt*, § 261 Rn. 1 ff. m. w. N.

gefunden hat.[137] Es handelt sich bei den verschiedenen Theorien[138] oft nicht um einander strikt ausschließende Ansätze, sondern lediglich um die Fokussierung auf unterschiedliche Teilaspekte der Wahrheitsproblematik.[139] Die Frage ist, ob „Wahrheit" eine Universalie ist, die objektiv und allgemeingültig ist bzw. sein kann; oder, ob sie tradiert ist; oder, ob sie stets von der Vernunft bestimmt ist; oder, ob sie demokratisch verifiziert werden kann?

Die Rspr. selbst nimmt (bisher) mit der Pflicht zur Erforschung der („materiellen") Wahrheit kaum auf einen bestimmten erkenntnistheoretischen Maßstab bzw. einen einheitlichen Wahrheitsbegriff Bezug, sondern gebraucht diese Pflicht v. a. als flexibel einsetzbaren Argumentationstopos. Man stößt sowohl auf korrespondenztheoretische[140] Spuren und ein rein objektives Verständnis von Wahrheit, als auch einen weit verbreiteten rein subjektiven Wahrheitsbegriff (der bis auf die reichsgerichtliche Entscheidung RGSt 66, 163, 164 zurückgeht) und einen Wahrscheinlichkeitsmaßstab. Auffällig ist auch, dass Fragen der strafprozessualen Wahrheit nicht (schwerpunktmäßig) im Rahmen des § 244 Abs. 2 StPO diskutiert werden, wo der Wahrheitsbegriff im Gesetz enthalten ist, sondern im Rahmen der freien richterlichen Überzeugung nach § 261 StPO.[141] Die Rspr. der obersten Gerichte (RG und BGH) bestimmt die Anforderungen, wenn der Inhalt der Beweiswürdigung nach § 261 StPO Gegenstand der Entscheidung ist.[142] Gleiches gilt für die Literatur.[143]

In der Rspr. des BGH können einerseits Anklänge an die Korrespondenztheorie und ein rein objektives Wahrheitsverständnis gefunden werden. Mit Formulierungen wie der Richter müsse „die Beweismittel erschöpfen, wenn auch nur die entfernte Möglichkeit einer Änderung der durch die vollzogene

---

137 Zuletzt dazu siehe die anspruchsvolle, scharfsinnige und detaillierte Auseinandersetzung zu den Wahrheitstheorien in *Seel*, Wahrheit im Strafprozess.

138 Hier einige im Überblick: Korrespondenz- und Konsenstheorie, kohärenztheoretische und deflationistische Ansätze, pragmatische Wahrheitstheorien, deflationistische Wahrheitstheorien.

139 *Neumann*, JZ 1/2022, S. 32. Ihm folgend sollte sich eine umfassende Theorie zur „Wahrheit im Strafprozess" deutlicher an den spezifischen Problemen eines strafprozessualen Wahrheitsbegriffs und der strafprozessualen Wahrheitsermittlung orientieren.

140 Im Kern beruht der korrespondenztheoretische Wahrheitsbegriff auf einer Relation von menschlichen Urteilen, Aussagen etc. einerseits und Objekten oder Sachverhalten andererseits. Sie stellt eine möglichst weitgehende Übereinstimmung mit dem historischen Geschehen in den Vordergrund (im Gegensatz zur Konsenstheorie), vgl. dazu vertiefend *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 69 ff.

141 *Stamp*, Die Wahrheit im Strafverfahren, S. 157.

142 Aktuellste Übersicht bei *Seel*, Wahrheit im Strafprozess, S. 119 ff.

143 Meyer-Goßner/*Schmitt*, § 261 Rn. 1 m. w. N.

Beweisaufnahme begründeten Vorstellung von dem zu beurteilenden Sachverhalt in Betracht kommt“[144] könnte man Wahrheit korrespondenztheoretisch als Annäherung von Vorstellung und Sachverhalt verstehen. Die Wortwahl in anderen Entscheidungen – Der Richter müsse nunmehr einen bereits bestehenden „wahren Sachverhalt“ ermitteln[145] – legt wiederum ein rein objektives Verständnis von Wahrheit nahe. Mit einem korrespondenztheoretischen Wahrheitskern lässt sich diese Objektivierung kaum vereinbaren. Andererseits haben zahlreiche andere Entscheidungen des BGH die Überzeugung des Tatrichters zum Bezugspunkt, und damit ein subjektives Wahrheitsverständnis.[146] Die ersten Entscheidungen des BGH zum im Strafverfahren geltenden Maßstab führen die bis auf Boehmer und Beccaria zurückgehende Rspr. des RG[147] zum Überzeugungsmaßstab fort bzw. ergänzten diese[148] und verschoben den Maßstab immer weiter in den subjektiven Bereich.[149] Wahrheitserforschung und Überzeugungsbildung konnten kaum mehr auseinandergehalten werden.[150] Schließlich wurde die richterliche Überzeugung als alleiniger Maßstab

144 Vgl. nur BGHSt 23, 176, 187 f.; 30, 131, 142 f.

145 BGHSt 23, 8, 12; BGH NStZ 2016, 489.

146 Vgl. nur BGHSt 36, 159, 164 ff.; BGH NStZ 1983, 210; 2017, 96, 97.

147 Seit jeher hat die Rspr. anerkannt, „dass die richterliche Überzeugung keine mathematische, jede Möglichkeit des Gegenteils ausschließende Gewißheit voraussetzen darf“, vgl. RGSt. 51, 127; 61, 202, 206 (etablierte ein Wahrscheinlichkeitskriterium); 66, 164 (trat dem Wahrscheinlichkeitskriterium entgegen und stellte einen rein subjektiven Wahrheitsbegriff auf); RGZ 15, 339; 95, 249; 162, 229 f.

148 BGH NJW 1951, 83: „Angesichts der durchgängigen Mehrheit dieser Sachverhalte und der beschränkten Mittel menschlichen Erkennens ist ein absolut sicheres Wissen über sie kaum je erlangbar und die abstrakte Möglichkeit des Irrtums so gut wie immer vorhanden. So wenig aber der Mensch überhaupt sich durch diese abstrakte Irrtumsmöglichkeit vom praktischen Handeln abhalten lassen kann, wenn er nicht untergehen will, so wenig darf sich auch der Richter, wenn nicht die Gerechtigkeit Schaden leiden soll, auf die Unmöglichkeit einer absoluten Wahrheitserkenntnis zurückziehen.“; BGH NJW 1951, 122: „Sie beruht, der Eigenart geisteswissenschaftlichen Erkennens gemäß, anders als das Ergebnis exakter, naturwissenschaftlicher Forschung nicht auf einem unmittelbar einsichtigen Denken, sondern auf dem Gewicht eines die Gründe klar abwägenden Urteils über den Gesamtzusammenhang eines Geschehens. Für sie ist es erforderlich, aber auch genügend, dass ein nach der Lebenserfahrung ausreichendes Maß an Sicherheit besteht, dem gegenüber vernünftige Zweifel nicht mehr laut werden können.“

149 BGH NJW 1953, 283: Der Richter verletze seine Aufklärungspflicht nicht, wenn er bereits die feste Überzeugung vom Vorliegen oder Nichtvorliegen einer Tatsache gewonnen habe. BGH NJW 1951, 325: Lehnte jegliches Beweismaß außerhalb der richterlichen Überzeugungsbildung und sah als einzige Grenze eine „denkgesetzlich unmögliche Grundlage“ an. BGH GA 1954, 152, 153: „Für die Verurteilung ist notwendig, aber auch genügend, dass der Sachverhalt für den Tatrichter zweifelsfrei feststeht; diese persönliche Gewissheit ist allein entscheidend.“

150 *Seel*, Wahrheit im Strafprozess, S. 119 f.

erklärt.[151] Bis heute folgen Entscheidungen diesem Maßstab.[152] Dabei kombinieren einige den subjektivistischen Ansatz mit Angriffen auf den Wahrscheinlichkeitsmaßstab.[153] Der streng subjektive Maßstab führt schließlich dazu, dass sogar lebensfremde[154] oder angesichts der Beweislage eher unwahrscheinliche[155] Annahmen des Tatgerichts unbeanstandet bleiben.[156] Es wird deutlich, dass wohl immer ein Restzweifel bleibt – ob es die Unmöglichkeit einer hundertprozentigen Wahrheit oder die eines hundertprozentigen Ausschlusses ist. Diese gilt es dann, im Rahmen der Würdigung nach § 261 StPO zu beurteilen (dazu im 4. Teil).

In der verfassungsgerichtlichen Rspr. überwiegt ein rein objektives Wahrheitsverständnis. Die erkenntnistheoretischen Gesichtspunkte sind aber deutlich unergiebiger als die des BGH. Wiederholt ist vom öffentlichen Interesse „an einer möglichst vollständigen Wahrheitsermittlung im Strafprozess" die Rede.[157] Viele Entscheidungen betonen, für den Strafprozess sei die „Ermittlung des wahren Sachverhalts" zentral.[158] Die Wortwahl impliziert, dass Wahrheit als eine von vornherein feststehende, nurmehr aufzufindende oder eben zu ermittelnde Eigenschaft von Sachverhalten selbst anzusehen ist. In

---

151 BGH NJW 1957, 1039: „Freie Beweiswürdigung bedeutet, daß es für die Beantwortung der Schuldfrage allein darauf ankommt, ob der Tatrichter die Überzeugung von einem bestimmten Sachverhalt erlangt hat oder nicht; diese persönliche Gewißheit ist für die Verurteilung notwendig, aber auch genügend. Der Begriff der Überzeugung schließt die Möglichkeit eines anderen, auch gegenteiligen Sachverhaltes nicht aus; vielmehr gehört es gerade zu ihrem Wesen, daß sie sehr häufig dem objektiv möglichen Zweifel ausgesetzt bleibt. Denn im Bereich der vom Tatrichter zu würdigenden Tatsachen ist der menschlichen Erkenntnis bei ihrer Unvollkommenkeit ein absolut sicheres Wissen über den Tathergang, demgegenüber andere Möglichkeiten seines Ablaufs unter allen Umständen ausscheiden müßten, verschlossen."

152 Vgl. nur BGHSt 25, 365, 367; 26, 56, 63; 29, 18, 20; BGH NStZ 1983, 277, 278; 2004, 35; 2013, 180; 2015, 343; BGH NStZ-RR 2013, 75, 77; 89, 90; 2015, 148; 2016, 54 f.; 117; 222; 2017, 318, 319; BGH StV 2005, 19.

153 BGH bei Dallinger MDR 1969, 154: „Aus der Summe mehrerer Wahrscheinlichkeiten und Möglichkeiten, also aus lauter Zweifeln, darf nicht eine Gewissheit konstruiert werden"; in BGHSt 36, 386, 390 heißt es bspw. „dass aus bloßen Möglichkeiten oder Wahrscheinlichkeiten keine Gewissheit begründet werden kann."

154 BGH NStZ 1984, 180; 2004, 35; BGH NStZ-RR 2003, 371; 2005, 147; 2006, 4 Nr. 13; 2007, 86; 2011, 50.

155 BGH NStZ 2015, 714, 715; 2017, 104 f.; BGH NStZ-RR 2013, 75, 77; 89, 90; 2015, 178; 2016, 47 ff.; 54 f.; 2017, 303, 304. Hier finden sich Aussagen wie: Die tatrichterliche Überzeugungsbildung sei „sogar dann hinzunehmen, wenn eine abweichende Würdigung der Beweise näherliegend gewesen wäre."

156 *Seel*, Wahrheit im Strafprozess, S. 122.

157 BVerfGE 33, 367, 383; 34, 238, 248 f.; 36, 173, 186; 77, 65, 76; 80, 367, 375; 122, 248, 273; 130, 1, 26 f.

158 BVerfGE 57, 250, 275; 63, 45, 61; 118, 212, 231; 122, 248, 270; 130, 1, 26; 133, 168, 199.

Übereinstimmung hiermit sieht das BVerfG die Erforschung der Wahrheit unter der StPO durch ein ausgeprägtes inquisitorisches Modell gesichert, in dem die Vorsitzende eine starke Stellung einnimmt und die Staatsanwaltschaft nicht als Partei zu verorten ist, sondern objektiv auf die Wahrheitsfindung hinarbeitet; die Mitwirkungsrechte des Beschuldigten haben demgegenüber nur eine die Wahrheitsermittlung unterstützende Funktion.[159] Man findet allerdings auch Spuren eines subjektiven Wahrheitsverständnisses. V. a. die ältere Rspr. verbindet gelegentlich das Interesse an möglichst vollständiger Wahrheitsermittlung unmittelbar mit der richterlichen Überzeugungsbildung.[160] Auch hat sich das BVerfG mit dem Wahrscheinlichkeitsmaßstab des zweiten Strafsenats auseinandergesetzt. Dabei hat es aus Art. 2 Abs. 2 S. 2 GG i. V. m. dem Rechtsstaatsprinzip Anforderungen an die Aufklärungspflicht und Beweiswürdigung abgeleitet.[161] Beide Prinzipien stünden „in vielfacher Verschränkung“: § 244 Abs. 2 StPO ziele auf die vollständige Erhebung aller bekannten Beweismittel, § 261 StPO auf die vollständige Beweiswürdigung als Urteilsgrundlage.[162] Gleichwohl hat sie den Wahrscheinlichkeitsmaßstab akzeptiert, als sie von der verfassungsrechtlichen Verpflichtung des Tatrichters spricht „in Wahrung der Unschuldsvermutung […] auch die Gründe, die gegen die mögliche Täterschaft sprechen, wahrzunehmen, aufzuklären und zu erwägen“ und dann einzuschreiten, wenn der rationale Charakter der Entscheidung verloren gegangen scheint und sie keine tragfähige Grundlage mehr für die mit einem Schuldspruch einhergehende Freiheitsentziehung sein kann.“[163]

Die Strafrechtswissenschaft ist in großen Teilen den Formeln der Rspr. gefolgt.[164] Von den wichtigsten philosophischen Wahrheitstheorien hat sie v. a.[165] die Korrespondenz-[166] und Konsensustheorie[167] aufgegriffen, Mischformen[168] etabliert oder Ansätze formuliert, die sich entweder an den Verfah-

159 Vgl. BVerfGE 57, 250, 279 f.; 63, 45, 63; BVerfG NStZ 1987, 419; BVerfG StV 1997, 1, 2.

160 Vgl. BVerfGE 36, 173, 186; 74, 358, 372 f.; 86, 288, 318; 133, 168, 204, 207; vgl. auch BVerfGE 64, 135, 148.

161 BVerfG NJW 2003, 2444, 2445 f.

162 BVerfG NJW 2003, 2444, 2445.

163 BVerfG NJW 2003, 2444, 2446.

164 *Seel*, Wahrheit im Strafprozess, S. 128 f.

165 Andere Theorien haben in der Diskussion, wenn, dann nur eine sehr geringe Bedeutung erlangt; vgl. *Seel*, Wahrheit im Strafprozess, S. 139 f. sowohl zum semantischen Wahrheitsbegriff, als auch zur Kohärenz-, deflationistischen und pragmatischen (Wahrheits-)Theorie.

166 *Seel*, Wahrheit im Strafprozess, S. 131 f.

167 *Seel*, Wahrheit im Strafprozess, S. 135 f.

168 *Seel*, Wahrheit im Strafprozess, S. 142 f.

renszielen des Strafprozesses orientieren oder sich auf Erkenntnisse aus Soziologie, Psychologie, Anthropologie, Linguistik oder Kommunikationswissenschaften stützen.[169] Zuletzt hat sich ausführlich Seel[170] mit einer wissenschaftlichen Aufarbeitung des Wahrheitsbegriffs im Strafverfahren beschäftigt. Er erteilt der Korrespondenz- und Konsenstheorie eine Absage und schätzt die kohärenztheoretischen und deflationistischen Ansätze eher skeptisch ein. Vielmehr bekennt er sich zu den pragmatischen Wahrheitstheorien. Ihm folgend sind diese nicht nur philosophisch überzeugend, sondern auch für „das Verständnis von Wahrheit im Strafprozess außerordentlich fruchtbar".[171] Insbesondere kann ein pragmatisches Konzept von Wahrheit „das Verhältnis der im Strafprozess zentralen Begriffe Wahrheit, Überzeugung und Untersuchung schlüssig erklären".[172] Danach wird Wahrheit – anders als im Modell einer materiellen bzw. objektiven Wahrheit – nicht schlicht gefunden, sondern im Wege der Beweisaufnahme hergestellt. Dass Wahrheit ein Produkt dieses Herstellungsprozesses ist, bedeutet einerseits, dass für die richterliche Überzeugung (§ 261 StPO) „keine subjektive, sondern nur eine in der Untersuchung validierte Überzeugung" genüge.[173] Andererseits ist diese Wahrheit insofern eine relative und vorläufige Wahrheit, als eine erneute Untersuchung zu anderen Ergebnissen führen kann.[174]

Hinzu tritt dieser Diskussion bzgl. der Wahrheitssuche mithilfe digitaler Spuren, dass Propheten der Digitalisierung eine Revolutionierung des Erkenntnisgewinns mithilfe der theoriebasierten Suche nach Kausalitäten in Richtung der theorielosen Korrelationsanalyse mutmaßen. Die schnelle und effiziente Auswertung nie dagewesener Datenmengen und -arten führt dazu, dass herkömmliche Annahmen und Praktiken anhand aufgedeckter Korrelationen hinterfragt und neu bewertet werden müssen.[175] Das bedeutet gleichzeitig, dass den bisherigen Annahmen und Praktiken mehr misstraut werden muss. Das liegt v. a. darin begründet, dass die Softwaresysteme, die als Sachverständigenwerkzeug zum Einsatz kommen, teilweise so kompliziert und vernetzt sind, dass selbst die Anwenderinnen sie nicht bis ins Letzte begreifen. Die Digitalisierung verheißt also einerseits umfassenderes und nicht theorie-

169 *Seel*, Wahrheit im Strafprozess, S. 143 f.

170 *Seel*, Wahrheit im Strafprozess, S. 23 f.

171 *Seel*, Wahrheit im Strafprozess, S. 367.

172 *Seel*, Wahrheit im Strafprozess, S. 395.

173 *Seel*, Wahrheit im Strafprozess, S. 395.

174 Unter Achtung der Rechtsfriedensfunktion mit Rechtskraft des Urteils abgeschlossen.

175 *Mayer-Schönberger/Cukier*, Big Data, S. 93: „Tatsächlich bietet Big Data vielleicht gerade deswegen eine neue Sicht der Dinge und neue Erkenntnisse, weil es nicht von der konventionellen Denkweise und den inhärenten Vorurteilen der Theorien eines spezifischen Fachgebiets belastet ist."

gebundenes Wissen, kostet aber andererseits das Verständnis, wie dieses Wissen entsteht.[176] Dieses verborgen entstandene Wissen stellt v. a. für die Rechtsprechung und ihre Tatsachenermittlung eine enorme Herausforderung dar: Tatrichterinnen dürfen sich diesen „objektiven" Erkenntnissen über die „Wirklichkeit" zwar nicht verschließen und sind gehalten, sich ihre Überzeugung über den zu entscheidenden Sachverhalt möglichst ohne jede Art von Vorurteilen zu bilden. Jedoch ist ein Wissen, das ohne erkennbare kausale Begründung und daher auch ohne direkt verständliche Nachvollziehbarkeit zustandekommt, eine bestenfalls ungewohnte, schlimmstenfalls zweifelsbeladene Grundlage für rechtsstaatliche Entscheidungen.[177] Das gilt sowohl für die zur Entscheidung berufenen Tatrichterinnen selbst, als auch für den durch die gerichtliche Entscheidung belasteten Einzelnen. Dieser erwartet vom Rechtsstaat zu Recht, dass er eine für ihn nachvollziehbare, auf zutreffenden Tatsachenannahmen basierende Entscheidung erhält. Verlagert das Tatgericht die Tatsachenermittlung aber auf einen IT-Sachverständigen, bei dessen Analyse nicht nachvollziehbare Methodiken zur Anwendung kommen, indem es deren Ergebnisse ohne Prüfung für „bare Münze" nimmt, wird diese Erwartung an den Rechtsstaat enttäuscht. Die Entscheidung verlagert sich wieder in ein Mysterium – diesmal das der Daten und Algorithmen.[178]

Was in einem Strafverfahren als „Wahrheit" gelten darf, hängt wohl von der Betrachtungsweise und Methodologie der Betrachtung ab.[179] Gesichert ist jedenfalls, dass jenes tatsächliche Stück der analogen und digitalen Welt, auf das sich eine Verurteilung stützen muss, sowohl empirisch wahr als auch nach den jeweils geltenden Standards der empirischen Wissenschaften aufgeklärt ist. Das wiederum hat die Richterin zu verantworten, eigenständig nachzuvollziehen und für alle Verfahrensbeteiligten transparent zu machen (siehe dazu später im 4. Teil). „Mehr" lässt sich wohl auf dem Gebiet der prozessualen Wahrheit prinzipiell nicht erreichen.[180]

---

176 *Mysegades*, Software als Beweiswerkzeug, S. 1 f. m. w. N.

177 *Mysegades*, Software als Beweiswerkzeug, S. 2 f. Vertiefter zu Einflüssen von Legal-Tech-Anwendungen und digitalen Beweismitteln auf die freie Beweiswürdigung siehe auch bei *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 393 ff.

178 *Mysegades*, Software als Beweiswerkzeug, S. 3.

179 *Hassemer*, Grundlagen des Strafrechts, S. 839. Vgl auch interessant *Ewald*, in: Smeulers/Haveman (Hrsg.), Supranational Criminology, S. 399 ff.: Das Erkenntnisverfahren als analytischer Informationsverarbeitungsprozess, der strafprozessual abgebildet werden muss.

180 So auch *Hassemer*, Grundlagen des Strafrechts, S. 839 f.

2. Der Umfang der Wahrheitserforschung i. S. d. § 244 Abs. 2 StPO

Die Aufklärung des Sachverhalts[181] bzw. die „Suche nach der materiellen Wahrheit“[182] im Wege der Beweisaufnahme ist dabei originäre Aufgabe des Tatgerichts, § 244 Abs. 2 StPO,[183] d. h. das Gericht muss selbst den gesamten verfahrensrelevanten Tatsachenstoff ermitteln. Die Pflicht zur vollständigen und erschöpfenden Wahrheitsermittlung bedeutet, dass das Gericht vom Vorliegen sämtlicher entscheidungserheblicher Tatsachen überzeugt sein muss und zu diesem Zweck Beweismittel zur Bildung bzw. Überprüfung einer Überzeugung heranziehen muss.[184]

So muss das Tatgericht selbst tätig werden, wenn in Daten enthaltene Informationen im Wege eines „einfachen“ Augenscheins- oder Urkundenbeweises in die Hauptverhandlung eingeführt und gewürdigt werden sollen, wenn davon auszugehen ist, dass sich aus den bei dieser Art der Beweismitteleinführung verloren gehenden (bspw. Meta-)Daten weitere verfahrensrelevante Informationen ergeben würden. Das Tatgericht darf sich v. a. nicht auf die Unterstützung der Verfahrensbeteiligten durch Beweisanträge zurückziehen.

Im Ergebnis hängt die Frage, ob das Gericht einen IT-Sachverständigen mit der Auswertung der Daten beauftragen muss oder ob die Einbringung der in den Daten enthaltenen (Teil-)Informationen im Wege des Urkunden- oder Augenscheinsbeweises genügt (siehe oben A. IV.), von den Umständen des Einzelfalles ab.[185] Eine pauschale Festlegung, wann das zur Erforschung der materiellen Wahrheit erforderliche Tatsachenmaterial vollständig ist, ist nicht möglich.[186] Das Tatgericht muss das unter Berücksichtigung seiner Amtsaufklärungspflicht, den Prinzipien der vollständigen und erschöpfenden Beweiswürdigung sowie der Pflicht zur Verwendung des bestmöglichen und sachnächsten Beweismittels im konkreten Fall entscheiden. Dabei kommt es v. a. darauf an, ob die durch ein IT-Sachverständigengutachten zu erwartenden zusätzlichen Informationen (wie die zu erwartenden (Meta-)Informationen und der (wahrscheinliche) Ausschluss einer Manipulation) – unter Beachtung des

---

181 Auch Kognitionspflicht, Untersuchungsgrundsatz oder Instruktions- bzw. Inquisitionsgrundsatz bezeichnet.

182 *Kudlich/Nicolai*, JA 2020, 881 (886); vgl. nur aus der Rspr. des BVerfG zur Pflicht zur Suche nach der Wahrheit im Strafverfahren: BVerfGE 57, 250 (275); 118, 212 (231); 122, 249 (270); 130, 1 (26); 133, 168 (199 und 226) sowie *Landau*, NStZ 2015, 665 (669).

183 Löwe/Rosenberg/*Becker*, § 244 Rn. 50 f.

184 *Eisenberg*, Beweisrecht der StPO, Rn. 11; vgl. zum Amtsermittlungsgrundsatz auch *Mysegades*, Software als Beweiswerkzeug, S. 71 ff.

185 So auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 660 f.

186 Zur Grenze der Wahrheitserforschung siehe vertiefend *Stamp*, Die Wahrheit im Strafverfahren, S. 50 ff.

(beschränkten) „Verbots der Beweisantizipation“[187] – auch durch andere Beweismittel[188] oder eine glaubhafte Einlassung des Beschuldigten[189] gewonnen werden können und somit die Einholung des Gutachtens überflüssig ist.[190] Hinsichtlich des Nichtvorhandenseins bzw. der Nichtwiederherstellbarkeit versteckter oder gelöschter Daten wird es wohl selten alternative Beweismittel geben, welche hierüber Auskunft geben können. Insbesondere ist es schwierig, einer entsprechenden Einlassung des Angeklagten, dass es solche Dateien nicht gäbe, Glauben zu schenken. Gerade (vermeintlich) gelöschte Dateien lassen sich bei Datenträgern häufig wiederherstellen.[191] Hier wird es v. a. auf die Verfahrensrelevanz der potentiell wiederherstellbaren Daten ankommen, was im Einzelfall beurteilt werden muss: Geht es bspw. um den Beweis der Existenz (bzw. der Nichtexistenz) bestimmter Daten oder Spuren auf einem Datenträger (wie der Besitz von Kinderpornografie auf einer Festplatte), ist die Verfahrensrelevanz versteckter oder gelöschter, aber wiederherstellbarer Dateien äußerst naheliegend. Beschränkt sich das Beweismittel dagegen sowieso von vornherein nur auf einen Teil der Daten eines Geräts (wie eine E-Mail-Konversation, die den Vorsatz nach §§ 15, 16 StGB belegen soll) drängt sich die Verfahrensrelevanz „irgendwelcher“ gelöschter Daten nicht auf.[192]

Ganz allgemein ergibt sich als Untergrenze der Wahrheitserforschungspflicht, dass das Gericht zumindest diejenigen Tatsachen ermitteln muss, welche die Grundlage der Entscheidung bilden.[193] Tatsachen sind alle für den Prozess subsumtionsrelevanten Umstände, also „(…) etwas Geschehenes oder Bestehendes, das zur Erscheinung gelangt und in die Wirklichkeit und das daher dem Beweis zugänglich ist.“[194] Entscheidend für das Vorliegen einer Tatsache ist ihre grundsätzliche Nachprüfbarkeit, ohne dass es auf eine konkrete Möglichkeit des Beweises ankommt.[195] Relevant meint dabei, dass die

---

187 Danach darf ein sicheres Urteil darüber, welchen Wert ein vom Antragsteller vorgeschlagenes Beweismittel hat, regelmäßig erst nach der Beweisaufnahme möglich sein; dazu vertiefend auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 309.

188 Vgl. *Jahn/Brodowski*, in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 67 (89).

189 Wie hier *Jahn/Brodowski*, in: FS Rengier, S. 409 (412 f.).

190 Vgl. auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 664.

191 Vgl. allgemein dazu etwa *Povar/Bhadran*, ICDF2C 2010; S. 137 ff.

192 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 663.

193 Löwe/Rosenberg/*Becker*, § 244 Rn. 39 f.

194 Vgl. RGSt 55, 130, 131; *Stinshoff*, Operative Fallanalyse, S. 79; in Ausführlichkeit zum „Tatsachenbegriff“ und der Nähe zum „Wahrheitsbegriff“ siehe *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 63 ff.

195 Vgl. BVerfGE 90, 241, 247; 94, 1, 8; BVerfG NJW 2008, 358, 359; BGHZ 3, 270, 273 f.; 45, 296, 304; 139, 95, 102; dazu auch EGMR NJW 2006, 1645, 1648 f. [Rz. 76]; Meyer-Goßner/*Schmitt*, Vor § 48 Rn. 2; Jarass/Pieroth-*Jarass*, Art. 5 Rn. 5.

Wahrscheinlichkeit[196] einer für den Ausgang des Verfahrens bedeutsamen Tatsache gemindert (negative Relevanz) oder erhöht (positive Relevanz) wird. Die relevanten Tatsachen werden in der Urteilsbegründung in einer syllogistischen Struktur dargestellt.[197]

Den (groben[198]) Filter über die erheblichen[199] Tatsachen bilden die in der Anklageschrift bezeichnete Tat, die abgeurteilt werden soll (prozessuale Tat i. S. d. §§ 155 Abs. 1, 264 Abs. 1 StPO)[200] und die einschlägige Sanktionsnorm.[201] Innerhalb dieses vorgegebenen Rahmens ist die materielle Wahrheit vollständig und bestmöglich zu erforschen,[202] zumal das Gericht im gleichen Umfang zu einer Erkenntnis verpflichtet ist (Kognitionspflicht, § 264 Abs. 1 StPO).[203]

Hierzu gehören auch die sog. Beweisthemen des Sachverständigenbeweises. Das Beweisthema des Sachverständigen ist eine Tatsachenbehauptung,

---

196 Gemeint ist eine Hypothesenwahrscheinlichkeit.

197 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 104. Siehe dazu später im Viertel Teil, A. III. 5.

198 Der in der Anklage bezeichnete Sachverhalt und die Kognitionspflicht des Gerichts müssen sich nicht decken, vgl. vertiefend dazu BGHSt 13, 21 (25); 23, 141 (145); 32, 146 (149); 32, 215 (221).

199 Für die Entscheidung *erheblich* sind alle (äußeren und inneren) Tatsachen, die den Schuld- und Rechtsfolgenausspruch beeinflussen können, vgl. *Eisenberg*, Beweisrecht der StPO, Rn. 6; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 117.

200 Die prozessuale Tat wird durch den Sachverhalt bestimmt, der erforderlich ist, um zu identifizieren, welches Verhalten eine Sanktionsnorm hinsichtlich ihres Voraussetzungsteils erfüllt. Das sind sog. sachverhaltsbegründende Tatsachen, vgl. weiter dazu *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 117 ff.

201 Siehe vertiefend zum Beurteilungsspielraum des Gerichts und zur Begrenzung des „Tatbegriffs" *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 118 f.

202 Eine Einschränkung und Modifikation der Aufklärungspflicht bewirken die sog. Schätzklauseln namentlich in Vorschriften des materiellen Rechts. Die grundsätzliche Fortgeltung der Aufklärungspflicht verbietet jedoch bloße Mutmaßungen, vgl. *Eisenberg*, Beweisrecht der StPO, Rn. 33a. Zu beachten gilt stets der Zweifels-Grundsatz. Speziell im Steuerstrafrecht dürfen Richterinnen Schätzungen übernehmen (jedoch nur unter Berücksichtigung der vom Besteuerungsverfahren abweichenden Grundsätze des Strafverfahrens), vgl. BGH NStZ 07 589; *Gehm*, NZWiSt 12, 412 ff. (bei unterschiedlichen Schätzergebnissen der geringste Wert, ggf. Sicherheitsabschlag). Die Grundlagen der Schätzung müssen dann aber nachprüfbar mitgeteilt werden, vgl. BGH NStZ 10, 635; Bay StV 93, 529. Das ist v. a. im Hinblick auf Massendelikte wie die Verbreitung von Schadsoftware interessant, vgl. Kemptener Bitcoin-Fall (mehr dazu im 4. Teil). Hier ist die Anwendung einer Schätzklausel jedoch misslungen. Denn von dem eben genannten sind besondere Fallkonstellationen zu unterscheiden, bei denen eine Bestimmung des Schuldumfangs im Wege der Schätzung geschieht, soweit eine nähere Aufklärung unmöglich geworden ist (bspw. bei Serienhehlerei, vgl. BGH NStZ 95, 203 oder z. B. Zigarettenschmuggel, StV 00 600).

203 *Eisenberg*, Beweisrecht der StPO, Rn. 10.

die das Gericht mangels eigener Sachkunde nicht ohne den Sachverständigen zu beweisen vermag (siehe dazu in diesem Teil, B. II. 3. d)).

Die im Wege des § 244 Abs. 2 StPO gesammelten (beweisbedürftigen)[204] Tatsachen lassen sich unterteilen in Haupttatsachen, Indizien und Hilfstatsachen[205].[206] Auch die Beweisthemen des IT-Sachverständigenbeweises lassen sich diesen drei Kategorien zuordnen.

Zu den Haupttatsachen, gehören alle Umstände, die aus sich selbst heraus (also ohne weitere Beweiserhebung oder induktive Schlüsse) die Subsumtion unter einen Rechtssatz (gesetzliche Tatbestandsmerkmale[207], Rechtfertigungs- oder Schuldausschließungs-, Strafausschließungs- oder Strafaufhebungsgründe, Umstände aus § 46 StGB) ermöglichen.[208] Sie begründen also durch sich selbst die Strafbarkeit oder schließen diese aus. Zum Beispiel hat ein Zeuge den Täter bei der Tat beobachtet; oder er hat gesehen wie der Täter in Notwehr gehandelt hat. Man spricht auch von einem „direkten" Beweis.[209]

Beispiele in der forensischen Informatik können bspw. E-Mails und Chatverläufe sein, wenn sie als Beweismittel in Fällen von Betrug, Erpressung und Cyber-Mobbing dienen; Social-Media-Beiträge (Kommentare, Tweets und Facebook-Updates), bei Fällen von Cyberstalking und Hate Speech; oder Fotos und Videos in Fällen des Besitzes kinder- oder jugendpornografischen Materials, Stalking, Einbruch und Diebstahl.

Indizien hingegen sind Tatsachen, die einen Schluss auf eine unmittelbar beweiserhebliche Tatsache zulassen, wenn beispielsweise der Verdächtige das Opfer unmittelbar vor der Tat bedroht hat oder nach der Tat Spuren verwischt.

---

204 Nicht beweisbedürftig sind Tatsachen, wenn sie z. B. bereits erwiesen oder „offenkundig" sind, vgl. *Eisenberg*, Beweisrecht der StPO, Rn. 15.

205 Hilfstatsachen lassen einen Schluss auf die Güte eines Beweismittels zu. Das kann bspw. durch ein Gutachten zur Glaubwürdigkeit eines Zeugen bzw. zur Glaubhaftigkeit seiner Aussage geschehen, vgl. *Stamp*, Die Wahrheit im Strafverfahren, S. 104.

206 Siehe dazu auch *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 50 ff.

207 Beispielsfall: A schlägt B ins Gesicht; B blutet und hat Schmerzen. Das könnte eine „vorsätzliche Körperverletzung" sein: „Wer eine andere Person körperlich misshandelt oder an der Gesundheit schädigt, wird … bestraft" (§ 223 Abs. 1 StGB). A ist A und B ist B; mit der Feststellung „andere Person" dürfte man also wenig Schwierigkeiten haben. Bleiben noch drei Merkmale: Handlung des A (Schlagen), Erfolg bei B (Bluten, Schmerzen), Vorsatz (Wissen und Wollen des Erfolgs durch A); https://www.zeit.de/gesellschaft/zeitgeschehen/2015-09/strafprozess-beweis-indiz-fischer-im-recht [27.6.2023].

208 *Eisenberg*, Beweisrecht der StPO, Rn. 8; *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 562.

209 *Stamp*, Die Wahrheit im Strafverfahren, S. 104.

Insoweit liegt ein „indirekter" Beweis vor.[210] Indizien ermöglichen allein oder i. V. m. weiteren Zwischengliedern allenfalls den (positiven oder negativen) induktiven Schluss auf eine Haupttatsache.[211]

Im Bereich der forensischen Informatik werden digitale Spuren häufig als Indizien verwendet: So können Kommunikationsinhalte wie E-Mails und Nachrichten als Indiz für die Absichten oder Aktivitäten einer Person in strafrechtlichen Angelegenheiten dienen; Bilder von Überwachungskameras, Mobiltelefonen und anderen digitalen Geräten können dabei helfen, Täter zu identifizieren und Taten zu rekonstruieren; Standortdaten von Mobiltelefonen und GPS-Systemen können dafür verwendet werden, um die Positionen von Personen oder Objekten zu verfolgen und zu bestätigen; oder IP-Adressen sowie Zugriffsdaten, bspw. auf Online-Konten oder Websites, unterstützen dabei, einen Verdächtigen mit einer bestimmten Straftat in Verbindung zu bringen.

Die Begriffe und die Unterscheidung werden v. a. an späterer Stelle dieser Arbeit im Rahmen des Beweisthemas und der objektiven Tatsachengrundlage bzgl. § 261 StPO bei der Bestimmung der Nähe der Tatsachen zum Sachverhalt wichtig.

3. Die Rationalisierung des Wahrheitsfindungsprozesses

Die oben geschilderten verschiedenen Theorien zum strafprozessualen Wahrheitsbegriff – v. a. die stark subjektive Ausrichtung – und die subjektive Komponente der tatrichterlichen Überzeugung im Rahmen des § 261 StPO verdeutlichen die Gefahr der Willkürlichkeit.[212] Denn diese innere, subjektive Überzeugung von einem bestimmten Grad an Richtigkeitswahrscheinlichkeit der aufgestellten Hypothese hinsichtlich Tathergang und Tatbeteiligung[213] ist einer Überprüfung durch Dritte nicht zugänglich.[214]

---

210 *Stamp*, Die Wahrheit im Strafverfahren, S. 104.

211 Aus dem Beispiel von *Fischer*: Es findet sich bspw. eine Visitenkarte des A am Tatort, der aber eigentlich behauptet hat, woanders gewesen zu sein. Das ist gewiss keine „Haupttatsache", denn § 223 StGB setzt Visitenkarten nicht voraus. Aber es ist ein „Indiz". Diese sind also solche Umstände, die nach (vorerst unbekannten) Regeln der Plausibilität und der Logik die Schlussfolgerung zulassen (nicht: erzwingen!), eine Haupttatsache sei gegeben, vgl. https://www.zeit.de/gesellschaft/zeitgeschehen/2015-09/strafprozess-beweis-indiz-fischer-im-recht [27.6.2023].

212 So *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 362 f. in Bezug auf die Bejahung oder Verneinung des Tatverdachts bzw. des Erreichens einer bestimmten Tatverdachtsschwelle schon im Ermittlungsverfahren. Diese Grundsätze und Überlegungen können auch auf die Urteilsfindung übertragen werden, sieht man sie als die „höchste" der Verdachtsstufen.

213 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 362; in Bezug auf die tatrichterliche Überzeugung i. S. d. § 261 StPO muss man vom höchsten

Die Willkürlichkeit kann durch eine Rationalisierung des Wahrheitsfindungsprozesses minimiert werden. Dementsprechend kommt den einzelnen verobjektivierbaren Elementen im Rahmen der Wahrheitserforschung und Überzeugungsbildung zur Erhaltung eines rechtsstaatlichen Strafverfahrens[215] eine große Bedeutung zu und stellen die notwendige tragfähige Grundlage der subjektiven Überzeugung von der Richtigkeitswahrscheinlichkeit dar.[216]

So muss der Grad der persönlichen Gewissheit im Rahmen der tatrichterlichen Überzeugung – in anderen Worten: Wann ein Tatrichter von der Wahrheit des dargelegten Sachverhalts bzw. der Richtigkeitswahrscheinlichkeit der aufgestellten Hypothese überzeugt sein darf – auf einer objektiven Tatsachengrundlage aufbauen.[217] Weiter wird die objektive Stärke der tatrichterlichen Überzeugung von den Schlussfolgerungen, welche aus den vorhandenen Tatsachen gezogen werden, und der/den Hypothese(n), die aus den Schlussfolgerungen hinsichtlich Tathergang und Tatbeteiligung gewonnen werden sowie der objektiven Wahrscheinlichkeit der Richtigkeit dieser Hypothese bestimmt. Diese objektiven Elemente müssen so transparent und rational wie möglich ausgestaltet sein, um einer willkürlichen Bejahung oder Verneinung der tatrichterlichen Überzeugung zu begegnen.[218]

In Bezug auf den IT-Sachverständigenbeweis, der für die Richter und Staatsanwältinnen in Bezug auf ein bestimmtes Beweisthema die Tatsachenbehauptung für die Wahrheitsermittlung liefert, ergeben sich dabei Besonderheiten, die sowohl an den verschiedenen Aussagekategorien des Sachverständigenbeweises anknüpfen, aber auch im Besonderen durch die Eigenart der ihr zugrundeliegenden (automatisierten) Datenverarbeitungs- und -analysemethoden und Erfahrungssätze sowie der Beachtung der Standards der forensischen Informatik entstehen.[219] Auf diese soll im Laufe der Arbeit an den jeweiligen Stellen eingegangen werden.

Richtigkeitswahrscheinlichkeitsmaßstab ausgehen (im Vergleich zu den anderen Verdachtsgraden der StPO).

214 *Bach*, Jura 2007, 12 (14); *Pollähne*, Kriminalprognostik, S. 23 f.; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 371 in Bezug auf den Tatverdacht.

215 Sowohl im Ermittlungsverfahren bei der Sammlung des Tatsachenstoffes, als auch in der Hauptverhandlung bei der Beweisaufnahme und der abschließenden tatrichterlichen Überzeugungsbildung.

216 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 362 f. in Bezug auf den Tatverdacht; *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 108 ff.

217 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 536.

218 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 362 f. in Bezug auf den Tatverdacht.

219 Siehe dazu vertieft auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 371 f.

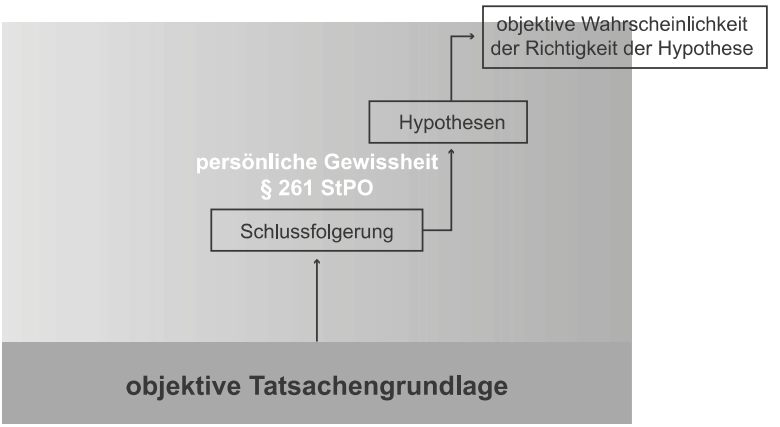


Abbildung 1: „Die objektive Stärke der tatrichterlichen Überzeugung i. S. d. § 261 StPO“

II. Der IT-Sachverständige im Strafverfahren

Im Folgenden soll untersucht werden, inwieweit die Vorschriften der StPO bei der forensischen Wahrheitssuche unter Zuhilfenahme des IT-Sachverständigenbeweises helfen können.

1. Der Begriff des „Sachverständigen“

Wie eingangs erwähnt, ist der Sachverständigenbegriff gesetzlich nicht definiert. Eine Definition des Begriffs wird daher aus den Aufgaben des Beweismittels sowie der Zweckbestimmung seiner Tätigkeit abgeleitet.[220]

Bei der Frage was man unter einem Sachverständigen zu verstehen hat, antwortet ChatGPT[221]: „Ein Sachverständiger ist eine Person, die über spezifisches Fachwissen oder Expertise auf einem bestimmten Gebiet verfügt und in der Lage ist, eine unabhängige und objektive Meinung zu einem Sachverhalt zu äußern. Sachverständige werden oft in rechtlichen oder technischen Angelegenheiten hinzugezogen, um Gutachten, Expertisen oder Bewertungen abzugeben. Sie müssen in der Regel eine formale Qualifikation auf ihrem jeweiligen Fachgebiet nachweisen.“

Wie durch die Antwort von ChatGPT deutlich wird, gibt es verschiedene Gegebenheiten, in denen Sachverständige tätig bzw. beauftragt werden. Sie

220 *Bleutge*, NJW 1985, 1185 (1187).

221 https://chatgpt.org/de/chat [26.6.2023].

können sowohl von Gerichten, Parteien[222], gewerblichen Auftraggebern oder privaten Endverbrauchern[223] bestellt werden. Am häufigsten kennt man sie wohl aus Zivil- und Strafprozessen, der Baubranche oder der Politik. In dieser Arbeit soll es um die gerichtlich bestellten Sachverständigen in einem Strafverfahren gehen.

Wie vermutlich laienhaft erwartet, bedeutet der Begriff gerade nicht, dass ein Sachverständiger immer auf persönliche Eignung und fachliche Kompetenz staatlich zertifiziert ist und evaluiert wird.[224] Die Bezeichnung „Sachverständiger" ist als Qualifikation nicht geschützt.[225]

Im Zusammenhang mit dem Begriff des Sachverständigen in einem Strafverfahren liest und hört man häufig Bezeichnungen wie „Richter in Weiß"[226], „Richtergehilfen"[227] bzw. „Erkenntnisgehilfen"[228] oder „Helfer des Richters"[229]. Letztlich spiegeln diese Bezeichnungen die verschiedenen Prozessrollen des Sachverständigen wider, die sich im Laufe der Jahrhunderte[230] vom („gelehrten", „rationalen") Zeugen[231], dem „Gehilfen des Richters"[232], einem

---

222 Siehe dazu vertieft auch die erst kürzlich erschienene Monographie von *Roider*, Der Einfluss von Sachverständigen – eine emprische Untersuchung am Beispiel der Strafgesetzgebung.

223 So auch die „Privatsachverständigen" beauftragt vom Angeklagen, Verteidiger, Opfer, Privatbeteiligte oder deren Vertreter.

224 Siehe auch *Bleutge*, Sachverständigenrecht, S. 13; Forderung: Es wird daher vorgeschlagen, die Führung der Bezeichnung „Sachverständiger" und vergleichbare Bezeichnungen im Geschäftsverkehr davon abhängig zu machen, dass die betreffende Person zuvor von einer staatlichen Stelle auf persönliche Eignung nach dem Vorbild eines Versteigerers in § 34b GewO geprüft wurde.

225 *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 1.

226 So ging *Gebauer* von einer gar königlichen Stellung des medizinischen Sachverständigen aus, vgl. *Gebauer*, MedSachv. 53 (1957), S. 30 (31). *Leferenz* versteht den Sachverständigen als eine dem Richter gleichwertige Instanz (Richter: Souveränität des Urteils; und Sachverständiger: Fachwissen), vgl. *Leferenz*, Krim. Biol. Gegenwartsfragen, Heft 5, S. 1.

227 BGH deutlich in BGHSt 7, 239; 9, 292; 13, 4; *Walter*, Sachverständigenbeweis, S. 10.

228 *Langelüddeke/Bresser*, Gerichtliche Psychiatrie, S. 251.

229 So *Jessnitzer*, Der gerichtliche Sachverständige, S. 70 ff.

230 Zur geschichtlichen Entwicklung vertiefend *Stinshoff*, Operative Fallanalyse, S. 85 ff. v. a. zur Begründung der immer noch bestehenden Abgrenzungsschwierigkeiten zu den anderen Prozessrollen.

231 *Glaser*, Beiträge, S. 383 ff.

232 Vgl. nur RGSt 52, 161; 57, 158; 69, 98; *v. Hippel*, Lehrbuch des Strafrechts, S. 411; *Wetzell*, System des ordentlichen Civilprocesses, S. 528. Dieser Begriff wurde jedoch uneinheitlich verwendet und kann somit kein eigenständiges dogmatisches Verständnis des Sachverständigenbeweises vermitteln, vgl. *Poppen*, Die Geschichte des Sachverständigenbeweises, S. 228 m. w. N.

Beweismittel eigener Art[233] hin zur heutigen verfahrensrechtlichen Stellung entwickelten.[234] Hier verdeutlicht sich die Schwierigkeit der Abgrenzung der verfahrensrechtlichen Stellung des Sachverständigen von anderen Prozessrollen wie des Richters, des (sachverständigen) Zeugen oder des Augenscheinsgehilfen (mehr dazu unter B. III.). Mit welchem Titel man auch die Rolle des Sachverständigen versehen mag, nach der StPO ist er (neben dem Zeugen) ein persönliches Beweismittel,[235] und wird immer dann hinzugezogen, wenn das einerseits ausdrücklich vorgeschrieben ist (siehe Beispiele der gesetzlichen Sondervorschriften unter B. II. 2.) oder andererseits, wenn Tatsachen festzustellen sind oder Fragen zu beantworten sind im Rahmen der Wahrheitserforschung nach § 244 Abs. 2 StPO, bezüglich deren Feststellung oder Beurteilung das Gericht nicht die erforderliche Sachkunde hat, §§ 73, 78 StPO.[236]

Der Beweis durch den Sachverständigen wird in §§ 72 ff. StPO gesetzlich festgelegt. § 72 StPO schreibt vor, dass auf den Sachverständigen der sechste Abschnitt über Zeugen entsprechend anzuwenden ist, soweit dort nicht abweichende Vorschriften getroffen sind.[237] Im Hauptverfahren erstattet der Sachverständige als eines der vier „Strengbeweismittel" (i. S. v. § 244 Abs. 1 StPO) im Wege der Vernehmung in der Hauptverhandlung, §§ 250 ff. StPO sein Gutachten.[238] Dieses hat er mündlich zu erstatten, zu erörtern und Fragen des Gerichts zu beantworten (vgl. §§ 240, 248, 250, 253 StPO). Allerdings können nicht nur Richter in der Hauptverhandlung Sachverständige beauftragen. Vielmehr ist der Regelfall der Praxis, dass Staatsanwälte (vgl. Nr. 69 f. RiStBV i. V. m. §§ 161a, 73 ff. StPO) bzw. die Polizei (§ 163 Abs. 3 S. 2 StPO)[239] im Ermittlungsverfahren bereits einen Sachverständigen hinzuziehen. Jede Person, die die Voraussetzungen des § 75 StPO erfüllt, ist dann grds. (Gutachten-

---

233 *Zachariae*, II, S. 425 f.; *Birkmeyer*, Deutsches Strafprozessrecht, S. 445; *Mittermaier*, GA 1853, 7.

234 Vertiefend zur geschichtlichen Entwicklung des Sachverständigenbeweises und der sich daraus ergebenden Schwierigkeiten der Abgrezung von anderen Prozessrollen vgl. *Stinshoff*, Operative Fallanalyse, S. 85 ff.

235 *Hegler*, AcP 104 (1909), 151, 152; *Mezger*, AcP 117 (1918), Beilagenheft, 1 f.; SK-StPO/*Rogall*, Vor § 72 Rn. 3; *ders.*, in: FS-Gössel, S. 511; Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 1; KK/*Senge*, Vor § 72 Rn. 1; *Löwe/Rosenberg/Krause*, Vor § 72 Rn. 2; *Ranft*, Strafprozessrecht, Rn. 479.

236 So auch schon *Walter*, Sachverständigenbeweis, S. 12; *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 73.

237 Ein Unterschied zum Zeugenbeweis ergibt sich v. a. im Hinblick auf die Ablehnung des Sachverständigen nach den Vorschriften über die Richterablehnung, § 74 StPO sowie die Vereidigung, § 79 StPO. Hierzu wird vertieft in diesem Teil, B. III. 2. eingegangen.

238 Vgl. auch *Beulke/Swoboda*, Strafprozessrecht, S. 146 ff.

239 BeckOK-StPO/*Sackreuther*, § 161a Rn. 11; KK/*Griessbaum*, § 163 Rn. 18.

verweigerungsrecht nach § 76 StPO)[240] zur persönlichen Erstattung des in Auftrag gegebenen Gutachtens verpflichtet, vgl. § 250 StPO.

Das vorausgesetzt, lässt sich für den Sachverständigen die folgende Definition formulieren: Sachverständige ist eine Person, die wegen der bei ihr als vorhanden vorausgesetzten besonderen Sachkunde von dem zuständigen Strafverfolgungsorgan beauftragt wird, ihre Sachkunde – objektiv und weisungsfrei – in Form von Mitteilung abstrakter Erfahrungssätze und/oder Begutachtung konkreter Tatsachen anzuwenden und/oder Befundtatsachen wahrzunehmen und dem Strafverfolgungsorgan darüber Auskunft zu erteilen.[241]

In den nächsten Abschnitten soll nun auf die verschiedenen Voraussetzungen der Definition eingegangen werden. V. a. in Bezug auf die Abgrenzung zu Zeugen (wie Ermittlungspersonen) soll an späterer Stelle verdeutlicht werden, inwiefern sich diese Definition für die IT-Sachverständige im Konkreten darstellt und spezifiziert.

2. Auftrag und Auswahl

Im „Münchener Anwaltshandbuch für die Strafverteidigung“ schrieb Deckers[242] zum Problem der Auswahl und Kontrolle des Sachverständigen: „Der Auswahl des jeweiligen Sachverständigen kommt für die Entscheidungen im Strafverfahren große Bedeutung zu. Deshalb ist gerade dieses Element ein im Verfahren hart umkämpftes Terrain.“ Und an anderer Stelle: „In allen Fachgebieten gilt, dass die Auswahl des Sachverständigen weichenstellenden Charakter für das Verfahren insgesamt hat.“[243] So ist „der Auftrag“ der Beweisperson nicht nur (mit)entscheidend für ihre Verfahrensstellung (als Sachverständigenbeweis oder Zeuge), sondern es kann u. U. auch einen qualitativen Unterschied für den Fortgang der Ermittlungen bzw. den Ausgang des Verfahrens machen, wann ein IT-Sachverständiger hinzugezogen wird; die Praxis meint, je früher desto besser.[244] Dieser erste Schritt, die Beauftragung eines

---

240 Der Sachverständige kann gem. § 76 Abs. 1 S. 1 StPO das Gutachten aus denselben Gründen verweigern, die einen Zeugen berechtigen, das Zeugnis zu verweigern. Auch aus anderen Gründen kann der Sachverständige von der Verpflichtung ein Gutachten erstatten zu müssen entbunden werden, vgl. § 76 Abs. 1 S. 2 StPO. Vgl. SK-StPO/*Rogall*, § 76 Rn. 17; KK/*Senge*, § 76 Rn. 4; Löwe/Rosenberg/*Krause*, § 76 Rn. 4; Meyer-Goßner/*Schmitt*, § 76 Rn. 3; *Bleutge*, DRiZ 1977, 170 (172).

241 *Mezger*, AcP 117 (1918), Beilageheft, 1, 3, 5; SK-StPO/*Rogall*, Vor § 72 Rn. 7; dem folgend *Stinshoff*, Operative Fallanalyse, S. 166 f.

242 MAH/*Deckers*, § 81 Rn. 17.

243 *Eisenmenger*, Ärztliches Strafrecht, S. 49.

244 Bspw. schon als kriminaltechnischer Sachbeweis im Ermittlungsverfahren und nicht erst in der Hauptverhandlung. Ein kriminaltechnischer Sachbeweis wird regelmäßig durch die entsprechenden Dienststellen der Strafverfolgungsbehörden erbracht.

Gutachtens, kann also entscheidungsrelevant sein. Denn angesichts der zahlreichen Heuristiken[245] und möglichen Urteilsverzerrungen[246], die mit der Sachverständigenauswahl zusammenhängen, jedenfalls aber in Anbetracht der oft eigenen Ahnungslosigkeit hinsichtlich der technologischen Zusammenhänge, ist es von entscheidender Bedeutung, die richtigen IT-Sachverständigen auszuwählen und sie in prozessordnungsgemäßer Weise zu beauftragen. So kann die Chance gesteigert werden, brauchbare Gutachten zu erhalten – und zu rechtsstaatlichen Entscheidungen zu gelangen.[247]

Dabei ergibt sich die Verfahrensstellung der IT-Sachverständigen nicht von selbst. Sie muss ausgewählt und bestellt werden (so wird sie aktiv in das Verfahren einbezogen), und zwar von dem Prozessorgan, das ihre Sachkunde in Anspruch nehmen will.[248] Die Auftragserteilung bestimmt den Gegenstand des Beweises (mit).[249]

Im Hinblick auf die Entscheidung der Notwendigkeit der Bestellung eines Sachverständigen hat das Strafverfolgungsorgan als Auftraggeber grds. einen Beurteilungsspielraum.[250] Jedenfalls besteht grds. keine Verpflichtung, wenn es selbst die erforderliche Sachkunde besitzt, vgl. § 244 Abs. 4 S. 1 StPO.[251] Ausnahme bilden einige gesetzlich vorgeschriebene Fälle, in denen die Hinzuziehung eines Sachverständigen vorgeschrieben ist, vgl. §§ 80a (Zuziehung im Vorverfahren), 81a Abs. 1 (körperliche Untersuchung der beschuldigten Person), 81c Abs. 2 S. 2 (körperliche Untersuchung anderer Personen), 81e i. V. m. f Abs. 2 (molekulargenetische Untersuchung), 87 S. 1[252] (Leichenschau und Leichenöffnung), 91 Abs. 1 (Vergiftung), 92 Abs. 1 (Geld- oder Wertzeichenfälschung), 93 (Schriftvergleichung), 246a Abs. 1 (Unterbringung), 275a Abs. 4, 414 ff. (Sicherungsverwahrung), 454 Abs. 2 StPO (Straf-

---

Die Kriminaltechnik dient dem Entschlüsseln von Spuren am Tatort zur Unterstützung der Ermittlungen, vgl. mehr zum kriminaltechnischen Sachbeweis SK-StPO/*Rogall*, Vor § 72 Rn. 182 ff.; *Peters*, Strafprozess, S. 295, 325; *Eisenberg*, Beweisrecht der StPO, Rn. 1895 ff.

245 Heuristik bezeichnet die Kunst, mit begrenztem Wissen (unvollständigen Informationen) und wenig Zeit dennoch zu wahrscheinlichen Aussagen oder praktikablen Lösungen zu kommen, vgl. *Gigerenzer/Todd*, Simple heuristics that make us smart, ABC Research Group (2000) Vol. 23, S. 727.

246 Siehe dazu in diesem Teil, B. II. 2. c) ee).

247 Vertiefend dazu *Vogel/Volkmann*, GesR 2021, 753 (754).

248 Vgl. *Stinshoff*, Operative Fallanalyse, S. 119 f.

249 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 270.

250 RGSt 70, 336, 338; vgl. *Mayer*, in: FS-Mezger, S. 455, 461; vgl. nur *Beulke/Swoboda*, Strafprozessrecht, Rn. 199; *Peters*, Strafprozess, S. 366; SK-StPO/*Rogall*, Vor § 72 Rn. 21; a. A. *Goldschmidt*, Der Prozess als Rechtslage, S. 440; *Müller*, Der Sachverständige im gerichtlichen Verfahren, Rn. 67.

251 SK-StPO/*Rogall*, Vor § 72, Rn. 20.

252 Mit Einschränkung in § 87 Abs. 1 S. 2 StPO.

aussetzung), §§ 43 Abs. 2 S. 2, 73 JGG (Feststellungen zum Entwicklungsstand). Teilweise findet man in diesen Vorschriften ebenfalls Bestimmungen über die Anzahl der hinzuzuziehenden Sachverständigen, über die Person und über die Art der Beweiserhebung, vgl. bspw. §§ 87 Abs. 2, 91 StPO.[253] Besteht keine gesetzliche Pflicht zur Bestellung eines Sachverständigen, muss das Gericht nach seinem eigenen Sachverstand und Ermessen entscheiden, ob es selbst die nötige besondere Sachkunde zur Bewertung und Würdigung des Sachverhalts aufbringen kann.[254]

a) Die Grenzen der eigenen Sachkunde des Auftraggebers

Die Entscheidung des Auftraggebers darüber, wann ein Sachverständiger beauftragt werden soll – wann also die eigene Sachkunde nicht mehr ausreicht, um den Sachverhalt in Bezug auf die jeweiligen Fragen zu erforschen – kann man auch beschreiben als einen „Balanceakt" zwischen „Selbstvertrauen oder Selbstmisstrauen".

§ 261 StPO verlangt, dass eine vertrauenswürdige Überzeugung von dem Sachverhalt nur aus dem Inbegriff der Verhandlung geschöpft werden darf und gem. § 244 Abs. 2 StPO erst dann, wenn das Gericht die Beweisaufnahme auf alle zur Verfügung stehenden und beweisbedürftigen Tatsachen und Beweismittel erstreckt hat, die (aus der Perspektive des Gerichts zum Zeitpunkt der Urteilsfindung) für die Entscheidung von Bedeutung sind.[255] Sachverständige werden in Wissensgebieten eingesetzt, in denen die Auftraggeber sich misstrauen müssen, weil ihnen die erforderliche Sachkunde fehlt. Das Wissen der Auftraggeber kann lediglich lückenhaft sein, so dass die Mitteilung einzelner Erfahrungssätze genügt. Es kann aber auch in dem Umfang fehlen, dass ein umfassendes Sachverständigengutachten mit Schlussfolgerungen notwendig wird (vgl. zu den verschiedenen Aussagekategorien B. II. 3. d))[256]. Je nachdem wird dann die Beweisfrage formuliert und an den Sachverständigen zur Beantwortung übergeben. Nach dem Konzept der StPO ist es Aufgabe des Gerichts, die Entscheidung zu treffen, wann ein Sachverständiger hinzuzuziehen ist – wann es sich selbst also nicht mehr genug vertrauen kann, seiner Aufgabe aus § 244 Abs. 2 StPO nachzukommen und Hilfe bei der Sachverhaltsermittlung benötigt. Aus dem Gesetz folgt dieser Grundsatz aus § 244

253 SK-StPO/*Rogall*, Vor § 72 Rn. 16 f. und § 73 Rn. 20; *Ulrich*, Der Gerichtliche Sachverständige, Rn. 116 ff.; *Peters*, Strafprozess, S. 366 ff.; vgl. *Eisenberg*, Beweisrecht der StPO, Rn. 1501.

254 Vgl. auch *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 26 ff., 31; *Stinshoff*, Operative Fallanalyse, S. 122.

255 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 57.

256 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 57.

Abs. 4 S. 1 StPO (Beurteilung von Beweisanträgen), der es dem Gericht ermöglicht (über die Gründe des Abs. 3 S. 3 hinausgehend), einen Beweisantrag abzulehnen, wenn das Gericht selbst die erforderliche Sachkunde besitzt. Es folgt aber im Rahmen der Amtsaufklärungspflicht auch daraus, dass der konstitutive Sprachgebrauch in Bezug auf die Sachverhaltsfeststellungen der Autoritätsposition des Gerichts vorbehalten bleibt.[257] Das Gericht muss sich also wenigstens in Bezug darauf vertrauen dürfen, dass es die Fähigkeit besitzt, die Bereiche, in denen es dem eigenen Urteil vertrauen darf, von denjenigen zu unterscheiden, in denen Misstrauen angebracht ist.[258]

Es stellt sich damit die Frage, wann die Grenze des Ermessens in Bezug auf die eigene Sachkunde des Auftraggebers erreicht ist.[259]

Zu der Frage, wann der Richter[260] im Rahmen seines Ermessens einerseits und seiner Aufklärungspflicht andererseits einen Sachverständigen hinzuziehen muss, hat die höchstrichterliche Rspr. bis heute allgemeine Grundsätze aufgestellt.[261] Das RG hat am Anfang seiner Rechtsprechung die Meinung vertreten, dass der Tatrichter auch dann, wenn die Beurteilung des Sachverhalts besondere Sachkunde erfordere, nicht verpflichtet sei, einen Sachverständigen zuzuziehen; er dürfe, wenn er sich die erforderliche Sachkunde selbst zutraue, ohne Anhörung eines Sachverständigen entscheiden.[262] Das

---

257 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 59.

258 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 57.

259 Vertiefend dazu auch *Arab-Zadeh*, NJW 1970, 1214.

260 *Exkurs*: Uneinheitlich wird dabei die Frage beantwortet, ob bei einem Kollegialgericht sämtliche Mitglieder über die jeweils erforderliche Sachkunde verfügen müssen. *Zustimmend*: Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, S. 714; Löwe/Rosenberg/*Gollwitzer*, § 244 Rn. 301; *Kleinknecht/Meyer*, § 244 Rn. 73; *Laufs*, Arztrecht, S. 113; *Lenckner*, Strafe, Schuld und Schuldfähigkeit, S. 140; *Mengel*, Die Erhebung des Sachverständigenbeweises im Strafprozess, S. 79; *Mösl*, DRiZ 1970, 112; *Roxin/Schünemann*, Strafverfahrensrecht, S. 257; *G. Schäfer*, Die Praxis des Strafverfahrens, S. 350; *Schlüchter*, Das Strafverfahren, Rn. 554.1. *Ablehnend* (v. a. mit Hinweis darauf, dass sich andernfalls die richterliche Urteilsbildung auf sachverständige Äußerungen in der geheimen Beratung stützen würde): *Göppinger*, Forensischen Psychiatrie, Bd. 2, S. 1498 (1532); *Gössel*, Strafverfahrensrecht, S. 257; *Ligges*, Die Stellung des Sachverständigen, S. 117 f.; KMR/*Paulus* § 244 Rn. 466; *Peters*, Strafprozess, S. 313; *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 115, der die Hinzuziehung von Sachverständigen jedenfalls dann fordert, wenn sich mind. eines der übrigen Mitglieder des Gerichts durch die vermittelte Sachkunde der anderen nicht überzeugen lässt; vgl. auch *Eb. Schmidt*, Nachträge, § 244 Rn. 24; wohl auch KK/*Herdegen*, § 244 Rn. 30; ferner dazu *Bockelmann*, GA 1955, 327; *Döhring*, JZ 1968, 642; *Hanack*, JZ 1972, 116; *Kohlhaas*, NJW 1962, 1330; *Pieper*, ZZP 84 (1971), S. 1 (17 f.); *Rosenberg/Schwab/Gottwald*, Zivilprozessrecht, S. 730; *Tröndle*, JZ 1969, 374.

261 Vgl. dazu auch *Stinshoff*, Operative Fallanalyse, S. 123 f.; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 61, 179.

262 Vgl. z. B. RGSt 3, 176; 14, 276, 278; 25, 326; 47, 100, 108; 51, 42; 52, 61, 62 f.

galt, trotz gelegentlich nicht unbedenklicher Ergebnisse, selbst in technischen Fragen,[263] was jedoch im Einklang mit der damaligen Rechtsordnung stand.[264] Gegen diese Rspr. wehrten sich Verteidiger[265] und einige Stimmen im Schrifttum.[266] 1927 führte das RG[267] dann den längst fälligen Wandel herbei, und entschied, dass der Tatrichter in seinem Zutrauen auf die eigene Sachkunde die Zuziehung eines Sachverständigen nur dann unterlassen dürfe, wenn er diese Sachkunde nach der Erfahrung des Lebens[268] auch haben könne.[269] Diese Leitlinie erhärtete sich in der weiteren Rspr.[270], schließlich auch in der des BGH's.[271] Später begrenzte der 4. Strafsenat die Freiheit des erkennenden Gerichts bzgl. der Hinzuziehung eines Sachverständigen dahingehend, dass es sich dann nicht mit der eigenen Sachkunde zufrieden geben darf, wenn es „(…) nicht die unbedingte Gewissheit besitzt, dass seine Sachkunde ausreicht (…)"[272] und wegen der Besonderheit des Sachverhalts Zweifel über die ausreichende Sachkunde des Gerichts aufkommen können.[273] Das erkennende Gericht muss somit grds. in den Fällen einen Sachverständigen hinzuziehen,

---

263 Beispiel aus RGSt 25, 326.

264 Vgl. nur *Binding*, Grundriss des Deutschen Strafprozessrechts, S. 152; *Hahn*, Die gesamten Materialien zur Strafprozessordnung, S. 120.

265 Allen voran Alsberg, z. B. in *Alsberg*, LZ 1915, 482 ff.

266 *Lobe*, DRiZ 1913, 362, der schon damals auf die Gefährlichkeit von Halbwissen bei der Urteilsbildung hinwies; dem folgend z. B. *Goldschmidt*, Der Prozess als Rechtslage, S. 440; *Kohlhaas*, NJW 1962, 1330; *Kruse*, DÄBl. 1978, 2919; *Rudolph*, Die Justiz 1969, 25; Löwe/Rosenberg/*Sarstedt*, § 73 Rn. 1; *Sieverts*, Fachpsychologische Aufgaben, S. 97; *Eb. Schmidt*, Arzt als Sachverständige, S. 164. Einige Stimmen der Literatur billigten diese Rechtsprechung aber auch, bspw. *Beling*, Deutsches Reichsstrafprozessrecht, S. 297; *Graf zu Dohna*, S. 102; *Bockelmann*, GA 1955, 322 Fn. 7 m. w. N.

267 RGSt 61, 273.

268 Diesen Begriff grenzte das RG danach ab „was herkömmlicherweise als richterlicher Erfahrung zugänglich und als von richterlicher Erfahrung beherrschbar angesprochen worden ist", vgl. dazu auch *Eb. Schmidt*, in: FS-Schneider, S. 259 f.

269 Vgl. zu diesem „Wendepunkt" *Alsberg/Nüse/Meyer*, Der Beweisantrag im Strafprozess, S. 690 f.; *Bockelmann*, GA 1955, 325; *Plewig*, Funktion und Rolle des Sachverständigen, S. 33; *Eb. Schmidt*, Der Arzt im Strafrecht, S. 154 f.; *ders.*, Lehrkommentar II, § 244 Rn. 67; *Wolschke*, S. 48 ff.; *Wüst*, S. 16.

270 Z. B. JW 1928, 2988; 1931, 1493 f.; 1932, 3358; 1936, 1976; 1937, 1360; 1938, 3163; 1939, 754; HRR 1939 Nr. 1208; 1940 Nr. 207; RGSt 76, 350; 77, 198. Der BGH führte diese Rechtsprechung fort und verwendete einen entsprechenden Maßstab der „allgemeinen Erfahrung": BGHSt 2, 163, 164 = LM StPO § 244 Abs. 2 Nr. 6 mit Anm. Jagusch = NJW 1952, 554; 3, 169, 175 = LM StPO § 244 Abs. 2 Nr. 11 mit Anm. Kohlhaas = NJW 1952, 1343 = JZ 1953, 44; 5, 34, 36 = NJW 1954, 83.

271 BGHSt 3, 52 ff.

272 BGHSt 23, 8, 12.

273 Zu derartigen Besonderheiten siehe auch SK-StPO/*Rogall*, Vor § 72 Rn. 22; *Jansen*, Zeuge und Aussagepsychologie, Rn. 103 ff. m. w. N.

in denen eine Sachkunde erforderlich ist, die ein forensisch erfahrener Richter im Normalfall nicht hat.[274] Wenn der Richter mehr als Allgemeinwissen in Anspruch nimmt, um den Sachverhalt ohne Hinzuziehung eines Sachverständigen zu beurteilen, muss er das Innehaben dieser Sachkunde im Urteil explizit darlegen, um die Überprüfbarkeit im Revisionsverfahren[275] zu gewährleisten.[276] Eigene hinreichende Sachkunde des Gerichts kann bspw. durch richterliche Tätigkeit auf einem bestimmten Gebiet erworden werden[277] oder sonstige berufliche Erfahrungen, intensive Beschäftigung mit außerjuristischen Fachfragen, Zusatzausbildungen oder auch technische Fähigkeiten können zum Erwerb eines Spezialwissens führen.[278] Eine bloß theoretische Information (wie etwa das Studium von Fachliteratur) soll aber in der Regel nur genügen, wenn es um „gesicherte, einfach strukturierte und bei Anwendung im Einzelfall leicht zu handhabende Erfahrungssätze" geht.[279] Die Berufung auf eigene Sachkunde ist rechtsfehlerhaft, wenn sich das Gericht die Sachkunde gezielt im Freibeweisverfahren verschafft.[280]

Wenn die Beantwortung der Beweisfrage jedoch Anwendungs- oder Auswertungswissen voraussetzt, das nur in besonderer Ausbildung und praktischer Betätigung erworben werden kann (wie etwa aus Wissenschaftsgebieten wie Medizin, Chemie oder bestimmte Disziplinen aus der Kriminaltechnik)[281], wird die richterliche Kenntnis in der Regel nicht ausreichen. So ist es inzwischen gesicherte Auffassung, dass sich die Tatrichter die Entscheidung in medizinischen und psychiatrisch-psychologischen Fragen[282] sowie auch in

---

274 Vgl. SK-StPO/*Rogall*, Vor § 72 Rn. 23 mit Beispielen.

275 Diese Grenze des Ermessens in Bezug auf die eigene Sachkunde des Auftraggebers ist auch revisionsgerichtlich überprüfbar, vgl. SK-StPO/*Rogall*, Vor § 72 Rn. 21; vgl. auch BGHSt 3, 27, 28; BGH StV 1987 mit abl. Anm. Peters; Alsberg/Nüse/Meyer, Der Beweisantrag im Strafprozess, S. 696. Dabei sind die Prozessbeteiligten hinsichtlich der eigenen (ggf. ungenügenden) Sachkunde der Gerichtspersonen auf den Nachweis einer ungenügenden Darstellung im Urteil angewiesen, um erfolgreich Revisionsrügen erheben zu können (Aufklärungsrüge gem. § 344 Abs. 2 S. 2 StPO, wegen unzulänglicher Ausschöpfung eines Beweismittels).

276 *Stinshoff*, Operative Fallanalyse, S. 124 m. w. N.; KK/*Krehl*, § 244 Rn. 198.

277 Vgl. vgl. BGH NStZ 1983, 325.

278 KK/*Krehl*, § 244 Rn. 45 f.

279 KK/*Herdegen*, § 244 (5. Auflage 2003) Rn. 27.

280 BGH StV 2019, 811 (812); NStZ 2022, 372 (373) m. Anm. *Krehl* NStZ 2022, 374.

281 KK/*Krehl*, § 244 Rn. 45 m. w. A.

282 So ist bspw. den Anträgen auf Zuziehung eines Sachverständigen stattzugeben, wenn es um die Beurteilung der Glaubwürdigkeit kindlicher Zeugen geht (vgl. BGHSt 7, 82 = LM StPO § 244 Abs. 2 Nr. 15 mit Anm. von Jagusch = NJW 1955, 599; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 152 ff., 160 ff.) oder um die Schuldfähigkeit eines Täters, der geistig zurückgeblieben ist (vgl. BGH NJW 1967, 299) oder um die Auswirkung hochgradiger Affektzustände auf die Schuld-

verschiedenen anderen Fällen[283] nicht allein zutrauen dürfen. Keinesfalls darf sich das Gericht jedenfalls mit reinen Vermutungen und Unterstellungen begnügen statt einen Sachverständigen zu beauftragen.[284] Schon beim geringsten Zweifel an ausreichender eigener Sachkunde muss das Gericht einen Sachverständigen hinzuziehen.[285]

Dagegen haben sich in der Rspr. auch Standardfälle herausgebildet, in denen die richterliche Sachkunde ausreichend ist[286] bzw. entbehrlich ist. Letztgenanntes dann, wenn insoweit durch die höchstrichterliche Rechtsprechung anerkannte wissenschaftliche Erfahrungssätze vorliegen, die der Richter nach der Rechtsprechung des BGH „hinnehmen" muss (zu gesicherten wissenschaftlichen Erfahrungssätzen siehe 4. Teil, A. III. 4. b) cc) (2) (a)):[287] bspw. die Funktionsfähigkeit und Messgenauigkeit von standardisierten Messverfahren bei Geschwindigkeitsmessungen.[288] Diese werden gelegentlich als

---

fähigkeit des Täters (vgl. BGH NJW 1952, 633 = LM StPO § 244 Abs. 2 Nr. 7; NJW 1969, 1578 = JR 1969, 426; VRS 16, 186, 188; 37, 430, 437; OLG Köln VRS 6, 49; OLG Schleswig SchlHA 1953, 67) festzustellen; weitere Beispiele vgl. *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 29 f.

283 BGH 23.2.1999 NJW 99, 1860: Zu den Voraussetzungen unter denen ein Sachverständigengutachten zum Hergang eines Verkehrsunfalls eingeholt werden muss; § 43 JGG siehe *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 77 Fn. 48. Insb. ist die Beauftragung eines ärztlichen Sachverständigen geboten, wenn Anhaltspunkte dafür vorliegen, dass die angeklagte Person zur Zeit der Tat an einer krankhaften seelischen Störung, einer tiefgreifenden Bewusstseinsstörung oder Schwachsinn oder einer schweren anderen seelischen Abartigkeit gelitten hat, §§ 20 ff. StGB vgl. *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 77, Fn. 49, 50.

284 *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 73.

285 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 59; BGHSt 23, 8 (12); *Pfeiffer*, NStZ 1982, 189; KK/*Herdegen*, § 244, Rn. 28.

286 Die Rückrechnung zur Feststellung der BAK zur Tatzeit kann sich das Gericht im Normalfall selbst zutrauen, soweit die Fahrtüchtigkeit eines Kraftfahrers zu beurteilen ist und der Fall keine Besonderheiten aufweist. Weiter hierzu *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 79 Fn. 63. Auch die Glaubwürdigkeit von Zeugen darf das Gericht regelmäßig ohne einen Sachverständigen beurteilen, *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 80, Fn. 65, 66.

287 *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 81. Vgl. auch die Ausführungen von *Mysegades*, Software als Beweiswerkzeug, S. 231 ff. zu standardisierten Verfahren im Strafprozess.

288 Vgl. etwa: VerfG Saarland, Beschl. v. 27.4.2018 – Lv 1/18; VerfG Saarland, Urt. v. 5.7.2019 – Lv 7/17; OLG Bamberg, Beschl. v. 13.6.2018 – 3 Ss OWi 626/18; OLG Bamberg, Beschl. v. 4.10.2017 − 3 Ss OWi 1232/17; OLG Bamberg, Beschl. v. 4.4.2016 – 3 Ss OWi 1444/15; OLG Zweibrücken, Beschl. v. 28.2.2018 – 1 OWi 2 SsBs 106/17; OLG Oldenburg, Beschl. v. 13.03.2017 – 2 Ss [OWi] 40/17; OLG Saarbrücken (Bußgeldsenat), Beschl. v. 9.11.2017 – Ss Rs 39/2017 (60/17 OWi); BayObLG, Beschl. v. 9.12.2019 – 202 ObOWi 1955/19; OLG Bamberg, Beschl. v. 13.6.2018 – 3 Ss OWi 626/18; LG Düsseldorf (2. Senat für Bußgeldsachen), Beschl. v. 21.1.2021 – 2 RBs 1/21; OLG Koblenz, Beschl. v. 22.2.2021 – 3 OWi 6 SsBs 275/20

„antizipierte Sachverständigengutachten“ bezeichnet.[289] Dabei ist jedoch zu beachten, dass diese Regeln ein Sachverständigengutachten keinesfalls ersetzen können, weil sie nicht in einem gesetzgeberischen Verfahren zustande gekommen sind.[290] Außerdem sind sie wegen der Fortentwicklung der Technik oder Gesellschaft oft nicht mehr dem aktuellen Stand entsprechend[291]; oder unterliegen bisher unentdeckten Fehlern, die regelmäßig geprüft werden sollten.[292] Die aktuellen Verhältnisse können nur durch den sich ständig fortbildenden Sachverständigen ermittelt werden.

An späterer Stelle (4. Teil, A. III. 4. b) cc) (2)) sollen die Methodiken und Erfahrungssätze der forensischen Informatik in eine „Zuverlässigkeitsskala“ eingeordnet werden und dabei gezeigt werden – nicht zuletzt aufgrund der Besonderheit der Technologie[293] und der dadurch bedingten Schnelllebigkeit – dass zum jetzigen Stand der Forschung bei der Einbringung und Bewertung von digitalen Spuren im Rahmen eines IT-Sachverständigenbeweises nicht von einem gesicherten Erfahrungswissen gesprochen werden kann. D. h. wurden bspw. bei der Ermittlung digitaler Spuren Datenverarbeitungs- und -analysemethoden eingesetzt oder bestimmte Erfahrungssätze aus dem Bereich der forensischen Informatik angewendet und finden diese nun Eingang in ein Strafverfahren, dürfen die Richter ihre Beweiswürdigung nicht dergestalt abkürzen, dass es sich bei den angewendeten Methodiken um „standardisierte Verfahren“ bzw. „gesicherte Erfahrungssätze“ handeln würde. Die Richterinnen treffen stattdessen vielmehr umfangreichen Prüf- und Darstellungsanforderungen bzgl. der Methodiken und Erfahrungssätze sowie der zugrundeliegenden Prämissen. All diese gehören zum Tatsachenstoff, der in der Hauptverhandlung erörtert werden muss. Eine Erklärung und Nachvollziehbarkeitskontrolle dürfte den Richterinnen, denen eine eigene Plausibilitätskontrolle der Ergebnisse aufgrund fehlender besonderer Sachkunde im Bereich der forensischen Informatik regelmäßig verwehrt sein. Dazu müssten dann i. d. R. IT-Sachverständige gehört werden.

(AG Wittlich), BeckRS 2021, 15340; VGH Baden-Württemberg, Urt. v. 16.1.2023 – 1 VB 38/18; zuletzt BVerwG, Urt. v. 2.2.2023 – 3 C 14/21. Hier konnte in letzter Zeit ein Disput der Gerichte beobachtet werden, in welchem Umfang die Prozessbeteiligten die zugrundeliegenden Daten „einsehen“ dürfen, um die Funktionsweise dieser standardisierten Verfahren überprüfen zu können. Dazu später unter B. V. 2. b) mehr.

289 Vgl. dazu bspw. die Ausführungen zu Geschwindigkeitsmessgeräten in Bußgeldverfahren als „antizipierte Sachverständigengutachten“ in: *Mysegades*, Software als Beweiswerkzeug, S: 293 ff.

290 *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 82.

291 Vgl. nur den „aktuellsten“ Stand des BSI-Leitfaden zur forensischen Informatik „Version 1.0.1 (März 2011)“.

292 Vgl. die o. g. Rechtsprechungsübersicht zu den standardisierten Messverfahren bei Geschwindigkeitsmessungen in Fn. 320.

293 Vgl. dazu die Ausführungen im 2. Teil A. III.

Um die Ausführungen von oben (beim Umfang der Wahrheitserforschung, siehe B. I. 2.) an dieser Stelle noch einmal hervorzuheben: Das Gericht muss seine Ermessensentscheidung bzgl. der Notwendigkeit einer Sachverständigenbestellung unter Berücksichtigung seiner Amtsaufklärungspflicht, den Prinzipien der vollständigen und erschöpfenden Beweiswürdigung sowie der sich daraus ergebenden Pflicht zur Verwendung des bestmöglichen und sachnächsten Beweismittels im konkreten Fall entscheiden. Das gilt insb. im Hinblick auf zu erwartende zusätzliche Informationen (wie etwa die zu erwartenden [Meta-]Informationen und der [wahrscheinliche] Ausschluss einer Manipulation), die in den Daten enthalten sein könnten. In Bezug auf digitale Daten bzw. Datenverarbeitungsvorgänge werden die Tatgerichte wohl in den allermeisten Fällen im Zusammenhang mit der Verwendung und Bewertung von Daten als Beweismittel dazu verpflichtet sein, einen IT-Sachverständigen als bestmögliches und sachnächstes Beweismittel zu beauftragen, soweit die Richter ihrer eigenen Sachkunde auf diesem Gebiet misstrauen werden müssen.[294]

Nicht nur in der Rechtswissenschaft wird das Erfordernis von besonderer Sachkunde in Bezug auf die Handhabung digitaler Spuren bestätigt.[295] Auch Wissenschaftler der forensischen Informatik betonen, dass ein hohes Maß an Fachwissen erforderlich ist, um die gängigen Beweisfragen beantworten zu können, was von („durchschnittlichen") Richtern nicht erwartet werden kann.[296] Das könnte darin begründet liegen, dass die forensische Informatik, im Vergleich zu anderen forensischen Disziplinen, durch einen wesentlich komplexeren Prozess zum Ergebnis des Beweisthemas gelangt, bei dem Ermittler die Aktivitäten des Benutzers nachverfolgen müssen und keine einfache Ja-oder-Nein-Antwort geben können.[297] So ist bspw. die Interpretation der gespeicherten Daten von sehr vielen Randbedingungen abhängig, etwa installierten Programmversionen und persönlichen Einstellungen, und ist darum eine komplexe Angelegenheit, für die man geschulte Spezialistinnen braucht. Eine weitere Schwierigkeit ist oft die schiere Datenmenge, die schon auf kleinen Geräten gespeichert ist; oft begleitet von schlecht formulierten Untersuchungsaufträgen – d. h., wenn man also nicht genau weiß, wonach man suchen soll, wird es noch schwieriger. Hinzu kommt das Phänomen der

---

294 Vgl. dazu auch *Marshall*, Digital Evidence and Electronic Signature Law Review (2020) Vol. 17, S. 2; *Mason/Seng*, Electronic Evidence, S. 101 ff.

295 So auch *Wenzel*, NZWiSt 2016, 85; *Mysegades*, Software als Beweiswerkzeug, S. 135 in Bezug auf die Beurteilung der Zuverlässigkeit „opaker" Software, die weder weit verbreitet ist noch eine unabhängige Überprüfung aufweist.

296 Vgl. bspw. *Dewald/Freiling*, Forensische Informatik, S. 13.

297 „… much more involved process where the investigator must trace user activity and cannot provide a simple yes or no answer", vgl. *Carrier/Spafford*, Journal of Digital Evidence (2003) Vol. 2, S. 177.

„Verschlüsselung“, die eine technische Auswertung nochmal komplizierter macht. Auch der Gesetzgeber sieht im Umgang mit digitalen Daten ein hohes Maß an technischer Expertise als erforderlich (vgl. bspw. die Gesetzesbegründung zu § 110 StPO).[298] Ebenso verdeutlicht die aktuelle Rspr. in Bezug auf die Qualitätsanforderungen einer Sachverständigentätigkeit (in Abgrenzung zu einfacher Ermittlungstätigkeit), dass häufig die (durchschnittliche) Sachkunde von Strafverfolgungsbehörden in Bezug auf die Auswertung von IT-Asservaten überstiegen wird (vgl. dazu B. IV.). Zuletzt wurde auch im Rahmen der Enchro-Chat-Verfahren beschrieben, dass das Verständnis und die Beurteilung möglicher Fehlerquellen im Zusammenhang mit der Integrität der Daten (d. h. deren Korrektheit, Vollständigkeit und Konsistenz) eine erhebliche technische Sachkunde erfordern, über die in aller Regel nur ein IT-Sachverständiger verfügt.[299] Das kann man – in Anbetracht der Universalität der Technologie – unendlich weit zuspitzen, vgl. nur den Fall U. S. v. Rudy Frabizio[300], wonach Multimedia-Forensik-Laien nicht mehr in der Lage waren, zu beurteilen, ob ein einfaches Foto echt oder unecht ist. Das wird wohl in der Zukunft einer noch „besseren KI“ immer schwieriger werden. Es ist jedoch immer auf den Einzelfall und die zu beantwortende Beweisfrage zu achten: Eine Beauftragung einer IT-Sachverständigen kommt eben nur hinsichtlich solcher Umstände in Betracht, für deren Feststellung und Beurteilung dem Gericht selbst die erforderliche Sachkunde fehlt. Für die Feststellung der Zahl (das bloße Zählen) sowie für die Beurteilung des Inhalts der aus den Speichermedien gewonnenen Dateien wird das Gericht selbst sachkundig sein; deren Inaugenscheinnahme ist originäre Aufgabe des Tatsachengerichts (Unmittelbarkeitsprinzip). In diesem Zusammenhang ist auch Nr. 69 RiStBV zu beachten, wonach die Staatsanwaltschaft einen Sachverständigen nur hinzuziehen soll, wenn sein Gutachten für die vollständige Aufklärung des Sachverhalts unentbehrlich ist.[301]

Dem Balanceakt des „Selbstvertrauens oder Selbstmisstrauens“ inhärent sind einige Probleme, die jedoch auch in anderen forensischen Disziplinen bestehen und in anderen wissenschaftlichen Arbeiten ausgiebig thematisiert wurden und hier deshalb nur überblicksartig Erwähnung finden sollen: 1) So sind Gerichtspersonen vor der Beweiserhebung häufig nicht in der Lage zu sehen, ob sich später herausstellen wird, dass Fragen auftreten, die ihr Wissen übersteigen; 2) Die Frage, ob die Mitteilung von Fachwissen hinreicht oder ob

298 Vgl. MüKoStPO/*Hauschild*, 2. Auflage, § 110 Rn. 11 m. w. N.

299 LG Berlin, EuGH-Vorlage v. 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22), Rn. 84.

300 United States of America, Appellant, v. Rudy Frabizio, Defendant, Appellee, 459 F.3d 80 (1st Cir. 2006).

301 Vgl. dazu auch BVerwG (2. Senat), Beschl. v. 18.6.2020 – 2 B 24.20.

dem Gericht auf dem Gebiet Wissen in dem Maße fehlt, dass ein umfassendes Gutachten erforderlich ist, ist oft zweifelhaft und der Übergang fließend. 3) Die Entscheidung über Selbstmisstrauen oder Selbstvertrauen setzt die Prognose darüber voraus, wie sich die Beweisaufnahme und die Beweiswürdigung gestalten, insbesondere darüber, welche Schwierigkeiten dabei auftreten können. Die vom Gesetz geforderte Entscheidung des Gerichts über die Zuziehung eines Sachverständigen wäre unmöglich, falls darin bereits eine unzulässige Beweisantizipation gesehen werden sollte.[302] Und 4) In manchen Fällen muss der Richter sich bereits fragen, ob er überhaupt allein über die Zuziehung eines Sachverständigen entscheiden kann.[303]

Zusammenfassend lässt sich feststellen, dass Strafverfolgungsbehörden einen Sachverständigen beauftragen sollten, wenn sie folgenden Aussagen zustimmen: Wenn ich 1) in dem einschlägigen Bereich kein hinreichendes Wissen besitze (Beweisthemen der Ersten Aussagekategorie), 2) nicht hinreichend sicher das Wissen anwenden kann (Beweisthemen der 2. Aussagekategorie), 3) nicht hinreichend genau beobachten kann (Beweisthemen der dritten Aussagekategorie) (zu den verschiedenen Aussagekategorien des Sachverständigen sogleich, B. II. 3. d))?[304]

Hilfreich in Bezug auf die Feststellung, wann die Grenze der eigenen Sachkunde zur Beantwortung der Beweisfrage erreicht ist, ist die Aneignung elementaren Grundwissens aus der jeweiligen forensischen Disziplin. Wenn die Strafverfolgungsbehörden und Gerichte (mithilfe dieses interdisziplinären Grundwissens) in der Lage sind, genau abschätzen zu können, was sie noch selbst entscheiden können und wo ihnen die Sachkunde dafür fehlt – also auch die nötigen Beweisfragen formulieren können (dazu ausführlich in B. II. 3. c)), die beantwortet werden sollen – hat der Auftraggeber die Zusammenarbeit mit dem IT-Sachverständigen und die jeweilige Ausgestaltung in der Hand und kann so eigenes Erfahrungswissen durch Fachwissen ergänzen und die Grenzen abstecken, in denen Fachwissen Berücksichtigung finden soll.[305]

---

302 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 60, 309 ff.

303 Vertiefend zu der Frage im Hinblick auf den (damaligen) psychologischen, psychiatrischen Sachverständigen vgl. *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 35 f.

304 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 319.

305 So auch Vertreter in Bezug auf den „Kompetenzverlust" bzw. „-verzicht" der Richter, vgl. *Haddenbrock*, DRiZ 1974, S. 38; *Leferenz*, Richter und Sachverständige, S. 8 f.; *Witter*, Beurteilung Erwachsener, S. 186; *Walter*, Sachverständigenbeweis, S. 120; *Gerchow*, in: FS-Weinig, S. 50.

b) Die möglichen Auftraggeber

Erstaunlich deutlich bestimmt § 73 StPO, dass im gerichtlichen Verfahren die Sachverständigenauswahl und -bestellung gemäß § 73 Abs. 1 S. 1 StPO durch das erkennende Gericht erfolgt.[306] Umso erstaunlicher ist es, dass die Praxis ganz anders aussieht.[307]

In den allermeisten Fällen bestellt die Staatsanwaltschaft schon im Ermittlungsverfahren einen Sachverständigen gem. § 161a Abs. 1 S. 2 StPO i. V. m. § 73 Abs. 1 StPO[308], um aus dessen Untersuchungsergebnissen ihre weiteren Entschließungen abzuleiten.[309] Dem Verteidiger soll Gelegenheit gegeben werden, zu der Auswahlentscheidung Stellung zu nehmen; hiervon kann dann abgesehen werden, wenn im Einzel fall ausnahmsweise eine erhebliche Verzögerung des Verfahrens zu befürchten ist.[310]

Dass der Staatsanwaltschaft die prozessuale Möglichkeit der Sachverständigenbestellung zukommt, ist ihrer Verfahrensstellung als überparteilichem Organ der Rechtspflege geschuldet.[311] Allerdings bleibt der Richter (theoretisch) nicht an diese Auswahl gebunden.[312] Gleichwohl ist es (praktisch) so, dass die Entscheidung des Staatsanwalts über die Person des Sachverständigen Einfluss auf das gesamte Verfahren nimmt, da das Gericht in den überwiegenden Fällen keinen neuen Sachverständigen im Hauptverfahren gem.

---

306 Nach überwiegender, aber umstrittener Auffassung bezieht sich § 73 Abs. 1 StPO ausschließlich auf das gerichtliche Verfahren, vgl. KK/*Senge*, § 73 Rn. 1; Löwe/Rosenberg/*Krause*, § 73 Rn. 2; SK-StPO/*Rogall*, Vor § 72 Rn. 26 f.; Meyer-Goßner/*Schmitt*, § 73 Rn. 1a; *Pfeiffer*, Strafprozessordnung, § 73 Rn. 1; AK/*Wassermann*, § 73 Rn. 4; Beck-OK-StPO/*Monka*, § 73 Rn. 1; *Eisenberg*, Beweisrecht der StPO, Rn. 1527; *Hellmann*, Strafprozessrecht, Rn. 741; *Schlüchter*, Das Strafverfahren, Rn. 526; *Ulrich*, Der Gerichtliche Sachverständige, Rn. 149 f.; *Detter*, NStZ 1998, 57 (59); *Kube/Leineweber*, Polizeibeamte als Zeugen und Sachverständige, S. 97; *Gössel*, DRiZ 1980, 363 (366); *Tröndle*, JZ 1969, 374 (375); *Lürken*, NJW 1968, 1161 f.; a. A. BGH NStZ 2003, 375, 376 Anm. Duttge m. w. N.; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S: 82 ff.; *ders*., in: FS-E. Müller, S. 125 (133 ff.); *E. Müller*, in: FS-Lüke, S. 493 (500 f.); *Dierlamm*, in: FS-Müller, S. 117 ff.; *Kühne*, Strafprozessrecht, Rn. 862; *Sarstedt*, NJW 1968, 177; kritisch: *Krauß*, ZStW 85 (1973), 320 (324).

307 Das stellte bereits *Walter*, Sachverständigenbeweis, S. 113 vor fast 50 Jahren fest; vgl. auch *Sarstedt*, NJW 1968, 177.

308 Zur Verfassungsmäßigkeit des § 161a StPO als entsprechender Ermächtigungsgrundlage BVerfG v. 31.8.2007 – 2 BvR 1681/07, BeckRS 2007, 26565.

309 Vgl. MüKoStPO/*Trück*, 1. Auflage, § 73 Rn. 4, 6. Zur Bestellung von Sachverständigen durch die Polizei: KK/*Griesbaum*, 8. Aufl. § 163 Rn. 16; *Stinshoff*, Operative Fallanalyse, S. 120.

310 *Wenzel*, NZWiSt 2016, 85 (87).

311 MüKoStPO/*Trück*, 1. Auflage, § 73 Rn. 1. Vgl. ferner zur Überparteilichkeit der Staatsanwaltschaft die Anm. in *Volkmann/Vogel*, StV 2021, 537.

312 BGH v. 12.2.1998 – 1 StR 588/97, NStZ 1998, 422; *Detter*, NStZ 1998, 57.

§ 73 StPO bestellt.[313] Dieser Bestellungspraxis kommt für den Ausgang des Verfahrens eine überragende Bedeutung zu: Empirische Studien zeigen, dass bis zu 97 Prozent der Richter dem Gutachtenergebnis des (gerichtlich beauftragten) Sachverständigen folgen.[314] Diese Bestellungspraxis kann mit dem sog. Schulterschlusseffekt erklärt werden. Damit gemeint ist eine Orientierung des Gerichts an von der Staatsanwaltschaft abgegebenen Beurteilungen sowie allgemein eine ganz unbewusste – auch „auf Grund gleicher beruflicher Sozialisation und Zielattributierung"[315] entstehende – Verquickung zwischen Gericht und Staatsanwaltschaft.[316] Man könnte auch von einem Vertrauen in die staatsanwaltschaftliche Auswahl sprechen. Darüber hinaus hat sich die Bestätigung des von der Staatsanwaltschaft bestellten Sachverständigen aber v. a. deshalb bewährt, weil Verfahren ansonsten erheblich verzögert, Kosten steigen sowie besonders gute Sachverständige für die Hauptverhandlung verloren gehen würden.[317] Die frühe Einbindung von Sachverständigen bereits im Ermittlungsverfahren hat zudem weitere Vorteile: Ermittler verfügen oft nicht über hinreichendes Verständnis von digitalen Systemen, um einschätzen zu können, wo und in welcher Form sich die gesuchten digitalen Spuren auf den sichergestellten physischen Beweismitteln vermeintlich befinden. Deshalb kann es vorkommen, dass digitale Spuren nicht gefunden werden, weil sie aus dem vom Ermittler festgelegten Raster fallen.[318] Das kann durch eine enge Zusammenarbeit zwischen Forensikerinnen und Strafverfolgungsbehörden bei der Sicherung, Erhebung und Aufbereitung digitaler Spuren vermieden werden.[319] Nur so kann sich bspw. die Möglichkeit der Hilfestellung durch die IT-Expertin ergeben bei der Entscheidung über das Vorgehen bei der Beschlagnahme, indem sie eine fachliche Einschätzung der Chancen und Ri-

313 BeckOK-StPO/*Sackreuther*, 39. Aufl., § 161a Rn. 11; KK/*Griessbaum*, 8. Aufl., § 163 Rn. 18.

314 *Gercke/Leimenstoll/Stirner*, Hdb. Medizinstrafrecht, Rn. 1629 m. w. N.; vertiefend dazu auch *Vogel/Volkmann*, GesR 2021, 753 (754).

315 *Schünemann*, ZIS 2009, 484 (494).

316 Vertiefend dazu *Vogel/Volkmann*, GesR 2021, 753 (754).

317 Vgl. insb. *Jessnitzer/Frieling*, Sachverständiger, Rn. 181; *Karpinski*, NJW 1968, 1173; *Kohlhaas*, NJW 1962, 1329 (1331).

318 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 344 f.

319 Das bestätigen auch Projekte und Studien aus anderen Ländern: Die Erfahrung aus einem Projekt im Osloer Polizeidistrikt war, dass eine enge Zusammenarbeit zwischen den IT-Forensikern und dem taktischen Ermittlungsteam zu erhöhter Motivation, Wissensaustausch und effizienter Kommunikation bei der Untersuchung von Sexualverbrechen gegen Kinder führte. In Finnland wurde die enge Zusammenarbeit als Erfolgsfaktor für eine kosteneffiziente Untersuchung von Computerintegritätsdelikten hervorgehoben, vgl. *Sunde/Dror*, Digital Investigation (2019) Vol. 29, S. 101 (104) m. w. N.

siken (wie Datenverlust oder unbeabsichtigte Manipulationen[320]) einer körperlichen Beschlagnahme bzw. einer logischen Sicherung vor Ort abgeben kann. Weiter kann eine gezieltere Auswertung der sichergestellten Geräte erfolgen, da vor Ort bereits digitale Spuren selektiert werden können.[321] Besonders bei Firmendurchsuchungen wird aufgrund des immensen Aufwands meist nur eine Teilsicherung der verfügbaren Daten durchgeführt. Durch eine frühe Einbindung kann weiter die Kommunikation zwischen Auftraggeber und Sachverständiger verbessert und dahingehend konkretisiert werden, was wirklich gewollt ist. Diese Präferenz der Bestellungspraxis bestätigen auch die Praktikerinnen.[322] Dabei sind jedoch stets die Grenzen zwischen Sachverständigen- und Zeugenbeweis (wenn der Forensiker als Ermittlungsperson tätig wird, siehe B. III. 2. b)) und ein mglw. begründetes Ablehnungsrecht (siehe B. V. 2. c)) zu beachten, wenn die Ergebnisse in die Hauptverhandlung eingeführt werden sollen.

Die Bestellung kann im Ermittlungsverfahren aber auch durch den Ermittlungsrichter erfolgen, allerdings nur in den Fällen der §§ 165, 166 StPO oder auf Antrag der Staatsanwaltschaft, vgl. § 162 StPO.[323]

---

320 So berichtet Johannes Pollach, M. Sc. von der ZCB, dass aufgrund einer Vielzahl von antiforensischen Techniken die Gefahr groß sei, dass der Verdächtige z. B. mit verschlüsselten Containern/Dateien verfahrensrelevante Informationen verstecken könnte. Vgl. *Dewald/Freiling*, Forensische Informatik, S. 345.

321 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 345, S. 349: Nicht zu vernachlässigen ist das Problem der technischen Grenzen der Verarbeitung zunehmender Datenmengen. Bspw. dauert das bitweise Sichern einer einzelnen 3-Terabyte-Festplatte mit aktuellen Technologien etwa 1,5 h. Wenn nun (wie in Unternehmen häufig üblich) hunderte Terabyte sichergestellt werden, wird das zum Problem. Andererseits wird von Praktikern angemerkt, dass eine umfassende Sicherung aus forensischer Sicht die Chance der effizienten Aufklärung des Tathergangs steigern würde. Als Beispiel wurde genannt, dass moderne Systeme meistens mit Verschlüsselungen und Zugriffsperren vor unbefugtem Zugriff geschützt sind. Mithilfe von älteren sichergestellten Asservaten/Daten könnten möglicherweise bereits verwendete Passwörter oder Informationen über die Zusammensetzung der Passwörter in Erfahrung gebracht werden, da bei älteren Geräten die Schutzmechanismen meistens leichter zu umgehen sind. Mit diesem Wissen wird die Wahrscheinlichkeit markant erhöht ein aktuelles Gerät erfolgreich zu entschlüsseln. Das spreche jedenfalls für eine großzügigere prozessuale Beschlagnahme der Geräte der verdächtigten Person. Trotz der umfangreichen Sicherstellungen wird bei jedem Asservat in der Praxis eine Abwägung stattfinden müssen, welchen Nutzen es für das jeweilige Verfahren hat und welcher Aufwand damit verbunden ist.

322 Vgl. *Sunde*, Non-technical Sources of Errors S. 58.

323 SK-StPO/*Rogall*, § 73 Rn. 10; OLG Düsseldorf 29.4.1999 JMinBl NRW 99, 270: Bei molekulargenetischen Untersuchungen erfolgt die Benennung des Gutachters gem. § 81 f Abs. 1 S. 2 StPO durch den Ermittlungsrichter, wenn die betroffene Person nicht schriftlich eingewilligt hat und keine Gefahr im Verzug besteht.

Auch Behörden und Beamte des Polizeidienstes können, unter Leitung der Staatsanwaltschaft, im Ermittlungsverfahren einen Sachverständigen hinzuziehen, vgl. §§ 161a Abs. 1, 163 Abs. 1 S. 1, Abs. 3 S. 2 StPO. Eine Gutachtenerstattung kann hier jedoch nur aufgrund von Freiwilligkeit erfolgen. Eine gesetzliche Pflicht eines Sachverständigen zur Gutachtenerstattung besteht nur gegenüber dem Richter oder der Staatsanwaltschaft, nicht aber gegenüber der Polizei oder den Ermittlungspersonen der Staatsanwaltschaft.[324] Man könnte daran denken eine Gutachtenerstattungspflicht gegebenenfalls aus der Pflicht zur Leistung von Rechts- und Amtshilfe aus Art. 35 Abs. 1 GG abzuleiten, wenn der Sachverständige Amtsträger einer öffentlich-rechtlichen Körperschaft ist.[325] Allerdings begründet diese Vorschrift ein „Wohlwollensgebot", wodurch sich auch hier keine unbedingte Gutachtenerstattungspflicht ergibt.[326]

Übrige Verfahrensbeteiligte, etwa die beschuldigte Person oder ein Nebenkläger, sollen keine prozessuale Möglichkeit haben, einen Sachverständigen „kraft behördlichen Auftrags" zu bestellen.[327] Das ergebe sich aus einem Umkehrschluss: Diese Verfahrensbeteiligten seien parteilich; eine „neutrale" Sachverhaltsaufklärung sei deshalb nicht sichergestellt.[328] Die Verteidigung hat generell das Recht Stellung zur Auswahl zu nehmen, jedoch erschöpft sich hier die Möglichkeit ihrer Einflussnahme im Ermittlungsverfahren. Der Angeklagte kann die Vernehmung eines Sachverständigen im Hauptverfahren ausschließlich durch unmittelbare Ladung aus §§ 220, 245 Abs. 2 StPO bewirken.[329] In den meisten Fällen wird bspw. die Einholung eines weiteren (privaten) Sachverständigengutachten notwendig sein, um so substantiierte Einwendungen gegen das bereits geleistete (aber fragwürdige) gerichtliche Sachverständigengutachten geltend zu machen i. S. d. § 244 Abs. 4 StPO.[330] Eine unmittelbare Ladung durch die Prozessbeteiligten oder die Stellung eines Beweisantrags führen jedoch noch nicht zur Eigenschaft einer Person als

---

[324] SK-StPO/*Rogall*, § 75 Rn. 4; Löwe/Rosenberg/*Krause*, § 75 Rn. 1; KK/*Senge*, § 75 Rn. 1; Meyer-Goßner/*Schmitt*, § 75 Rn. 1; *Kühne*, Strafprozessrecht, Rn. 863.

[325] Löwe/Rosenberg/*Krause*, § 75 Rn. 1; *Roxin/Schünemann*, § 27 Rn. 13.

[326] SK-StPO/*Rogall*, § 83 Rn. 17, § 75 Rn. 3; *Ulrich*, Der Gerichtliche Sachverständige, Rn. 178.

[327] Zu berücksichtigen sind insoweit allerdings die Möglichkeit des Privatgutachtens, das Beweisantragsrecht und das Selbstladungladungsrecht.

[328] Insbesondere soll dem Angeklagten nicht die Möglichkeit gegeben werden „nur den Sachverständigen seines Vertrauens […] bestellen zu lassen" und so § 73 StPO bzw. § 244 Abs. 2 und 3 StPO zu unterlaufen, BGH v. 12.2.1998 – 1 StR 588/97, NStZ 1998, 422 (425).

[329] *Eisenberg*, Beweisrecht der StPO, Rn. 1527a; SK-StPO/*Rogall*, § 73 Rn. 16; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 60 ff.

[330] *Mysegades*, Software als Beweiswerkzeug, S. 160 m. w. N.

Zeuge oder Sachverständiger. Es handelt sich um sog. Erwirkungshandlungen.[331] Es bedarf also noch einem Akt der Zulassung durch das Gericht (wobei es dazu in weitem Umfang verpflichtet sein wird)[332], damit die Auskunftsperson die durch die Selbstladung intendierte Stellung des Sachverständigen erlangt, vgl. § 73 Abs. 1 S. 1 StPO. Wird ein Beweisantrag gestellt, darf das Gericht ihn zwar nur unter den Voraussetzungen der §§ 244 Abs. 4, 245 Abs. 2 S. 2 und 3 StPO ablehnen; in der Entscheidung, welche Person es zum Sachverständigen ernennt, ist es jedoch nach der h. M.[333] frei. In der Praxis scheitert die Möglichkeit eines Privatgutachters der Verteidigung häufig an den fehlenden finanziellen Möglichkeiten des Angeklagten[334] und daran, dass die potenziellen Sachverständigen häufig nicht als „Sachverständige der Verteidigung" auftreten möchten, da sie ihre Unparteilichkeit nicht gefährden wollen;[335] eine Besorgnis, die die Gerichte teilweise durch ihre Verhandlungsleitung verstärken.[336]. Liegen allerdings privatsachverständige Einwendungen vor, muss das Gericht sich mit diesen im Detail auseinandersetzen.[337]

---

331 SK-StPO/*Rogall*, § 72 Rn. 31; vertiefend zum Begriff und der Lehre von Prozesshandlungen vgl. auch *Eb. Schmidt*, I, Rn. 213 ff.; *Stinshoff*, Operative Fallanalyse, S. 119 f.

332 Vgl. *Perron*, Das Beweisantragsrecht des Beschuldigten im deutschen Strafprozess, S. 271 ff.

333 Vgl. nur SK-StPO/*Rogall*, Vor § 72 Rn. 31; § 73 Rn. 16, 22, m. w. N.; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 366; *Hanack*, JZ 1970, 561 (564); Löwe/Rosenberg/*Becker*, § 244 Rn. 145 m. w. N.; *Hamm*, Die Revision in Strafsachen, Rn. 611; *Sarstedt*, NJW 1968, 177 ff.; *Schäfer*, Die Praxis des Strafverfahrens, Rn. 1171, 1176; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 345 ff. mit der Einschränkung, dass eine vorherige Anhörung der Beteiligten stattfinden müsse; vgl. auch SK-StPO/*Frister*, § 244 Rn. 52; BGHSt 34, 355, 357; BGH StV 1999, 463 m. Anm. Grabow und Zieschang = NJW 1998, 2458; a. A. *Schulz*, StV 1983, 341; *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 256 ff.; *Detter*, in: FS-Meyer-Goßner, S. 431 ff.; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 59 ff.

334 *Detter*, in: FS-Meyer-Goßner, S. 431, 442; *ders*. NStZ 1998, 57, 61; *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 332 ff.; *Lürken*, NJW 1968, 1161 (1163); *Sarstedt*, NJW 1968, 177, 178.

335 MAH/*Deckers*, § 81 Rn. 17; *Rasch/Jungfer*, StV 1999, 513; *Detter*, NStZ 1998, 57, 61.

336 Vgl. MAH/*Deckers*, § 81 Rn. 17; BGH StV 1999, 463 m. Anm. Grabow und Zieschang = NJW 1998, 2458.

337 *Mysegades*, Software als Beweiswerkzeug, S. 161 m. w. N.

c) Die Auswahl

Die Auswahl der Person des Sachverständigen durch den Richter gem. § 73 StPO erfolgt nach freiem, pflichtgemäßem Ermessen.[338] Für die Staatsanwaltschaft gilt Nr. 70, 72 Abs. 4 RiStBV entsprechend.[339] Schon bei der Auswahl hat der Auftraggeber zweckmäßigerweise Zweifel an der Eignung des Sachverständigen ernst zu nehmen und zu prüfen, ob ggf. jemand Anderes zu beauftragen ist.

aa) Der Sachverständigenpool

§ 75 StPO Abs. 1 StPO verpflichtet nicht einfach einen bestimmten Personenkreis, sondern knüpft an die berufliche Beziehung „zur Erstattung von Gutachten der erforderten Art" an, d. h. zu dem bestimmten, im Prozess tangierten Wissenschaftszweig.[340] Es gibt also Expertinnen aus verschiedensten Fachgebieten, die in einem Strafverfahren als Sachverständige auftreten können, wie etwa Expertinnen der Psychiatrie, Daktyloskopie oder Wirtschaftsstrafsachen etc. In Bezug auf die Erstattung von Gutachten zu Beweisfragen über digitale Spuren (siehe mögliche Fragestellungen bei B. II. 3. c)), kommen die Expertinnen aus dem Wissenschaftszweig der IT, bspw. aus Bereichen der Informatik, der Software-Entwicklung, der IT-Sicherheit oder der Netzwerk- und Elektrotechnik.

Abgesehen von der jeweiligen Spezialisierung gibt es eine weitere Variation: So gibt es bspw. öffentlich bestellte und allgemein vereidigte Sachverständige,[341] amtlich anerkannte Sachverständige (für die technische Überwachung), angestellte oder freiberufliche Sachverständige in einer Sachverständigenorganisation, „freie" Sachverständige (= private oder selbsternannte), Behörden und deren Mitarbeiter als Sachverständige, ermächtigte Sachverständige (z. B. durch Berufsgenossenschaften, Bergbehörden), oder Wissenschaftler von Universitäten (wegen der besonderen Sachkunde auf einzelnen Forschungsgebieten). Diese Unterschiede finden sich auch unter den IT-Expertinnen, die in einem Strafverfahren auftreten: „Cyberkriminalistinnen" der Polizeibehörden, bei der Staatsanwaltschaft angesiedelte IT-Sachverständige, öffentlich bestellte und vereidigte[342] bzw. „einfache" Sachverstän-

338 Die Entscheidung ist jedoch nicht mittels Beschwerde anfechtbar, § 305 StPO, weil es sich um eine instruktionelle Vorschrift handelt, Löwe/Rosenberg/*Krause*, § 73 Rn. 22; KK/*Senge*, § 73 Rn. 6; *Ulrich*, Der Gerichtliche Sachverständige, Rn. 162.

339 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 247.

340 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 362.

341 https://svv.ihk.de/ [26.6.2023].

342 Hier findet sich eine Übersicht: https://svv.ihk.de/svw-suche/4931566/suche-extern [26.6.2023].

dige[343] oder private Sachverständigenbüros[344], die (teilweise) zertifiziert sind[345]. Aus § 76 Abs. 2 StPO und im Umkehrschluss aus § 74 Abs. 1 i. V. m. § 22 Nr. 4 StPO ergibt sich, dass auch Angehörige von Strafverfolgungsorganen grds. Sachverständige sein können, vgl. auch Nr. 70 Abs. 4, 66 RiStBV.[346] Das wird v. a. an späterer Stelle bei der Abgrenzung zwischen IT-Sachverständigen und Ermittlungspersonen relevant (B. III. 2. b)).

Wie aber finden die Strafgerichte in dem jeweiligen „Sachverständigenpool“[347] des ausgemachten Fachbereichs den Passenden für die zu beantwortenden Beweisfragen?[348]

Der Gesetzgeber hat als „erste Hilfe“ den öffentlich bestellten und vereidigten Sachverständigen[349] geschaffen (siehe § 132a Abs. 1 Nr. 3 StGB) und diesen Sachverständigentyp in gerichtlichen Verfahren favorisiert, vgl. § 73 Abs. 2 StPO.[350] Zu einem öffentlich bestellten und allgemein vereidigten Sachverständigen kommt man i. d. R. über die Industrie- und Handelskammer oder eine Handwerkskammer.[351] Diese Bestellungskörperschaften regeln in ihren Satzungen (i. V. m. §§ 36 und 36a GewO) die Voraussetzungen für den Erwerb eines solchen Titels. Die öffentliche Bestellung soll angeben, dass die Person zuverlässig und fachlich qualifiziert ist.[352] Aufgrund von bundes- oder

---

343 Auch hier findet man eine Übersicht: Bundesverband IT-Sachverständiger und Gutachter (BVDSG), https://www.bisg-ev.de/sachverstaendige-und-gutachter [26.6.2023]; Bundesverband Deutscher Sachverständiger und Fachgutachter (BDSF) https://www.bundesverband-gutachter.de/ [26.6.2023].

344 Nur um einige Beispiele zu nennen: https://www.fast-detect.de/; https://www.maax-forensik.de/ [26.6.2023]; https://www.digforit.de/ [26.6.2023]; https://www.comfor-it.de/ [26.6.2023]; https://www.forensik.it/ [26.6.2023]; GRIGA luK Auswertung GmbH.

345 Bspw. ISO-Zertifizierungen, vgl. ISO 9001 oder ISO 27001 wie etwa Fast Detect, https://www.fast-detect.de/ueber-uns/qualitaet-sicherheit/qualitaetsmanagement/ [15.1.2024].

346 Vertiefend dazu auch *Wenzel*, NZWiSt 2016, 85; sowie *Rogall*, in: FS Gössel, S. 511 f.; *Gössel*, DRiZ 1980, S. 363 f.

347 Vgl. *Stinshoff*, Operative Fallanalyse, S. 126.

348 Jedenfalls nicht indem man nach dem höchsten Schmiergeld Ausschau hält, vgl. erst kürzlich das Urteil des Frankfurter Landgerichts (LG Frankfurt a. M., Urt. v. 12.5.2023) das den früheren Oberstaatsanwalt zu sechs Jahren Haft u. a. wegen Bestechlichkeit verurteilte. Der Verurteilte hat eine Firma gegründet, die Sachverständige an Justizbehörden vermittelte, wobei er heimlich an den Gewinnen beteiligt gewesen sein soll.

349 Vertiefend dazu siehe *Hoppen/Streitz*, CR 2007 Heft 4, S. 270 ff.

350 Bspw. „Sollvorschrift“ aus § 404 Abs. 2 ZPO. Kritisch dazu siehe *Bleutge*, Sachverständigenrecht, S. 11.

351 Vgl. https://svv.ihk.de/svw-suche/4931566/suche-extern [26.6.2023].

352 Vgl. nur Löwe/Rosenberg/*Krause*, § 73 Rn. 22; *Ulrich*, Der gerichtliche Sachverständige, Rn. 162; *Rogall*, in: FS-Gössel, S. 511 (512 Fn. 6).

landesrechtlichen Vorschriften sind sie auf bestimmte Zeit für gewisse Fachgebiete bestellt (wie bspw. Gerichtsärzte).[353] So gilt zwar die öffentliche Bestellung als Indiz für eine persönliche und fachliche Eignung als Sachverständiger, jedoch hat das erkennende Gericht die Eignung individuell zu überprüfen.[354] Allerdings handelt es sich bei § 73 Abs. 2 StPO lediglich um eine Sollvorschrift und nicht alle Fachbereiche vermögen diesen Prozess zu leisten bzw. kennen ihn überhaupt.[355] Aufgrund der o. g. Besonderheit der Universalität der Technologie und der dadurch bedingten vielen Spezialbereiche der forensischen Informatik (bspw. Datenträgerforensik, Cloudforensik, Multimediaforensik, AI, etc.) sind in vielen Fällen weder im Ermittlungs- noch im Hauptverfahren öffentlich bestellte Sachverständige verfügbar. Das Problem besteht insbesondere, da die Industrie- und Handelskammer keinen Bedarf für die Zulassung von Sachverständigen in besonderen Spezialbereichen sieht.[356] Das ist gerade in Bezug auf die neuen Möglichkeiten in der Informationstechnik unhaltbar.[357] Nach öffentlich bestellten IT-Sachverständigen für die zu beantwortenden Beweisfragen zu suchen, bringt (Stand jetzt) oft wenig.

Hilft googlen? Auch schwierig: Das Sachverständigenwesen wird nur eher noch undurchsichtiger, wenn man die verschiedenen Qualifikationshinweise der werbenden Sachverständigen untersucht. Es gibt verbandsanerkannte, zertifizierte und geprüfte Sachverständige, TÜV-Sachverständige, Dekra-Sachverständige, Wertermittler (IHK) usw.[358] Ohne dabei den jeweiligen Grad der Qualifikation absprechen zu wollen, fehlt es jedoch an Transparenz, welchen (sonstigen) Qualifikationen man überhaupt noch Vertrauen schenken kann und welchen nicht.[359] So erlauben es die europäischen Normen zur Zertifizierung von Sachverständigen bspw., dass sie in Deutschland von jedermann benutzt werden können und die einzelnen Qualitätsmerkmale von den Nutzern selbst vorgegeben werden.[360] Das hat am Sachverständigenmarkt zu

---

353 Löwe/Rosenberg/*Krause*, § 73 Rn. 22; *Eisenberg*, Beweisrecht der StPO, Rn. 1530.

354 *Eisenberg*, Beweisrecht der StPO, Rn. 1530; *Müller*, Der Sachverständige im gerichtlichen Verfahren, Rn. 177.

355 Beispielsweise sind von den 8.000 Kfz-Sachverständigen nur 800 öffentlich bestellt. Der gesamte medizinische Bereich kennt den öffentlich bestellten Sachverständigen gar nicht, weil der Gesetzgeber hierfür keine Rechtsgrundlagen geschaffen hat, sodass dort keine fachliche Überprüfung und Vereidigung nach dem Vorbild des § 36 GewO stattfinden, vgl. *Bleutge*, Sachverständigenrecht, S. 11.

356 Vgl. auch *Farthofer*, HRRS 2021, 313 (314).

357 Siehe etwa VG Osnabrück (2. Kammer) 2 A 80/17, Urteil v. 18. Januar 2018 = GewA 2018, 197 (Anm. Dr. Peter Bleutge) = BeckRS 2018, 7876, Rn. 16.

358 Bspw. Zertifizierung nach ISO 27001 und ISO 9001 (vgl. etwa „Fast Detect“).

359 *Bleutge*, Sachverständigenrecht, S. 11.

360 *Bleutge*, Sachverständigenrecht, S. 12.

teilweise chaotischen Verhältnissen geführt. So gibt es einerseits Zertifizierungen für Sachverständige, die lediglich einen kurzen Lehrgang von drei Wochenenden oder ein einziges Seminar zur Voraussetzung haben und auf der anderen Seite (z. B. in der Kinder- und Jugendpsychiatrie) Zertifizierungen, die strenge Zugangsvoraussetzungen haben, eine lang dauernde Ausbildung fordern und eine Befristung mit erneuter Zertifizierung vorsehen. Um die Verwirrung zu verstärken: Das Normensystem kennt Zertifizierungen, die lediglich ein selbst geschaffenes Qualitätsmanagement zum Gegenstand haben (DINEN ISO 9001), die sog. Bürozertifizierung, und solche, die als sog. Personenzertifizierung die persönliche Eignung und fachliche Qualifikation eines Sachverständigen durch eine nach DINEN ISO/IEC 17024 akkreditierte Zertifizierungsstelle prüfen und ihn ständig überwachen. Alle Sachverständigen bezeichnen sich am Gutachtenmarkt als „zertifizierte" Sachverständige.[361] Es gilt also die entsprechenden Zertifizierungen und Qualifizierungen genau zu hinterfragen.

Besonders hilfreich bei der Suche nach und der Auswahl eines Sachverständigen ist bspw. die auf der vom Bundesministerium für Justiz zur Verfügung gestellten Website veröffentlichte Liste der Gerichtssachverständigen in Österreich[362] – es wäre wünschenswert das auch für Deutschland zu etablieren.

Durch die o. g. Definition wird deutlich, dass bei IT-Sachverständigen kein bestimmtes „Kompetenzniveau" verlangt wird, weder in Bezug auf die technische noch auf die investigative Kompetenz.[363]

Die Qualität der Experten muss sich – abgesehen vom konkreten Einzelfall und der jeweiligen Beweisfrage – v. a. dahingehend erweisen, zu erkennen, welche digitalen Spuren wertvoll für den Fall sind, welche interdisziplinären Fragen zu stellen sind, und beurteilen zu können, welchen Beweiswert die Informationen tatsächlich haben, die aus den Daten gewonnen werden konnten. Zu beachten ist, dass eine mangelnde Qualität der Experten das Risiko erhöht, dass einerseits der Beweiswert des Sachverständigengutachtens sinkt

---

361 *Bleutge*, Sachverständigenrecht, S. 13: Forderung, dass der Gesetzgeber die Zertifizierung von Sachverständigen einem bundeseinheitlichen Gesetzesregime unterwirft, wie er das bei der hoheitlichen Prüftätigkeit von zertifizierten Sachverständigen in vielen Bereichen bereits getan hat. Vorgeschlagen wird, dass die Zertifizierung von Sachverständigen dem § 36 GewO zugeordnet wird, indem man die öffentliche Bestellung zu einer öffentlichen Zertifizierung umfunktioniert. (Vorbild: VersteigererVO).

362 http://www.sdgliste.justiz.gv.at/edikte/sv/svliste.nsf/suche [26.6.2023]; Der Bereich der Informationstechnik ist in vierzehn Untergruppen geteilt in österreichischen Gerichtslisten, https://sdgliste.justiz.gv.at/edikte/sv/svliste.nsf/Suche?OpenForm&subf=svlfg&vL2obSVF=68&NAV=68&L1=Informationstechnik [15.1.2024].

363 Zu diesem Ergebnis kommt auch *Sunde*, Non-technical Sources of Errors, S. 39, die eine Studie zu IT-Experten im Strafverfahren in Norwegen durchführte.

und andererseits eine Urteilsfindung auf einer falschen Tatsachengrundlage beruhen kann.[364]

Letztlich könnte durch Transparenz im gerichtlichen Auswahlverfahren das Vertrauen in die Unabhängigkeit und Neutralität der IT-Sachverständigen erhöht und sichergestellt werden, dass die Strafverfolgungsbehörden qualifizierte Sachverständige ernennen.[365]

bb) Die besondere Sachkunde

Das erkennende Gericht muss weiter entscheiden, aus welcher Fachrichtung es den Gutachter hinzuziehen will („fachliche Eignung"[366]).[367]

Die Heranziehung eines Sachverständigen, der das Fachgebiet bestimmen soll, für das ein Gutachten erstellt werden soll (sog. Auswahlsachverständige)[368] ist unzulässig.[369] Das Gericht muss selbst festlegen, wer fachlich als Sachverständiger geeignet ist und darf die Entscheidung nicht Dritten überlassen.[370]

Hinweise darüber, wer fachlich als Sachverständige in Frage kommt, finden sich in § 75 StPO. Die Vorschrift legt fest, wer der Ernennung zum Sachverständigen Folge zu leisten hat und definiert damit den Sachverständigenpool, aus welchem der Auftraggeber auswählen kann. Das sind diejenigen, die sich zur Gutachtenerstattung vor Gericht bereit erklärt haben, § 75 Abs. 2 StPO, und diejenigen, die die Wissenschaft, die Kunst oder das Gewerbe[371], deren Kenntnis Voraussetzung der Begutachtung ist, öffentlich zum Erwerb ausüben, § 75 Abs. 1 StPO. Daraus folgt, dass die besondere Sachkunde nicht nur wissenschaftlicher Art sein muss, sondern auch das besondere Wissen um die

---

364 So auch *Casey*, Digital Evidence and Computer Crime; *Mandia et al.*, Incident Response & Computer Forensics; *Garfinkel*, Digital Forensics Research: The Next 10 Years, DFRWS 2010.

365 So auch schon im Entwurf eines Gesetzes zur Änderung des Sachverständigenrechts und zur weiteren Änderung des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit, Drucksache 18/6985, 2015.

366 Vgl. dazu auch *Stinshoff*, Operative Fallanalyse, S. 125 f.

367 BGHSt 34, 355, 357; Meyer-Goßner/*Schmitt*, § 73 Rn. 5; im Ermittlungsverfahren gilt das auch für die Staatsanwaltschaft, § 161a StPO.

368 AwK-*Krekeler/Werner*, § 73 Rn. 3.

369 OLG Koblenz VRS 36, 17, 18; *Eisenberg*, Beweisrecht der StPO, Rn. 1531.

370 *Eisenberg*, Beweisrecht der StPO, Rn. 1536; AK/*Wassermann*, § 73 Rn. 7; KK/*Senge*, § 73 Rn. 6.

371 Der Begriff ist weit auszulegen und umfasst jede Tätigkeit in Industrie, Handel, Gewerbe oder einem freien Beruf, die gegenüber einem zahlenmäßig unbekannten Personenkreis zum Erwerb ausgeübt wird, vgl. nur Meyer-Goßner/*Schmitt*, § 75 Rn. 1; Löwe/Rosenberg/*Krause*, § 75 Rn. 3; SK-StPO/*Rogall*, § 75, Rn. 20.

Kunst oder das Gewerbe (also die „bloße Kunstfertigkeit“[372]) ein entsprechendes Expertenwissen sein kann. Deshalb können eben auch kaufmännische Gepflogenheiten Gegenstand des Sachverständigenbeweises sein.[373] Ein abgeschlossenes Studium ebenso wie eine besondere Ausbildung oder Prüfungen, die das Bestehen einer besonderen Sachkunde bestätigen würden, sind gerade nicht erforderlich. Ebenso müssen wissenschaftlich gesicherte Erkenntnisse nur dann gefordert werden, wenn sich die Sachkunde gerade aus der Anwendung wissenschaftlicher Methoden und Erkenntnissen herleiten soll.[374] Es wird deutlich, dass es keine bestimmten Zugangsvoraussetzungen für den Sachverständigenbeweis gibt.[375]

Wenn es z. B. um die Erstellung eines Glaubwürdigkeitsgutachtens geht, kann das Gericht frei entscheiden, ob es einen Psychologen oder einen Psychiater hinzuzieht.[376] Die Entscheidungsfreiheit wird allerdings durch faktische Voraussetzungen eingegrenzt. So besteht die Wahlmöglichkeit zwischen Psychologen und Psychiatern z. B. nur insoweit, als dass keine medizinischen Fachkenntnisse erforderlich sind, die ein Psychologe nicht besitzt.[377]

Die digitale Forensik hat ihre Wurzeln in der Informatik, der Physik (Elektronik) und der mathematischen Theorie. IT-Sachverständige müssen demnach eine „besondere – technologische – Sachkunde“ auf dem Gebiet der IT vorweisen, um die jeweiligen Beweisfragen beantworten zu können.

Der Begriff „Sachkunde“ setzt sich zusammen aus „Wissen“ und „Fertigkeit“ und ist gleichzusetzen mit „Expertise“. Ein Sachkundenachweis setzt stets eine (Über-)Prüfung voraus.[378]

„Wissen“ bezieht sich auf die theoretische Kompetenz. Der Begriff „Fertigkeit“ bezieht sich auf die kognitive oder physische Fähigkeit, eine Aufgabe mit vorher festgelegten Ergebnissen auszuführen. „Expertise“ ist gekennzeichnet durch „besondere Fähigkeiten, die nur einige Menschen besitzen, im

---

372 *Glaser*, Handbuch, S. 671, der für den Sachverständigen zutreffend eine Überlegenheit des Könnens und des Wissens fordert, die durch regelmäßige Beschäftigung mit den gleichen Gegenständen entsteht gegenüber denjenigen, die diese nicht innehaben.

373 Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 2.

374 Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 2.

375 Vgl. auch *Ulrich*, Der gerichtliche Sachverständige, Rn. 1.

376 BGHSt 23, 12; BGH StraFo 2003, 97 mit Anm. Salditt = BGHR StPO § 244 Abs. 4 S. 1 Sachkunde 12; SK-StPO/*Rogall*, Vor § 72 Rn. 23.

377 BGH StV 1993, 522; BGH StV 1995, 398; BGH StV 1997, 61 f.; BGH StV 1999, 471, 472; BGHStV 2002, 293; SK-StPO/*Rogall*, Vor § 72 Rn. 23; *Jansen*, Zeuge und Aussagepsychologie, Rn. 116.

378 Vgl. *Dror*, The paradox of human expertise: why experts can get it wrong, S. 177 f.

Gegensatz zu anderen, die keine Experten sind – den Novizen –, die nicht das Niveau von Experten erreichen können“[379]. Diese Definition ist recht allgemein, daher bezieht sich der Begriff „Sachkunde“ in dieser Arbeit auf die Kombination von Wissen und Fähigkeiten auf einem höheren Niveau aufgrund umfangreicher Erfahrung zusätzlich zu den anderen Komponenten.[380]

Die Unterscheidung zwischen den verschiedenen Niveaus der technologischen Sachkunde ist für die Abgrenzung der verschiedenen Prozessrollen relevant (B. III.). Deshalb soll im Folgenden kurz darauf eingegangen und der Unterschied zwischen „einfacher“ und „besonderer“ Sachkunde dargestellt werden.

Was ist unter „besonderer“ Sachkunde genau zu verstehen, auf die man in diesem Zusammenhang in Rspr.[381] und Literatur stößt?[382] Auch wenn man in der StPO keine Norm findet, die explizit von „besonderer“ Sachkunde spricht,[383] kann nach dem Sinn und Zweck des Sachverständigenbeweises eine „einfache“ Sachkunde gerade nicht ausreichen.[384] Die Bedeutung des Gutachtens für die Urteilsfindung und die Aufklärungspflicht aus § 244 Abs. 2 StPO sowie die Auswahlmöglichkeit aus § 73 StPO des erkennenden Gerichts fordern, dass dieses den möglichst „Fähigsten“ auf dem Gebiet zu bestimmen hat, diesem das fehlende Wissen zu vermitteln.[385]

Für die Bestimmung des „besonderen“ Fachwissens ist eine Abgrenzung von der „einfachen“ Fachkunde hilfreich. Die Grenzen sind oft fließend, weshalb eine Unterscheidung nicht immer einfach ist.[386] Dass das Gesetz aber eine Unterscheidung kennt, wird durch § 85 StPO deutlich.

---

379 Vgl. *Dror*, The paradox of human expertise: why experts can get it wrong, S. 177 f. m. w. N.

380 So auch *Sunde*, Non-technical Sources of Errors.

381 Vgl. nur BGH NJW 1955, 840, 841.

382 Vgl. *Mezger*, AcP 117 (1918), Beilageheft, 1, 3 f.; *Geerds*, ArchKrim (1966) Vol. 137, 61 (67); *Kerameus*, Die Entwicklung des Sachverständigenbeweises im deutschen und griechischen Zivilprozess, S. 1 ff.; *Boetticher/Nedopil/Bosinski/Saß*, NStZ 2005, 57; *Bleutge*, DS 2007, 65; vgl. auch *Detter*, NStZ 1998, 57 (59).

383 Lediglich § 85 StPO spricht von „besonderer“ Sachkunde, jedoch regelt er den Fall des Zeugenbeweises.

384 Vgl. *Stinshoff*, Operative Fallanalyse, S. 127 Fn. 1002 mit Verweis auf Art. 182 f. der schweizerischen sowie Art. 126 Abs. 1 der österreichischen Strafprozessordnung, in denen von „besonderen Kenntnissen und Fähigkeiten“ bzw. „besonderem Fachwissen“ die Rede ist.

385 Löwe/Rosenberg/*Krause*, § 73 Rn. 9; *Rogall*, in: FS-Gössel, S. 511.

386 *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 53; *Stinshoff*, Operative Fallanalyse, S. 128.

Die Richterin muss auf der Grundlage der ihr von der Beweisperson vermittelten Sachkunde selbstständig urteilen können.[387] Notwendig ist daher, dass dem Gericht der „bestmögliche Sachverstand für die Beantwortung von Beweisfragen" vermittelt wird. In diesem Zusammenhang muss die Richterin äußerst sorgfältig arbeiten, denn es können sich innerhalb eines Fachgebiets und der jeweiligen Untergebiete signifikante Unterschiede im Wissensstand in Bezug auf die konkrete Beweisfrage ergeben.[388] Für das Merkmal der „besonderen" Sachkunde kann es gerade nicht ausreichen, dass eine Person mehr Wissen hat als eine andere beliebige Person, wenn dieses z. B. dem allgemeinen Wissen ihres Berufsstandes entspricht.[389] Die Person, die zum Sachverständigen ernannt werden soll, muss sie auch gegenüber anderen ihres Berufsstands oder Wissens- und Erfahrungsstand haben und zwar auch innerhalb eines sehr speziellen Expertengebiets.[390] Denn ansonsten handelt es sich innerhalb dieser Expertengruppe wohl nur um „einfache" Sachkunde, auch wenn es sich für jeden anderen außerhalb um Expertenwissen handelt. Kommt es dem Gericht z. B. auf die Beurteilung einer bestimmten Operationsmethode an, muss es von den beiden Chirurgen denjenigen wählen, der die Methode entwickelt bzw. weitreichende Erfahrung damit hat.[391] Nicht speziell ausgebildete und entsprechend erfahrene Psychiaterinnen im Bereich der forensischen Psychiatrie als Sachverständige heranzuziehen[392] scheint jedoch in der Praxis durchaus üblich zu sein (wohl dem Mangel an Expertinnen geschuldet).[393] Auch wenn die Richterin grundsätzlich selbst und frei entscheiden darf, wen sie für am besten geeignet hält, ihr den Tatsachenstoff zu-

---

387 *Detter*, NStZ 1998, 57 (58).

388 Vgl. auch das Beispiel von *Stinshoff*, Operative Fallanalyse, S. 128 f.: Ein Facharzt für Chirurgie besitzt i. d. R. fundierteres Wissen zu bestimmten Operationen als ein Allgemeinmediziner. Wiederum hat ein forschender Chirurg, der eine bestimmte Operationsmethode entwickelt hat, mehr Wissen darüber als ein anderer Chirurg, der sich mit dieser Methode nicht beschäftigt hat. Dem Facharzt für Chirurgie ist also i. d. R. eine besondere Sachkunde gegenüber dem Allgemeinmediziner zuzusprechen und dem Spezialisten in der bestimmten Operationsmethode eine besondere Sachkunde gegenüber dem anderen Chirurgen.

389 Bayerlein-*Böttger*, § 1 Rn. 7 f.

390 Vgl. SK-StPO/*Rogall*, Vor § 72 Rn. 7; *Ulrich*, Der gerichtliche Sachverständige, Rn. 1; *Bremer*, Der Sachverständige, S. 21; *Bleutge*, NJW 1985, 1185 (1187); *Zimmermann*, DS 2006, 304 (307).

391 Vgl. auch *Mayer*, in: FS-Mezger, S. 455 (474), der ausführt, dass psychiatrische Untersuchungen Psychiatern vorbehalten sind, da Amtsärzte i. d. R. nicht die ausreichende Sachkunde haben. Die Ausführungen sind aber insofern nicht ausreichend, als nicht jeder Psychiater innerhalb dieser Fachgruppe die besondere Sachkunde für die Beantwortung der konkreten Beweisfrage haben muss, so jedenfalls *Stinshoff*, Operative Fallanalyse, S. 129 Fn. 1018.

392 *Stinshoff*, Operative Fallanalyse, S. 129 f.

393 Vgl. *Detter*, NStZ 1998, 57 (60 f.) m. w. N.

gänglich zu machen, darf sie sich nicht einfach auf einen ihr bekannten und bewährten Sachverständigen berufen, der auf dem Fachgebiet der konkreten Beweisfrage auch kundig ist.[394] Das ist für das Innehaben der „besonderen" Sachkunde nicht ausreichend. Wenn sich ergibt, dass nur eine einzige Person die erforderliche besondere Sachkunde aufweist und diese Person nicht zur Gutachtenerstattung verpflichtet ist gem. § 75 StPO, kann es eben sein, dass die besondere Sachkunde für den Prozess nicht eingeholt werden kann.[395]

Zusammenfassend ist festzuhalten, dass man als Teil besonderer Sachkunde den Besitz spezieller Kenntnisse aufgrund besonderer wissenschaftlicher, künstlerischer, technischer oder gewerblicher Ausbildung und Tätigkeit oder Lebenserfahrung verstehen kann. Hinzukommen besondere Geschicklichkeit sowie Fähigkeiten, die ebenfalls durch spezielle Ausbildung, Tätigkeit und Lebenserfahrung gewonnen werden können.[396] Diese Fähigkeiten müssen allerdings besonders trainiert worden sein. Ein Anlesen oder lediglich rudimentäre Kenntnisse können für eine besondere Sachkunde gerade nicht ausreichen.[397]

Das Vorliegen dieser Sachkunde hat das Gericht vor der Auswahl genauestens zu prüfen.[398] Dabei handelt es sich um eine Prognoseentscheidung,[399] denn das Gericht bestimmt die jeweilige Person lediglich in der Annahme zum Sachverständigen, dass sie die benötigte Sachkunde besitzt.[400] Ob die Person in Bezug auf das konkrete Beweisthema tatsächlich die erforderliche besondere Sachkunde besitzt, wird sich erst bei der Gutachtenerstattung zeigen oder wenn der Sachverständige bei der Ernennung selbst darauf hinweist, dass ihm diese, ggf. auch teilweise, fehlt.[401]

---

394 Im Jahr 1986 ergab eine Studie, dass 76 % der Richter und Staatsanwälte ortsansässige Sachverständige bevorzugen, während es bei der Verteidigung nur etwa 37 % waren, vgl. *Detter*, NStZ 1998, 57 (59) m. w. N. Zum Problem der „bewährten" Gutachter vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 333 f.; *Tondorf/Tondorf*, Psychologische und psychiatrische Sachverständige im Strafverfahren, Rn. 248; *Detter*, NStZ 1998, 57 (59).

395 Nach *Stinshoff*, Operative Fallanalyse, S. 130 sei dann das Auswahlermessen der Richter auf Null reduziert.

396 *Hegler*, AcP 104 (1909), 151 (153 f.).

397 KK/*Krehl*, § 244 Rn. 45.

398 Löwe/Rosenberg/*Krause*, § 73 Rn. 37.

399 *Mezger*, AcP 117 (1918), Beilageheft 1, 3, 5; *Hegler*, AcP 104 (1909), 151 (153 f.); SK-StPO/*Rogall*, Vor § 72 Rn. 7.

400 Schon *Hegler*, AcP 104 (1909), 151 (249) spricht von „vermuteten, hypothetischen" Fähigkeiten; vgl. auch *Mezger*, AcP 117 (1918), Beilageheft 1, 3, 5; vgl. auch SK-StPO/*Rogall*, Vor § 72 Rn. 7.

401 Vgl. § 407a Abs. 1 ZPO, dessen Grundsätze auch im Strafprozess Anwendung finden, vgl. dazu auch *Ulrich*, Der gerichtliche Sachverständige, Rn. 334; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 275, S. 364; SK-StPO/*Rogall*, Vor

Stellt sich nach der Beauftragung heraus, dass dem Sachverständigen die besondere Sachkunde fehlt, ist die mangelnde Sachkunde im Rahmen der tatrichterlichen Beweiswürdigung nach § 261 StPO zu berücksichtigen (siehe dazu im 4. Teil).[402] Die Ernennung kann auch einen Verfahrensfehler darstellen, der eine Revision nach § 337 StPO i. S. einer Aufklärungsrüge (§ 244 Abs. 2 StPO) begründen kann. Das ist bspw. dann der Fall, wenn das Gutachten aufgrund der fehlenden Sachkunde Feststellungen enthält, die gegen die allgemeinen Denk- und Erfahrungssätze verstoßen und die Möglichkeit besteht, dass das Urteil auch darauf beruht.[403]

Eine gewissenhafte Auswahl des Sachverständigen durch das erkennende Gericht ist deshalb so wichtig, weil die übrigen Verfahrensbeteiligten gegen die Auswahl des Gerichts unmittelbar keine Einflussmöglichkeit haben (siehe dazu unter B. V.). Eine Beschwerde gegen die Auswahl des Sachverständigen ist nicht zulässig, vgl. bspw. § 305 S. 1 StPO.[404]

Dass die Beantwortung der (meisten) Beweisfragen in Bezug auf digitale Beweismittel und der forensischen Informatik in den meisten Fällen das Wissen eines durchschnittlichen Richters bzw. Staatsanwaltes übersteigen und besonderer Sachkunde bedürfen, wurde oben bereits dargestellt (siehe B. I. 2. und B. II. 2. a)).

cc) Die persönliche Eignung

Die besondere Sachkunde allein führt noch nicht zu einer Eignung des Sachverständigen.[405] So muss sich das erkennende Gericht bei der Auswahl auch an der persönlichen Eignung des Sachverständigen orientieren.[406] Diese umfasst persönliche Eigenschaften wie Gewissenhaftigkeit, einen gefestigten Charakter, Unbeeinflussbarkeit, eine klare und einfache Ausdrucksweise sowie Klarheit und Sicherheit der Wahrnehmung.[407]

---

§ 72 Rn. 50 ff. In Anlehnung an § 407a ZPO liegt eine Pflichtverletzung des Sachverständigen vor, wenn er seine mangelnde Sachkunde erkennt und diesen Umstand dem Gericht nicht unverzüglich anzeigt.

402 Vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 275; vgl. auch BVerwG, NJW 2011, 1983.

403 Meyer-Goßner/*Schmitt*, § 73 Rn. 19.

404 Vgl. dazu Meyer-Goßner/*Schmitt*, § 73 Rn. 18.

405 Löwe/Rosenberg/*Krause*, § 73 Rn. 24; *Eisenberg*, Beweisrecht der StPO, Rn. 1529 und 1537.

406 Meyer-Goßner/*Schmitt*, § 73 Rn. 4; *Tondorf/Tondorf*, Psychologische und psychiatrische Sachverständige im Strafverfahren, Rn. 248; *Ulrich*, Der gerichtliche Sachverständige, Rn. 165.

407 AK/*Wassermann*, § 73 Rn. 8, 1.

Nach Nr. 72 Abs. 1 RiStBV ist vor der Beauftragung des IT-Sachverständigen gegebenenfalls zu klären, ob dieser in der Lage ist, das Gutachten in angemessener Zeit zu erstatten. Somit erfasst die persönliche Eignung auch die Bereitschaft des Sachverständigen, das Gutachten zeitnah zu erstatten.[408]

dd) Die Pflicht zur Objektivität, vgl. § 79 Abs. 2 StPO

Weitere Voraussetzungen aus der obigen Definition, die eng mit der persönlichen Eignung verbunden sind, sind die Unabhängigkeit und Objektivität des IT-Sachverständigen im Rahmen seiner Auftragserledigung und Aussage.[409] Hierauf hat der Auftraggeber schon bei der Auswahl und Auftragserteilung zu achten bzw. hat der Sachverständige bei der Auftragsanbahnung auf solche Mängel hinzuweisen[410].

Die Pflicht zur Objektivität, vgl. § 79 Abs. 2 StPO, macht das Wesen des Sachverständigenbeweises aus;[411] man kann auch sagen, es sei die „vornehmste Pflicht" des Sachverständigen.[412] Er muss von allen Verfahrensbeteiligten unabhängig sein, sich diese „äußere und innere Unabhängigkeit"[413] bewahren und weisungsfrei arbeiten. Das ergibt sich schon aus dem Verfassungsrecht: Das Rechtsstaatsprinzip i. V. m. dem allgemeinen Freiheitsrecht (Art. 2 Abs. 1 GG) gewährleistet dem Beschuldigten das Recht auf ein faires, rechtsstaatliches Strafverfahren[414]. Hierzu gehört auch, dass das Strafverfahren in gesetzmäßiger und objektiver Weise durchgeführt wird. Staatsanwaltschaft und Gerichte haben die Aufgabe der Justizgewährung; sie sind hierbei an das Legalitätsprinzip gebunden.[415] Die Grenzen der einzubeziehenden Personen und die Grenzen der ihnen übertragbaren Tätigkeiten ergeben sich aus Aufgabe und Stellung, die den Ermittlungsbehörden im gesetzlich geordneten Strafverfahren zukommen. Aus dieser vom Legalitätsprinzip geprägten besonderen Stellung folgt, dass an die Anklagebehörde und die Personen, deren Hilfe sie sich bedienen, hohe Anforderungen hinsichtlich ihrer Unparteilichkeit zu stellen sind. An diesem Maßstab ist somit auch die Einbeziehung

---

408 *Eisenberg*, Beweisrecht der StPO, Rn. 1537; *Ulrich*, Der gerichtliche Sachverständige, Rn. 165; vgl. auch Nr. 72 Abs. 1 RiStBV. *Stinshoff*, Operative Fallanalyse, S. 132 weist darauf hin, dass die Absprache einer Frist und deren Einhaltung mit Ordnungsmitteln gem. § 77 Abs. 2 StPO erzwungen werden können.

409 Vertiefend dazu *Ulrich*, Der gerichtliche Sachverständige, S. 112 f.

410 OLG Koblenz MDR 2002, 1152 f.; SK-StPO/*Rogall*, Vor § 72 Rn. 52; *Zöller-Greger*, § 413 Rn. 4.

411 Vgl. *Detter*, NStZ 1998, 57 (59); *Zimmermann*, DS 2006, 304 (310 f.).

412 So *Ulrich*, Der gerichtliche Sachverständige, Rn. 353.

413 *Detter*, NStZ 1998, 57 (59).

414 Vgl. BVerfGE 64, 135 (145).

415 Vgl. BVerfGE 20, 162 (222); 46, 214 (223).

von IT-Sachverständigen sowohl in das staatsanwaltschaftliche Ermittlungsverfahren als auch in das Hauptverfahren zu messen.

Das erkennende Gericht soll einen Sachverständigen auswählen und beauftragen, der das Gutachten unparteiisch und unbefangen erstatten kann. Denn durch die überlegene Sachkunde gegenüber dem erkennenden Gericht besteht die Gefahr der Beeinflussung desselben zugunsten einer „Partei".[416]

Die Unabhängigkeit soll mit dem Instrument der Ablehnung sichergestellt werden. So begründet ein Verstoß gegen die Objektivität und Unabhängigkeit einen Ablehnungsgrund nach § 74 i. V. m. §§ 22 ff. StPO (siehe dazu B. V. 2. c)).[417] Danach haben die Verfahrensbeteiligten die Möglichkeit, während des Verfahrens einen Befangenheitsantrag zu stellen. Eine möglicherweise bestehende Parteilichkeit wird auch im Rahmen der Beweiswürdigung nach § 261 StPO bei der Beurteilung der Glaubwürdigkeit von den Tatrichterinnen zu berücksichtigen sein (siehe dazu im 4. Teil B. III.).[418]

ee) Urteilsverzerrungen („bias")

Erwähnenswert an dieser Stelle sind die Auswirkungen von Urteilsverzerrungen („bias")[419], die geeignet sind, die Objektivität des IT-Sachverständigen zu „trüben".[420] Relevant im Hinblick auf den IT-Sachverständigenbeweis sind v. a. diese drei Typen: „anchoring bias", „availability bias" und „confirmation bias".

„Anchoring bias" ist darauf zurückzuführen, dass Informationen, denen Menschen zuerst begegnen, einen größeren Einfluss haben als Informationen,

---

416 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 361, 247; SK-StPO/*Rogall*, Vor § 72 Rn. 72; *Lürken*, NJW 1968, 1161; vgl. dazu auch *Mysegades*, Software als Beweiswerkzeug, S. 162 f.

417 Löwe/Rosenberg/*Krause*, § 73 Rn. 24; Meyer-Goßner/*Schmitt*, § 73 Rn. 9; AK/*Wassermann*, § 73 Rn. 8; *Eisenberg*, Beweisrecht der StPO, Rn. 1537; *Ulrich*, Der gerichtliche Sachverständige, Rn. 165.

418 Vgl. nur BGHSt 20, 222, 224.

419 „Bias" kann nach *Kahnemann/Sibony/Sunstein*, Noise, S. 180 mit „Urteilsverzerrungen" übersetzt werden.

420 So ergab auch eine Studie, dass IT-Forensiker anfällig für „bias" sind, https://www.theguardian.com/science/2021/may/31/digital-forensics-experts-prone-to-bias-study-shows [26.6.2023]. Vgl. zum „hidden bias" in forensischen Wissenschaften auch *Garrett*, Autopsy of a Crime Lab, S. 108 ff.; oder die „Entscheidungsarchitekten" aus *Thaler/Sunstein*, Nudge, S. 29 ff.; oder Allgemeines zum Thema „bias" und „noise" in der Wissenschaft bei *Kahnemann/Sibony/Sunstein*, Noise, S. 19 ff., 47 ff.; interessant in diesem Zusammenhang ist auch das Urteil von Rudy Frabizio, in dem der Zweitgutachter wegen „bias" nicht zugelassen wurde, vgl. United States of America, Appellant, v. Rudy Frabizio, Defendant, Appellee, 459 F.3d 80 (1st Cir. 2006).

die später zugänglich werden. Sobald Sachverständige die ersten Informationen erhalten, fixieren sie sich grds. auf diese, fokussieren ihre Analyse darauf, und entwickeln ggf. einen „Tunnelblick".[421]

Der „availability bias" führt dazu, dass Menschen die Wahrscheinlichkeit eines Ergebnisses aufgrund der Fähigkeit, sich an ähnliche Fälle zu erinnern, überbewerten. Das hat v. a. Auswirkungen auf die Hypothesenbildung bei sachverständigen Beobachtungen.[422]

Das wiederum führt zum (wohl bekanntesten der drei) „cognitive bias".[423] Er beruht auf der Tendenz von Menschen, unter unsicheren Bedingungen mentale Abkürzungen (Heuristiken) zu verwenden.[424] Das soll nicht heißen, dass Heuristiken per se problematisch sind, denn sie können adaptiv und effektiv sein, wenn Entscheidungen schnell getroffen werden müssen.[425] Wenn man sich jedoch zu sehr auf intuitives Denken und „enthusiastische erste Eindrücke"[426] verlässt, kann das zu fehlerhaften Entscheidungen führen.[427] Der „confirmation bias" äußert sich wie folgt: Es wird (ausschließlich) nach Informationen gesucht, die die Hypothese stützen; auch neue Informationen werden lediglich in Bezug auf die bestehende Hypothese interpretiert; mehrdeutige oder neutrale Informationen werden als Bestätigung der Hypothese interpretiert; Informationen, die der Hypothese widersprechen, werden ignoriert, wegerklärt oder als eher irrelevant bewertet. „Confirmation bias" wird auch durch Emotionen beeinflusst, z. B. durch Selbstvertrauen, Frust, Trauer und Wut, persönliche Verantwortung und die Sorge über zukünftige Konsequenzen.

Diese Phänomene gelten v. a. für Experten.[428] So haben Untersuchungen aus verschiedenen forensischen Disziplinen sowie realen Strafverfahren gezeigt, dass Sachverständige im Rahmen ihrer forensischen Untersuchungen,

---

421 *Tversky/Kahneman*, Psychological Review (1996) Vol. 103(3), S. 582.

422 *Tversky/Kahneman*, Psychological Review (1996) Vol. 103(3), S. 582.

423 *Sunde/Dror*, Digital Investigation (2019) Vol. 29, 101 ff. Vgl. dazu auch *Sagana*, in: Barton/Dubelaar/Kölbel/Lindemann (Hrsg.), Vom hochgemuten, voreiligen Griff nach der Wahrheit, S. 133 ff.

424 Vgl. auch *Kahneman/Tversky*, Psychological Review (1996) Vol. 103(3), S. 582.

425 *Gigerenzer/Todd*, Simple heuristics that make us smart, ABC Research Group (2000) Vol. 23, S. 727.

426 *Soll/Milkman/Payne*, A User's Guide to Debiasing: „enthusiastic first impressions".

427 *Hartley/Winburn*, Journal of Forensic Science, (2021) Vol. 66, S. 1 ff.

428 Im Gegensatz zu dem, was viele glauben, ist ein Experte in verschiedener Hinsicht anfälliger für „bias" im Vergleich zu Nicht-Experten, was auf die besondere Expertise zurückzuführen ist, *Dror*, The paradox of human expertise: why experts can get it wrong, S. 177 f.; allgemein – auch für andere forensische Disziplinen – siehe *Garrett*, Autopsy of a Crime Lab, S. 41 ff.

der damit einhergehenden Subjektivität (v. a. bei der Interpretation) anfällig für „bias" sind.[429] Das gilt ebenso für IT-Sachverständige und z. T. auch für die zugrundeliegenden Datenverarbeitungsmethoden.[430] So hat in allen forensischen Prozessschritten der forensischen Informatik (der Datenauswahl, der Datenverarbeitungsmethode, der Interpretation der Ergebnisse bis hin zur Art und Weise der Präsentation der Ergebnisse vor Gericht) die zu beantwortende Beweisfrage bzw. zu prüfende Hypothese tiefgreifende Auswirkungen auf die Beobachtungen und Schlussfolgerungen des IT-Sachverständigen. Wenn bspw. eine Person unter Tatverdacht steht, kann der „cognitive bias" dazu führen, dass sich ausschließlich auf das Auffinden von Spuren und Informationen konzentriert wird, die mit der Schuldhypothese übereinstimmen, während tendenziell Informationen übersehen oder wegerklärt werden, die der Schuldhypothese widersprechen, und die verdächtige Person entlasten würden. Die Quellen für diese Verzerrungen, denen IT-Sachverständige unterliegen, entspringen nach Dror[431] 1) der kognitiven Architektur und dem menschlichen Gehirn, 2) der Ausbildung (bzgl. mangelnde Sensibilisierung des Themas „bias"[432]) und der Motivation (v. a. relevant bei §§ 184b ff. StGB[433]), 3) organisatorischen Faktoren (v. a. die interdisziplinäre Kommunikation[434], dazu II. 3. c) aa)), 4) bisherigen Erfahrungswerten (bspw. welche Datenträger beschlagnahmt werden sollen und welche Tools für die Durchsicht anzuwenden sind[435]), 5) irrelevanten Informationen zum Fall (z. B. welche Meinung

---

429 *Sunde/Dror*, Digital Investigation (2019) Vol. 29, S. 102 f. m. w. N.

430 Vgl. dazu https://www.theguardian.com/science/2021/may/31/digital-forensics-experts-prone-to-bias-study-shows [26.6.2023]; *Drösser*, Total Berechenbar?, S. 215; *Rollberg*, Algorithmen in der Justiz, S. 44 ff.; *Nink*, Justiz und Algorithmen, S. 172 ff., *Martini*, Blackbox Algorithmus, S. 17 ff., 47 ff.; *Zweig*, Ein Algorithmus hat kein Taktgefühl, S. 205 ff.

431 Vgl. auch die Pyramide von *Dror*, Journal of Forensic Science (2017) Vol. 62.

432 Was die Ausbildung anbelangt, so hat die forensische Informatik ihre Wurzeln in der Informatik, der Physik (Elektronik) und der mathematischen Theorie (s. o.). Innerhalb dieser Wissenschaften und Theorien wird die Rolle der kognitiven Prozesse und des menschlichen Gehirns i. d. R. in den Lehrplänen keine große Rolle. Dem typischen IT-Forensiker fehlt meist Wissen über kognitive Mechanismen, Verzerrungen und entsprechende Gegenmaßnahmen. Das zeigte sich auch in den Interviews mit norwegischen IT-Forensikern, vgl. *Sunde*, Non-technical Sources of Errors.

433 V. a. bei der forensischen Arbeit in Bezug auf §§ 184b ff. StGB könne die Tätigkeit der IT-Sachverständigen von einer Motivation geprägt sein, den Kindern zu helfen und sie zu schützen und die (vermeintlichen) Täter zu „überführen", vgl. *Sunde/Dror*, Digital Investigation (2019) Vol. 29, 101 ff.

434 Die Worte, die wir verwenden, die Terminologie, das Vokabular und das Fachjargon können zu Fehlern bei der Interpretation und dem Verständnis von Informationen führen, vgl. auch mit *Zapf/Dror*, International Journal of Forensic Mental Health (2017), S. 227.

435 In der Erhebungsphase kann die Entscheidung über die Art der Erhebung (z. B. live oder post mortem) auch von den Erwartungen aus früheren Erfahrungen darüber

andere Verfahrensbeteiligte zur Beweisfrage haben[436]), wobei die Besonderheit besteht, dass – im Gegensatz zu anderen forensischen Disziplinen[437] – die Beantwortung der Beweisfrage durch den IT Sachverständigen häufig mehr Kontextinformationen benötigt.[438] 6) Referenzmaterial (wie bei einem Hashsummen-Abgleich[439] oder der Abgleich mit einem Alibi[440]), 7) weiteren Beweismitteln[441] zum Fall.[442]

---

beeinflusst werden, was erfolgreich war oder welcher Aufwand sich nicht gelohnt hat. In der Untersuchungsphase kann die Wahl der Tools von den Erwartungen an die Befunde beeinflusst werden, oder davon wie viel Aufwand die Forensikerinnen für das Entpacken komprimierter, archivierter oder entschlüsselter Dateien aufwenden.

436 Irrelevante Fallinformationen zu digitalen Beweismitteln können z. B. die offizielle Akte sein oder informelles Wissen der an den Ermittlungen beteiligten Personen über den Fall. Das können sachliche Informationen sein bspw. ob der Verdächtige gestanden hat oder Ergebnisse der Analyse anderer Beweismittel. Unerhebliche Fallinformationen können subjektive Informationen sein, wie persönliche Meinungen darüber, welche Deliktshypothese sie für die wahrscheinlichste halten, wie sie über den Verdächtigen denken oder ihre Sympathie für das Opfer. Wenn der Fall die Aufmerksamkeit der Medien erregt, können dort weitere verzerrende, irrelevante Informationen ihren Ursprung haben.

437 Im Bereich der Fingerabdrücke z. B. kann der Experte den Identifizierungsprozess mit begrenzten Kontextinformationen durchführen, die sich darauf beschränken, wie die Abdrücke aufgenommen und entwickelt wurden, von welcher Oberfläche die Abdrücke genommen wurden usw.

438 Hier bedarf es dann bestimmter Selektionsmethoden bei der Durchsicht großer Datenbestände. Auch bei der Beantwortung der Beweisfrage bedarf es mehr Kontextinformation durch die IT-Sachverständigen, vgl. vertiefter dazu *Sunde/Dror*, Digital Investigation (2019) Vol. 29, 105. Das wurde in dieser Arbeit auch bei II. 2. a. thematisiert.

439 In der digitalen Forensik könnte Referenzmaterial verwendet werden, wenn die Forensikerin die Aufgabe hat, festzustellen, ob eine bestimmte Datei, z. B. ein Bild, ein Dokument oder ein Video auf einem Computer vorhanden ist. Die Aufgabe bestünde in einer Berechnung einer Prüfsumme und Suche nach einer Übereinstimmung. In solchen Fällen ist nur wenig Gefahr von bias vorhanden.

440 Es gibt jedoch Aufgaben, bei denen das Referenzmaterial durchaus geeignet ist, die Interpretation der tatsächlichen Beweise zu verzerren. So werden digitale Spuren oft zur Gegenprüfung von Informationen verwendet, die im Laufe der Ermittlungen, z. B. aus polizeilichen Vernehmungen gesammelt wurden. Beim Lesen dieser zu überprüfenden Vernehmungen, wird die Forensikerin regelmäßig mehr (verzerrenden) Informationen ausgesetzt, als bei der Durchführung des Abgleichs vllt. erforderlich wären. Um mögliche Verzerrungen zu minimieren, benötigt die Forensikerin weder die vollständige Aussage, noch alle Details der Vernehmung, sondern nur einige Schlüsselinformationen aus der Aussage.

441 Beispiele hierfür könnten Bilder von sexuellem Missbrauch, Chatprotokolle über die Planung eines Terroranschlags oder ein Internet-Suchprotokoll, das Suchbegriffe darüber enthält, wie man mit Mord davonkommt oder wie man ein Getränk mit Drogen versetzt, um eine Vergewaltigung zu ermöglichen.

442 Vertiefend zu den einzelnen Schritten siehe auch *Sunde/Dror*, Digital Investigation (2019) Vol. 29, S. 104.

Überall wo (sowohl menschliche als auch computergenerierte) Entscheidungen getroffen werden, muss wohl ein gewisser Grad an „bias" in Kauf genommen werden. Allerdings gibt es Methoden, um diesen zu minimieren:[443] Etwa das Bilden von Alternativhypothesen[444], lediglich fallrelevante Informationen zur Verfügung zu stellen und Sensibilität[445] für das Vorhandensein von „bias" unter den Verfahrensbeteiligten zu schaffen.[446]

d) Die Ernennung (Form der Bestellung)

Ist eine geeignete Person ausgewählt, bedarf es für die Erlangung dieses Status einer Prozesshandlung der zuständigen Strafverfolgungsbehörde.[447] Diese Handlung („Auftrag"[448] oder auch „Bestellung"[449]) liegt in der Ernennung (auch „Zuziehung"[450] oder „Beauftragung"[451]) des Sachverständigen, § 75 Abs. 1 StPO.[452] Die richterliche Handlung ist entweder eine sachleitende Anordnung i. S. d. § 238 Abs. 1 StPO oder ein förmlicher Beweisbeschluss, wobei Name und prozessuale Stellung explizit anzugeben sind.[453] Wenn die richterliche Anordnung gem. § 238 Abs. 2 StPO beanstandet wird, ist ein Be-

---

443 Vertiefter dazu *Sunde/Dror*, Digital Investigation (2019) Vol. 29, S. 106.

444 So auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 385 f.

445 Das ergab auch die Untersuchung von *Sunde*, Non-technical Sources of Errors, S. 72 in Bezug auf norwegische IT-Forensiker im Strafverfahren. Eine Maßnahme, die dabei helfen soll, die Objektivität zu gewährleisten, soll v. a. die Sensibilisierung für dieses Thema unter den Verfahrensbeteiligten sein; vertiefend dazu auch *Sunde*, Forensic Science International: Digital Investigation (2022) Vol. 40, S. 1 ff.

446 Siehe zu „Qualitäts-Measurements": https://www.vegs-akademie.eu/seminare/it-sachverstaendiger, https://www.bisg-ev.de/ [12.4.2023], *Garrett*, Autopsy of a Crime Lab, S. 41 ff. v. a. in Bezug auf das „blind-testing"; Allgemeines dazu auch in *Thaler/Sunstein*, Nudge, S. 331 ff.; *Kahnemann/Sibony/Sunstein*, Noise, S. 245 ff.; die Wirtschaft wirbt mit polizeilich geprüften und abgenommenen Experten und Räumen (siehe bspw. „Fast Detect").

447 *Mezger*, AcP 117 (1918), Beilageheft, 1, 6; SK-StPO/*Rogall*, Vor § 72 Rn. 32, § 73 Rn. 9; Löwe/Rosenberg/*Krause*, § 73 Rn. 2; *Stinshoff*, Operative Fallanalyse, S. 133.

448 Z. B. *Mezger*, AcP 117 (1918), Beilageheft, 1, 6; SK-StPO/*Rogall*, Vor § 72 Rn. 32.

449 Z. B. *Mezger*, AcP 117 (1918), Beilageheft, 1, 6; Meyer-Goßner/*Schmitt*, § 72 Rn. 2.

450 Nr. 69 RiStBV.

451 § 78c Abs. 1 S. 1 Nr. 3 StPO.

452 Wobei die Auswahl und die Bestimmung der Anzahl lediglich formlose, i. d. R. interne Vorgänge sind, die der eigentlichen Prozesshandlung vorausgehen, vgl. auch SK-StPO/*Rogall*, Vor § 72 Rn. 32, § 73 Rn. 42; a. A. *Gössel*, DriZ 1980, 363, 367, der von der Teilbarkeit der Prozesshandlung in Auswahl und Mitteilung des Beweisthemas ausgeht.

453 So schon *Mezger*, AcP 117 (1918), Beilageheft, 1, 7 f.

schluss notwendig.[454] Außer in letztgenanntem Fall ist eine bestimmte Form für den Auftrag nicht vorgeschrieben,[455] wodurch er auch mündlich oder konkludent erfolgen kann.[456] So ist es möglich, dem Sachverständigen konkludent mit der Ladung einen Auftrag zu erteilen.[457] Wenngleich der Gutachtenauftrag mündlich erteilt werden kann, ist schon aus Beweisgründen eine rechtzeitige schriftliche Dokumentation (bspw. im Hinblick auf die Verjährungsunterbrechung[458]) unbedingt erforderlich.[459]

Die prozessuale Handlung muss jedoch für alle Verfahrensbeteiligten nach ihrem Inhalt und dem Zeitpunkt ihres Ergehens erkennbar sein und von diesen in ihrer Wirkung auf das Verfahren abgeschätzt werden; nicht zuletzt von der Beweisperson, von der durch den Auftrag eine Handlung bewirkt werden soll.[460] Auf die Frage, ob Prozesshandlungen als Willenserklärung i. S. d. §§ 116 ff. BGB mit den entsprechenden rechtlichen Folgen einzuordnen sind, was eine Empfangsbedürftigkeit zur Folge haben könnte, vgl. § 130 Abs. 1 BGB, kommt es deshalb schon nicht an, weil der Auftrag einen Empfang voraussetzt. Die h. M. lehnt eine solche Einordnung auch ab, da es sich bei den Prozesshandlungen nicht um ein Rechtsgeschäft handelt.[461] Auch Nr. 72 Abs. 2 RiStBV und die Leitungspflicht aus § 78 StPO (dazu unter B. VII.)

---

454 Meyer-Goßner/*Schmitt*, § 238 Rn. 19; Löwe/Rosenberg/*Becker*, § 238 Rn. 32; *Gössel*, DriZ 1980, 363, 367; a. A. KMR/*Paulus*, § 238 Rn. 50.

455 In der Schweiz ist dagegen eine schriftliche Auftragserteilung vorgesehen, vgl. Art, 184 Abs. 2 der schweizerischen StPO.

456 BGHSt 28, 381, 382; BGH NStZ 1984, 215; OVG Lüneburg NJW 2012, 1307; SK-StPO/*Rogall*, Vor § 72 Rn. 32, § 73 Rn. 32; *Gössel*, DriZ 1980, 363, 367. Zur Problematik der konkludenten Auftragserteilung siehe in diesem Teil, B. III. 3.

457 Vgl. OLG Köln VRS 58, 72.

458 Unter den in § 78c Abs. 1 Nr. 3 StGB genannten Voraussetzungen wird durch die Sachverständigenbestellung die Verjährung unterbrochen.

459 BGH v. 10.4.1979 – 4 StR 127/79, NJW 1979, 2414, wonach auch eine mündliche Beauftragung dem Inhalt und dem Zeitpunkt nach aus den Akten erkennbar sein muss; ähnlich BGH v. 6.10.1981 – 1 StR 356/81, MDR 1982, 156 = NJW 1982, 291; BGH v. 2.7.1986 – 3 StR 87/86, MDR 1986, 976 = StV 1986, 465; OLG Zweibrücken v. 9.10.1978 – WS 397/78, NJW 1979, 1995.

460 BGH JR 1954, 271, 272; *Mezger*, AcP 117 (1918), Beilageheft, 1, 8 spricht bspw. von einem nach außen hervorgetretenen richterlichen Willen; *Gössel*, DriZ 1980, 363, 367; vgl. aber BGHSt 27, 78, 79 für den Gutachtenauftrag i. S. d. § 33 OwiG; *Tröndle*, JZ 1969, 374 (376 f.); *Ulrich*, Der gerichtliche Sachverständige, Rn. 150; zur Auslegung von Prozesshandlungen siehe auch *Eb. Schmidt*, I, Rn. 184; *Henkel*, Strafverfahrensrecht, S. 243 f.

461 Vgl. *Stinshoff*, Operative Fallanalyse, S. 195 f., die die Erkennbarkeit des Auftrags v. a. entsprechend zur Inkulpation des Beschuldigten fordert; siehe auch *Glodschmidt*, Der Prozess als Rechtslage, S. 134 ff., 137 ff.; *Eb. Schmidt*, I, Rn. 183; *Volk/Engländer*, § 9 Rn. 3; *Henkel*, Strafverfahrensrecht, S. 236 Fn. 8; vgl. auch BGHSt 5, 338, 341; a. A. wohl KK/*Fischer*, vor § 72 Rn. 404; *Roxin/Schünemann*, § 22 Rn. 6 ff., die jedoch auch eine Ungültigkeit der Prozesshandlung wegen Irrtums ablehnen.

setzen eine Erkennbarkeit voraus. Danach ist dem Sachverständigen ein genau umgrenzter Auftrag zu erteilen und das Gericht muss im Rahmen seiner sachleitenden Anordnung das Beweisthema genau beschreiben (dazu genauer unter B. II. 3. c)).[462] § 74 Abs. 2 StPO verlangt sogar eine Namhaftmachung des Sachverständigen, wenn nicht besondere Umstände entgegenstehen. Wenn dem nachgekommen wird, ist eine Erkennbarkeit unproblematisch. Ansonsten muss die Verfahrensposition der Bezeichnung in der Ladung[463] oder der Belehrung vor der Vernehmung[464] entnommen werden.

Schwierigkeiten hinsichtlich der Erkennbarkeit des Auftrags entstehen, wenn dieser nur konkludent ergeht und insbesondere dann, wenn sich während der Vernehmung ein Statuswechsel[465] (bspw. vom IT-Sachverständigen zum Zeugen, vgl. dazu B. III. 2.) ergibt.[466] In diesen Fällen hilft ein Anknüpfen an dem Zweck der Vernehmung.[467] Wenn das Gericht die Beweisperson bspw. zu Erfahrungssätzen und Schlussfolgerungen befragt (erste und zweite Aussagekategorie) oder wenn das Gericht von der Beweisperson die Wahrnehmung von Befundtatsachen sowie eine Aussage darüber verlangt (die Wahrnehmung also erst *aufgrund* des gerichtlichen Begehrens erfolgt), dann ist von einem Sachverständigenauftrag auszugehen (siehe dazu vertiefter bei B. III. 3.).[468]

Ist ein Auftrag nicht erkennbar (auch nicht durch Anknüpfen am Zweck der Befragung), muss seine Existenz abgelehnt werden und die Beweisperson ist

---

462 *Gössel*, DriZ 1980, 363, 367; BGHSt 27, 76 für den Gutachtenauftrag i. S. d. § 33 OwiG; *Tröndle*, JZ 1969, 374, 376 f.; *Ulrich*, Der gerichtliche Sachverständige, Rn. 150.

463 Vgl. SK-StPO/*Rogall*, Vor § 72 Rn. 32; *Gössel*, DriZ 1980, 363 (367), wonach die Ladung jedoch nicht dazu geeignet sei, wenn lediglich die Auswahl der Person des Sachverständigen zum Ausdruck kommen soll, nicht aber das Beweisthema (aufgrund der von ihm vertretenen Teilbarkeit der Prozesshandlung); a. A. BGH NStZ 1985, 182; Löwe/Rosenberg/*Krause*, § 85 Rn. 1; AK/*Schreiber*, Vor § 72 Rn. 30; AwK-*Krekeler/Werner*, Vor §§ 72 ff. Rn. 3; KK/*Senge*, Vor § 72 Rn. 7; *Pfeiffer*, Vor § 72 Rn. 2; *Ulrich*, Der gerichtliche Sachverständige, Rn. 19; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 377; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 279; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 93 ff., der auf den Inhalt der Aussage abstellt; *Eisenberg*, Beweisrecht der StPO, Rn. 1513 nicht ganz eindeutig.

464 SK-StPO/*Rogall*, Vor § 72 Rn. 61; Meyer-Goßner/*Schmitt*, § 78 Rn. 3; Löwe/Rosenberg/*Krause*, § 78 Rn. 4; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 110 ff.; *Eb. Schmidt*, Nachtrag I, § 78 Rn. 8.

465 SK-StPO/*Rogall*, Vor § 72 Rn. 32.

466 Dazu auch *Stinshoff*, Operative Fallanalyse, S. 197.

467 Vgl. auch *Hegler*, AcP 104 (1909), 151, 246 ff., 260; *Mezger*, AcP 117 (1918), Beilageheft, 1, 4 f.; *Mayer*, in: FS-Mezger, S. 455 (464 f.).

468 So auch *Mezger*, AcP 117 (1918), Beilageheft, 1, 6, der vom „sachlichen Inhalt des Auftrags“ spricht.

als Zeuge zu verhören.[469] Entsprechend darf das Gericht aus der Aussage keine Sachkunde schöpfen und weder Erfahrungssätze noch Schlussfolgerungen aus der Aussage verwerten. Auch kann ein Beweisantrag auf Vernehmung eines Sachverständigen nicht mit den Begründungen abgelehnt werden, das Gericht habe selbst hinreichend Sachkunde, wenn es diese nicht auf eine eigene, bereits bestehende zurückführen kann, oder das Gegenteil der behaupteten Tatsache bereits durch ein früheres Gutachten bewiesen ist, § 244 Abs. 4 S. 1, 2 StPO.

Ist ein Auftrag (durch Ladung oder Beweisbeschluss) erteilt worden, muss dieser auf seine Richtigkeit hin überprüft werden (siehe dazu auch bei B. III. 2.). Ob der Auftrag rechtlich zutreffend erfolgt ist, muss unabhängig vom bestehenden Verfahrensstatus geprüft werden. Richtigerweise ist der Auftrag ergangen, wenn der Sachverständige – aufgrund seiner besonderen Sachkunde – zu einer der drei Aussagekategorien in Bezug auf eine Beweisfrage gehört werden soll. Soll er dagegen zu Tatsachen befragt werden, die er *vor* der Auftragserteilung wahrgenommen hat, ist die Sachverständigenbeauftragung falsch ergangen.[470] Oder stellt sich nach Beauftragung des Sachverständigen heraus, dass ihm aufgrund mangelnder Sachkunde der Auftrag zu Unrecht erteilt wurde, darf die Beweisperson nur noch als Zeuge zu den sog. Zusatztatsachen vernommen werden.[471] Das Gericht kann und sollte den als Sachverständigen bestellten entpflichten gem. § 76 Abs. 1 S. 2 StPO bzw. einem Beweisantrag auf Vernehmung eines weiteren Sachverständigen stattgeben nach § 244 Abs. 4 S. 2 StPO bzw. einen solchen im Rahmen seiner gerichtlichen Aufklärungspflicht nach § 244 Abs. 2 StPO selbst bestellen.[472]

e) Der Begutachtungszwang

Jede Person, die die Voraussetzungen des § 75 StPO erfüllt, ist grundsätzlich[473] zur persönlichen und mündlichen Erstattung des in Auftrag gegebenen

---

469 Vgl. auch *Peters*, Strafprozess, S. 262; *Rogall*, in: FS-Frisch, S. 1199 (1121 ff.); a. A. BGH GA 1976, 78 f.

470 Das kann bspw. sein, wenn sich der Sachverständige bereits vorher mit dem Beschuldigten oder seinem Umfeld beschäftigt hat (z. B. ein Arzt, der einen zu Begutachtenden bereits als Patienten hatte).

471 Folgt man dagegen der Ansicht, dass eine Sachverständigenposition trotz fehlender Sachkunde bestehen bleibt, muss die fehlende Sachkunde im Rahmen des § 261 StPO berücksichtigt werden; vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 275; BverwG NJW 2011, 1983; *Stinshoff*, Operative Fallanalyse, S. 200.

472 Vgl. dazu auch *Stinshoff*, Operative Fallanalyse, S. 134 f.

473 Der Sachverständige kann gem. § 76 Abs. 1 S. 1 StPO das Gutachten aus denselben Gründen verweigern, die einen Zeugen berechtigen, das Zeugnis zu verweigern. Auch aus anderen Gründen kann der Sachverständige von der Verpflichtung ein Gut-

Gutachtens verpflichtet, vgl. § 250 StPO. Der actus contrarius[474] zur Bestellung ist die Entpflichtung (§ 76 Abs. 1 S. 2 StPO[475]), womit der Sachverständige wieder aus seiner Verfahrensstellung entlassen wird. Die Norm legt fest, dass das Gericht den Sachverständigen auch aus anderen Gründen als denen, die den Sachverständigen zur Verweigerung der Gutachtenerstattung berechtigen, von der Verpflichtung der Gutachtenerstattung entbinden kann.[476]

Einer Bestellung zum Sachverständigen entgegenstehende Hindernisse sieht die StPO in den §§ 74 bis 76 StPO vor. Grds. geht das Gesetz von einer eingeschränkten Staatsbürgerpflicht zur Gutachtenerstattung parallel zur Zeugenpflicht[477] aus, die auf die Fälle des § 75 StPO beschränkt ist. Die Parallele zur Zeugenpflicht wird v. a. dadurch sichtbar, dass die Entschädigung im selben Gesetz, dem JVEG[478], geregelt ist, wenngleich der Sachverständige nach dem Leistungsprinzip vergütet wird, vgl. §§ 1 Abs. 1 S. 1 Nr. 1 und 3, 5 ff., 8, 9 JVEG während der Zeuge grds. nur versäumten Dienst geltend machen kann. Auch haben beide die Pflicht zum Erscheinen und zur mündlichen Gutachtenerstattung. Deshalb ist es konsequent, wenn das Gesetz den Sachverständigen auch parallel zu den Zeugnisverweigerungsrechten gem. § 76 Abs. 1 S. 1 StPO Gutachtenverweigerungsrechte einräumt.[479]

---

achten erstatten zu müssen, entbunden werden, vgl. § 76 Abs. 1 S. 2 StPO. Vgl. SK-StPO/*Rogall*, § 76 Rn. 17; KK/*Senge*, § 76 Rn. 4; Löwe/Rosenberg/*Krause*, § 76 Rn. 4; Meyer-Goßner/*Schmitt*, § 76 Rn. 3; *Bleutge*, DriZ 1977, 170, 172. Nach § 76 Abs. 2 StPO gelten für die Vernehmung von Richtern, Beamten und anderen Personen des öffentlichen Dienstes als Sachverständige die besonderen beamtenrechtlichen Vorschriften, vgl. dazu auch ausführlich *Kube/Leineweber*, Polizeibeamte als Zeugen und Sachverständige, S. 84 ff.

474 So führt eine erfolgreiche Ablehnung ipso iure zum Verlust der Gutachtereigenschaft, vgl. dazu in diesem Teil, B. V. 2. c) cc).

475 Nach SK-StPO/*Rogall*, Vor § 72 Rn. 33 sei die systematische Stellung der Norm unrichtig.

476 Zu den Gründen SK-StPO/*Rogall*, § 76 Rn. 17; KK/*Senge*, § 76 Rn. 4; Löwe/Rosenberg/*Krause*, § 76 Rn. 4; Meyer-Goßner/*Schmitt*, § 76 Rn. 3; *Bleutge*, DriZ 1977, 170, 172.

477 Zur Zeugenpflicht BVerfGE 38, 105 (118); 49, 280 (284); 76, 363 (383); BT Drs. 2/2545 S. 213 (dort auch zur Gutachtenerstattungspflicht); allg. dazu *Eisenberg*, Beweisrecht der StPO, Rn. 1055; speziell zur Gutachtenerstattungspflicht Meyer-Goßner/*Schmitt* § 75 Rn. 1; *Kube/Leineweber*, Polizeibeamte, S. 50; Löwe/Rosenberg/*Krause*, § 75 Rn. 1; *Eb. Schmidt*, Lehrkommentar § 75 Rn. 1; *Wolter*, ZStW 107 (1995), 793 (835).

478 Gesetz über die Vergütung von Sachverständigen, Dolmetscherinnen, Dolmetschern, Übersetzerinnen und Übersetzern sowie die Entschädigung von ehrenamtlichen Richterinnen, ehrenamtlichen Richtern, Zeuginnen, Zeugen und Dritten; siehe zur Vergütung später in diesem Teil, B. III. 2. d).

479 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 361 f.

Auch die Gründe, aus denen gem. § 55 StPO die Auskunft verweigert werden kann, sind zu beachten (über § 72 StPO). Nicht zu verwechseln ist das Recht zur Verweigerung der Gutachtenerstattung aufgrund vor Beginn der Sachverständigentätigkeit eingetretener Umstände gem. § 76 StPO mit der Problematik einer Zeugnisverweigerung in Bezug auf Informationen, die während der Sachverständigentätigkeit in Erfahrung gebracht wurden.[480]

Wenn keine der Varianten von § 75 Abs. 1 StPO eingreift, besteht eine Pflicht zur Gutachtenerstattung nur bei Bereiterklärung vor Gericht, in einem bestimmten Prozess das Gutachten erstatten zu wollen (ausdrücklich oder konkludent durch widerspruchslose Annahme des Auftrags bspw.) gem. § 75 Abs. 2 StPO.[481]

Außerdem weist die Literatur auf eine Zumutbarkeitsgrenze hin, wenn der Sachverständige z. B. beruflich stark überlastet ist, bereits einen anderen Gutachtenauftrag erhalten hat oder auf den Erholungsurlaub verzichten müsste.[482] Unter diesem Gesichtspunkt kann die grds. Pflicht zur Vorbereitung eines Gutachters eingeschränkt sein, z. B. wenn der Sachverständige erst kurz vor der mündlichen Verhandlung geladen wird und nicht hinreichend Zeit für die erforderliche Nachforschung erhält.

Wie oben bereits beschrieben, muss der Sachverständige dem Gericht mitteilen, wenn er sich in seiner Objektivität in einer Weise beeinträchtigt glaubt, dass die Voraussetzungen des § 74 StPO (i. V. m. §§ 22, 24 StPO) erfüllt wären.[483] Das Gericht kann den Sachverständigen dann gem. § 76 Abs. 1 S. 2 StPO von seiner Verpflichtung zur Gutachtenerstattung entbinden.[484]

Auch wenn der Sachverständige noch nicht vom Gericht ausgewählt und ernannt worden ist i. S. d. § 73 StPO, hat er doch der unmittelbaren Ladung durch die Staatsanwaltschaft (§ 214 Abs. 3 StPO) oder des Angeklagten

---

480 Vgl. *Rengier*, Zeugnisverweigerungsrechte, S. 270; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 364 f. Zur Problematik speziell bei Durchführung einer DNA-Analyse, die sich daraus ergibt, dass das zu untersuchende Material gem. § 81f Abs. 2 S. 3 StPO in anonymisierter Form übergeben wird und der Sachverständige deshalb nicht erkennen kann, ob er ein Gutachtenverweigerungsrecht besitzt, vgl. *Cramer*, NStZ 1998, S. 498.

481 Vgl. nur KK/*Senge*, § 75 Rn. 6; *Kleinknecht/Meyer-Goßner*, § 75 Rn. 2; Löwe/Rosenberg/*Krause*, § 75 Rn. 6; a. A. *Jessnitzer/Frieling*, Sachverständiger Rn. 143, der die allgemeine Bereiterklärung zur Erstattung von Gutachten bestimmter Art ausreichen lassen will, aber selbst einräumen, dass für die h. L. der übereinstimmende Wortlaut von §§ 407 Abs. 2 ZPO und § 75 Abs. 1 StPO sowie die Entstehungsgeschichte der ZPO sprechen.

482 Löwe/Rosenberg/*Krause*, § 75 Rn. 7.

483 Das wird aus der Pflicht zur Objektivität selbst abgeleitet, vgl. § 79 Abs. 2 StPO.

484 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 361 f.

(§§ 220 Abs. 1, 245 Abs. 2 StPO) Folge zu leisten, sofern auf ihn eine Variante des § 75 Abs. 1 StPO zutrifft und er kein Gutachtenverweigerungsrecht i. S. d. § 76 Abs. 1 S. 1 StPO geltend machen kann. Die Pflicht zum Erscheinen nach diesen Vorschriften ist ebenfalls Teil der Gutachtenerstattungspflicht.[485]

f) Die Übertragung des Auftrags auf andere (Hilfs-)Personen

Das Gesetz geht im Grundsatz von einer Einzelperson als Sachverständigen aus. Aus § 79 Abs. 2 StPO ergibt sich, dass der Sachverständige *selbst* das Gutachten nach bestem Wissen und Gewissen zu erstatten hat. Schon die Befugnis zur Auswahl der Person des Sachverständigen aus § 73 StPO zeigt, dass der Auftraggeber die Möglichkeit besitzen soll, zu bestimmen, in wessen Hände er die verantwortungsvolle Aufgabe der Vorbereitung der eigenen Überzeugung legt. Dieser Zweck würde vereitelt, wenn der Sachverständige selbst den Auftrag beliebig weitergeben könnte. Eine Ausnahme bildet § 83 Abs. 3 StPO: Wenn das Gericht Fachbehörden mit der Gutachtenerstattung beauftragt, lässt es damit bewusst die Frage der persönlichen Verantwortlichkeit bis zu einem gewissen Grad offen.[486]

Wenn die sogleich beschriebenen Voraussetzungen eingehalten werden, kann aber auch ein durch mehrere Personen generiertes Gutachten vor Gericht verwertet werden:

Grds. ist eine Übertragung des Auftrags auf eine andere Person als dem Sachverständigen nicht gestattet, vgl. § 407a Abs. 1, 3 ZPO.[487] Eine Hinzuziehung von Hilfspersonen ist allerdings erlaubt, vgl. § 407 Abs. 3 S. 2 ZPO, § 12 Abs. 1 S. 2 Nr. 1, Abs. 2 JVEG. Zweck des § 407a Abs. 3 ZPO ist es für klare Verantwortungsverhältnisse zu sorgen. § 407a Abs. 3 ZPO[488] sieht vor, dass Hilfskräfte, die nicht untergeordnete Verrichtungen bei der Vorbereitung des Gutachtens übernehmen (sofern der benannte Sachverständige die Hauptverantwortung behält), namhaft gemacht werden müssen. Übertragen lässt sich der Gedanke auch auf die Softwarenutzung bei der Tätigkeit des IT-

485 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 363.

486 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 364.

487 BGH StV 2011, 709; LR-Krause, § 75 Rn. 1; Meyer-Goßner/*Schmitt*, § 73 Rn. 1b; SK-StPO/*Rogall*, Vor § 72 Rn. 54, § 73 Rn. 39 f., § 75 Rn. 11; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 91; *Zimmermann*, DS 2006, 304 (309); zu den Gründen siehe auch *Bleutge*, NJW 1985, 1185 (1186 f.); vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 364 f.; *Müller*, Der Sachverständige im gerichtlichen Verfahren, Rn. 538 f.; *Ulrich*, Der gerichtliche Sachverständige, Rn. 337.

488 Der Grundgedanke gilt auch für andere Prozessarten als den Zivilprozess, vgl. *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, Rn. 231.

Sachverständigen, insbesondere dann, wenn wesentliche Teile des Gutachtens auf ihr basieren.[489] Eine untergeordnete Bedeutung haben Hilfsdienste dagegen in der Regel nur, wenn sie entweder keinen Einfluss auf das Ergebnis haben oder leicht überprüft und ersetzt werden können. Hilfsdienste in diesem Zusammenhang sind solche, die keine fachliche Ausfüllung von Lehr- und Erfahrungssätzen oder keine besonderen Fähigkeiten in der Befunderhebung voraussetzen, bspw. Schreibarbeit oder MTA's sein.[490] In Bezug auf Softwarenutzung wäre das bspw. ein Taschenrechner.[491] Diese müssen nicht gesondert genannt oder näher überprüft werden.

Ebenfalls einig ist man sich darüber, dass dem Sachverständigen die eigenständige Ernennung weiterer Sachverständiger nicht erlaubt ist.[492] Wenn der Gutachtenauftrag demnach über sein Sachgebiet hinausgeht und er die Ernennung eines weiteren Sachverständigen für notwendig hält, muss er das seinem Auftraggeber unverzüglich mitteilen, um die Ernennung zu veranlassen, vgl. § 407a Abs. 1 S. 2 ZPO.[493]

Die wohl h. M. gestattet dem Sachverständigen, auch Befunde anderer Sachverständiger („Hilfssachverständige"[494]) – nach eigener verantwortlicher Prüfung – für das eigene Gutachten zu verwenden.[495] Der Leiter bzw. Haupt-

---

489 *Mysegades*, Software als Beweiswerkzeug, S. 138.

490 *Schikora*, MDR 2002, 1033; SK-StPO/*Rogall*, Vor § 72 Rn. 55, 67; *Zimmermann*, DS 2006, 304, 310; für darüber hinausgehende Tätigkeiten von Hilfskräften vgl. Meyer-Goßner/*Schmitt*, § 73 Rn. 2; *Kube/Leineweber*, Polizeibeamte als Zeugen und Sachverständige, S. 68 f.; *Hanack*, NJW 1961, 2041 (2044).

491 *Mysegades*, Software als Beweiswerkzeug, S. 139.

492 Das kann nur das zuständige Strafverfolgungsorgan, BVerfGE 69, 70, 76; Löwe/Rosenberg/*Krause*, § 73 Rn. 7; Meyer-Goßner/*Schmitt*, § 73 Rn. 1b; SK-StPO/*Rogall*, Vor § 72 Rn. 110, § 73 Rn. 40; KMR/*Neubeck*, § 73 Rn. 4; AK/*Wassermann*, § 73 Rn. 6; BeckOK-StPO/*Monka*, § 73 Rn. 2; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 364; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 89 ff., 90 f.; *Zimmermann*, DS 2006, 304 (310); *Friederichs*, JZ 1974, 257 f.; a. A. OLG Hamm NJW 1973, 1427; KK/*Senge*, § 73 Rn. 4.

493 Meyer- Goßner/*Schmitt*, § 73 Rn. 3; *Zimmermann*, DS 2006, 304 (307); SK-StPO/*Rogall*, Vor § 72 Rn. 110 (auch für den Fall, in dem die Sachkunde des Sachverständigen nicht überschritten ist); *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 91.

494 Z. B. BGHSt 22, 268, 273; *Müller*, Der Sachverständige im gerichtlichen Verfahren, Rn. 194a, 538a; vgl. auch *Ulrich*, Der gerichtliche Sachverständige, Rn. 114; abl. SK-StPO/*Rogall*, Vor § 72 Rn. 55, 67, 110, § 73 Rn. 40; Löwe/Rosenberg/*Krause*, § 73 Rn. 7; Meyer- Goßner/*Schmitt*, § 73 Rn. 3; *Seyler*, GA 1989, 547, 552; *Friedrichs*, JZ 1974, 257 f.

495 BGHSt 22, 268, 272 f. = JR 1969 mit Anm. Peters; BGH NStZ 1997, 610; OLG Hamm NJW 1973, 1427 f. mit Anm. Friedrichs, NJW 1973, 2259; AK/*Wassermann*, § 73 Rn. 6; KK/*Senge*, § 73 Rn. 4; Löwe/Rosenberg/*Krause*, § 73 Rn. 8; KMR/*Neubeck*, § 73 Rn. 5; BeckOK-StPO/*Monka*, § 73 Rn. 2; *Eisenberg*, Beweisrecht der StPO, Rn. 1502; *Ulrich*, Der gerichtliche Sachverständige, Rn. 113; *Müller*, Der Sachver-

sachverständige dieser Sachverständigengruppe kann die Ergebnisse dann zusammengefasst vor Gericht vertreten.[496] Dem wird allerdings entgegnet, dass einerseits das Gesetz die vom BGH verwendeten Begriffe des „Haupt- und Hilfssachverständigen", des „Leiters" oder „Sachverständigengruppe" nicht kennt und andererseits die Position des „Leiters" auch nicht näher bestimmt wird.[497]

Daneben soll es auch das sog. Gruppengutachten geben. Jeder Sachverständige hat dabei aber einen eigenen abtrennbaren Teil zu bearbeiten und zu erstatten. Bei einem „Teamgutachten" dagegen hat jedes einzelne Teammitglied das gesamte Gutachten zu verantworten, da das Gutachten auf einer nicht trennbaren Gemeinschaftsleistung beruht.[498] In letzteren Fällen erscheint es sinnvoll zu prüfen, ob eine öffentliche Behörde das Gutachten erstellen kann, da das Gutachten dann nach § 256 StPO verlesen[499] werden kann, das sog. Behördengutachten.[500] Dabei handelt es sich um eine Urkunde i. S. v. § 249 Abs. 1 S. 1 StPO, die durch Verlesung in der Hauptverhandlung eingeführt wird.[501] Die erstattende Behörde[502] als Auftragnehmerin[503] können Landeskriminalämter,

---

ständige im gerichtlichen Verfahren, Rn. 193a, 194a; *Kube/Leineweber*, Polizeibeamte als Zeugen und Sachverständige, S. 69; *Bleutge*, NJW 1985, 1185; Meyer-Goßner/*Schmitt*, § 73 Rn. 2; *Seyler*, DA 1989, 546, 551; *Becker*, S. 63 f.; a. A. *Eb. Schmidt*, JZ 1970, 337 (343); *Friedrichs*, JZ 1974, 257 (258); SK-StPO/*Rogall*, § 72 Rn. 55, 110; § 73 Rn. 39 f. m. w. N.

496 BGHSt 22, 268, 273.

497 Vgl. dazu *Eb. Schmidt*, JZ 1970, 337, 343; *Friedrichs*, JZ 1974, 257, 258; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 91; SK-StPO/*Rogall*, Vor § 72 Rn. 55, 110; § 73 Rn. 39 f. m. w. N. Kritisch dazu auch *Stinshoff*, Operative Fallanalyse, S. 150 f.

498 Vertiefend dazu vgl. *Stinshoff*, Operative Fallanalyse, S. 151 f.; *Sunde*, Nontechnical Sources of Errors, S. 33: Aus ihrer Studie ergibt sich eine Präferenz der Praxis bzgl. Teamarbeit.

499 Ausnahme vom Mündlichkeitsgrundsatz, wonach die Gutachten grds. mündlich zu erstatten sind durch Vernehmung des jeweiligen Sachverständigen, § 250 StPO. Diese Ausnahme gründet auf einem besonderen Vertrauen des Gesetzgebers gegenüber öffentlicher Behörden in ihre Objektivität, Sachkunde und Zuverlässigkeit, vgl. dazu *Rogall*, in: FS-Gössel, S. 511 (512); Meyer-Goßner/*Schmitt*, § 256 Rn. 1; Alsberg/Nüse/Meyer, Der Beweisantrag im Strafprozess, S. 295 f.; *Ahlf*, MDR 1978, 981 (982); *Dästner*, MDR 1979, 545 (546); kritisch dazu *Eisenberg*, Beweisrecht der StPO, Rn. 1504.

500 Vgl. dazu *Stinshoff*, Operative Fallanalyse, S. 152 ff. So schon *Sarstedt*, NJW 1968, 177, 180.

501 Dazu v. a. *Rogall*, in: FS-Gössel, S. 511 (521) und *Stinshoff*, Operative Fallanalyse, S. 155 f. Wenn sich das Gericht gegen eine Verlesung des Gutachtens entscheidet, muss es eine natürliche Person als Sachverständigen bestellen und vernehmen.

502 Legaldefiniert in § 1 Abs. 4 VwVfG.

503 Also gerade nicht einzelne bestimmte Mitarbeiter dieser Behörde. Es wird das gesamte Fachwissen der Behörde in Anspruch genommen.

das BKA, öffentliche Kliniken, Universitätsinstitute oder öffentliche Behörden sein.[504] Teilweise wird vertreten, dass das Gutachten auch mündlich vorgetragen werden kann und in diesem Zusammenhang die Vorschriften des Sachverständigen direkt[505] bzw. analog[506] Anwendung finden sollen.[507]

Auch im Bereich der forensischen Informatik kann man grds. davon ausgehen, dass Gruppenarbeit die Qualität der Ergebnisse fördert. Jedenfalls wirkt die Gruppe als Korrektiv i. S.e. „4-Augen-Prinzips“[508] und man kann Expertise bündeln, eine Vielfalt der Hypothesenbildung erreichen und damit eine Objektivierung der Hypothesenprüfung gewährleisten. Auch kann die häufige Fülle des Datenmaterials in der forensischen Informatik Gruppenarbeit notwendig machen. Ob Gruppenarbeit aber möglich und erforderlich ist, ist wohl im Einzelfall zu entscheiden.

Verstößt der Sachverständige gegen die o. g. Pflichten, wie etwa Ausführungen eines anderen zu übernehmen ohne diese selbst kritisch zu würdigen, verliert er seinen Entschädigungsanspruch.[509] Das Gesetz orientiert sich in § 9 Abs. 1 JVEG am Prinzip der persönlichen Leistung.[510] Nennt er wichtige Mitarbeiterinnen nicht, so wird der Entschädigungsanspruch entsprechend gekürzt. Im Übrigen soll das Gutachten unverwertbar sein.[511] Faktisch wird sich eine Beeinflussung durch das Gutachten kaum mehr ausschließen lassen, nachdem es einmal in der mündlichen Verhandlung vorgetragen worden ist. Die wichtigste Konsequenz dürfte vielmehr darin zu sehen sein, dass es für die Darlegung zweifelhafter Sachkunde i. S. d. § 244 Abs. 4 S. 2 StPO aus-

---

504 BGH NJW 1968, 206; Meyer-Goßner/*Schmitt*, § 256 Rn. 13 m. w. N.

505 Vgl. *Glaser*, Handbuch, S. 690; *Gerland*, Der deutsche Strafprozess, S. 223 Fn. 280; *Gössel*, DRiZ 1980, S. 363 ff.; *Gollwitzer*, in: FS-Weißauer, S. 26; in der zivilrechtlichen Literatur und Rechtsprechung vgl. *Ulrich*, Der gerichtliche Sachverständige, Rn. 91; *Schnellbach*, Sachverständigengutachten kollegialer Fachbehörden im Prozess, S. 68; BGH NJW 1966, 502 (503); BGH NJW 1974, 701; 1998, 3355 (3356).

506 Vgl. SK/*Velten*, § 256 Rn. 19.

507 Die Diskussion wird v. a. im Zusammenhang mit § 256 Abs. 2 StPO geführt. Ebenfalls umstritten ist die Prozessrolle des Behördenbediensteten, wenn dieser das Gutachten nach der Verlesung vertritt und dazu persönlich vernommen werden soll. Vertiefend dazu *Stinshoff*, Operative Fallanalyse, S. 157 ff.

508 Vgl. zur sog. Berichtskritik nach dem Vier-Augen-Prinzip beim Wirtschaftsprüfer auch *Wolf*, ZWH 2012, 125 (126).

509 Insoweit wurde das Gutachten nicht „nach bestem Wissen und Gewissen“ erstattet, wie es die beauftragte Person gem. § 79 Abs. 2 StPO beeiden müsste, vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 365. Der BGH geht in solchen Fällen von einem Verstoß gegen den Grundsatz der mündlichen Gutachtenerstattung und den Unmittelbarkeitsgrundsatz i. V. m. einer nicht genügenden Beachtung der Aufklärungspflicht aus, vgl. BGHSt 22, 268 (270 ff.).

510 *Meyer/Höver/Bach*, JVEG § 9 Rn. 1 ff.

511 *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, Rn. 532.

reicht, wenn signifikante Anhaltspunkte dafür vorliegen, dass der Sachverständige sein Gutachten unkritisch von einer anderen Person übernommen hat. In diesen Fällen wäre demnach einer Anhörung eines weiteren Sachverständigen i. S. d. § 244 Abs. 4 S. 2 StPO, auch im Rahmen der Aufklärungspflicht nach § 244 Abs. 2 StPO, stattzugeben.[512]

3. Art und Umfang der Gutachtenerstattung

Nach dem gesetzlichen Normalfall beantwortet der IT-Sachverständige die Fragen – als Tatsachenbehauptung – im Rahmen der drei Aussagekategorien persönlich und mündlich. Die Art und der Umfang der Gutachtenerstattung hängen vom jew. Auftraggeber und dem Auftrag – der zu beantwortenden Beweisfrage – ab. Die konkreten inhaltlichen Anforderungen der Gutachtenerstattung werden im 3. Teil, B. III. 4. bei der Präsentation der Ergebnisse behandelt.

Wie stellt sich diese Gutachtenerstattung also genau dar?

a) Die Art der Gutachtenerstattung

Die StPO gibt vor, dass Gutachten mündlich in der Hauptverhandlung erstattet werden, vgl. den Unmittelbarkeisgrundsatz aus § 250 Abs. 1 S. 1 StPO. Nach § 256 Abs. 1 StPO sollte auch nur in Einzelfällen von der Möglichkeit Gebrauch gemacht werden, ein Sachverständigengutachten in der Hauptverhandlung zu verlesen. In der Hauptverhandlung dürfen schriftliche Gutachten nicht einmal in längeren, sprachlich komplexeren Passagen im Urteil zitiert werden, ohne dass der Wortlaut durch nur ausnahmsweise zulässige Verlesung gem. §§ 249 Abs. 1 ff. StPO (bzw. § 256 Abs. 1 StPO) in die Verhandlung eingeführt worden ist.[513]

Das Gericht geht jedoch in den meisten Fällen im Hinblick auf die Revisibilität des Urteils ein erhebliches Risiko ein, wenn es kein vorbereitendes schriftliches Gutachten anfertigen lässt und dieses nicht eine angemessene Zeit vor der mündlichen Verhandlung, in der der Sachverständige vernommen

---

512 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 364 f. Bisher hatte eine Revision in solchen Fällen selten Erfolg, da die Rspr. in weitem Umfang das Bedürfnis zur Arbeitsteilung anerkennt und eine eigene Gutachtenerstattung im Falle der Verwendung der übernommenen Daten mit der Begründung bejaht, der Gutachter habe diese „selbst geprüft und verarbeitet", vgl. dazu BGHSt 22, 268; OLG Hamm NJW 1973, 2260 m Anm. Friedrichs; OLG Hamm NJW 1973, 1427 m. Anm. Friedrichs.

513 BGH NStZ-RR 2001, 18; Aufgrund der Komplexität der Sachverhalte ergeben sich dadurch bei der mündlichen Gutachtenerstattung und der Würdigung häufig Probleme, siehe dazu im 3. Teil und 4. Teil.

wird, den Prozessbeteiligten zugänglich macht.[514] Auch aus dem Grundsatz eines fairen Verfahrens sowie der Leitungspflicht des Richters, gem. § 78 StPO, kann das in Auftraggeben eines vorbereitenden schriftlichen Gutachtens zur Erörterung für alle Verfahrensbeteiligten abgeleitet werden (siehe dazu B. VII.). Die Pflicht zur Kenntnisnahme vom schriftlichen Gutachten ergibt sich außerdem aus der Gewährleistung rechtlichen Gehörs (entspr. Art. 103 Abs. 1 GG), um einer Aufklärungsrüge bzw. einer Darstellungsrüge[515] vorzubeugen.[516]

Im Ermittlungsverfahren entscheidet gem. § 82 StPO die Anordnung, ob ein Gutachten mündlich oder schriftlich zu erstatten ist.[517]

Entgegen des gesetzlichen Normalfalls, ist der Regelfall der Praxis das in Auftrag geben eines schriftlich zu erstattenden Gutachtens im Auftrag der Staatsanwaltschaft im Ermittlungsverfahren.[518]

b) Der Umfang der Gutachtenerstattung anhand des Beweisthemas

Der Umfang der sachverständigen Tätigkeit richtet sich nach den konkret formulierten Fragen, die es zu beantworten gilt, dem sog. Beweisthema des Sachverständigenbeweises. Dabei handelt es sich um Tatsachenbehauptungen. Seine Grenze findet der IT-Sachverständige v. a. im jeweiligen – in der Praxis sehr offen und allgemein formulierten – Rahmen des Beweisthemas und der rechtsstaatlichen Bindung (siehe dazu B. VI.).

In Bezug auf den IT-Sachverständigen im Strafverfahren wird es sich um Beweisfragen aus dem Wissenschaftszweig der IT handeln, bei denen dem Gericht zur selbständigen Beantwortung die Sachkunde fehlt.

aa) Das Beweisthema als Tatsachenbehauptung

Bei der Beantwortung der Beweisfragen durch den Sachverständigen handelt es sich um Tatsachenbehauptungen (siehe zu den Begriffen oben, B. I. 2.), die der Auftraggeber mangels eigener Sachkunde nicht ohne den Sachver-

---

514 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 348.

515 Vgl. dazu BGHSt 7, 238; 8, 113 (118); 12, 311 (314); BGH StV 1982, 210 (211); 1983, 404; OLG Koblenz VRS 67, 442 (443); OLG Köln GA 1965, 156; Löwe/Rosenberg/*Hanack*, § 337 Rn. 121; *Sarstedt/Hamm*, Revision, Rn. 265 ff.

516 Die Prämissen, die das Gericht nicht ohne die Sachkunde des Gutachters hinreichend abzustützen in der Lage ist, kann es auch nicht plausibel in seine syllogistische Struktur einfügen, wenn es nicht imstande war, dem mündlichen Gutachten zu folgen; vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 353.

517 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 349.

518 Siehe dazu oben unter 2. b).

ständigen zu beantworten vermag. Indizien können stets Thema des Sachverständigenbeweises sein. Haupttatsachen sind dann unproblematisch Beweisthema des Sachverständigen, wenn das Gesetz technische Begriffe aus dem Wissenschaftszweig verwendet, der dem Gebiet angehört, auf dem der Sachverständige die besondere Sachkunde besitzt (bspw. „Zugangssicherung" i. S. v. § 202a StGB oder „verändert" i. S. v. § 303a StGB). Den technischen Begriffen ist es gleichzustellen, wenn der Sachverständige Aussagen trifft, aus denen sich im Wege bloßer Subsumtion auf die gesetzlichen Merkmale schließen lässt, da anerkannte Konventionen existieren, die eine Übersetzung der Aussagen in der Terminologie des Sachverständigen unmittelbar in die gesetzliche Terminologie gestatten. Das wird wohl der Fall sein, wenn es um die forensische Ermittlung kinder- oder jugendpornographischer „Dateien" auf Datenträgern geht und diese im IT-Sachverständigen-Gutachten als kinder- oder jugendpornographische „Inhalte" i. S. d. §§ 184b ff. StGB ausgewiesen werden.

Problematisch ist eine Haupttatsache dann, wenn der Sachverständige mit dem Instrumentarium seines Wissensgebiets lediglich Indizientatsachen zu ermitteln vermag, sodass der Schluss von der Indiztatsache auf die Haupttatsache Wertungen erfordert, für die die Wissenschaft des Sachverständigen keine oder nur unzureichende Anhaltspunkte bietet. Angeknüpft an das obige Beispiel könnten das bspw. Beurteilungen darüber sein, ob eine Datei kinder- (§ 184b StGB) oder jugendpornographische (§ 184c StGB) Inhalte zeigt oder der Nachweis der Kenntnis des Besitzes solcher Dateien anhand der Ablagestruktur, der Dateibezeichnung oder aufgrund von Kommunikation mit Dritten.

bb) Die Trennung zwischen Rechts- und sonstigen Tatsachenbehauptungen[519]

Beweisthema können de lege lata[520] nicht Rechts-, sondern nur sonstige Tatsachenbehauptungen sein (Grundsatz „iura novit curia").[521] Vom Gericht wird grundsätzlich verlangt, dass es die erforderliche Sachkunde zur Beantwortung von Rechtsfragen besitzt, für die die Berufsrichter ausgebildet wurden (vgl. § 5 DRiG).[522]

---

519 Vertiefend siehe auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 62, S. 135 ff.

520 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 136.

521 So die h. M., vgl. *Alsberg/Nüse/Meyer*, Der Beweisantrag im Strafprozess, S. 137 f.; Meyer-Goßner/*Schmitt*, § 72; vertiefend zu Grenzziehung zwischen Sachverhaltserforschung und unzulässiger Entscheidung über Rechtsfragen vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 135 ff.

522 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 126 f.

Davon sind folgende Ausnahmen anerkannt: Aus § 293 ZPO[523] kann abgeleitet werden, dass bzgl. des Bestehens inländischen Gewohnheitsrechts[524] sowie ausländischen Rechts[525] die Erhebung eines Sachverständigenbeweises zulässig ist.[526] Auch sollen Sachverständige hinzugezogen werden können, wenn das Gesetz technische Begriffe verwendet, die in außerjuristischen Spezialgebieten entwickelt worden sind und für deren Beurteilung eine nichtjuristische Spezialausbildung erforderlich wäre (häufig im Nebenstrafrecht, Beispiele: §§ 58, 59 LFGB, §§ 63 ff. Bundes-Seuchengesetz, § 328 StGB, § 27 ChemG).[527]

Dieser Ansicht liegt das Verständnis einer Trennbarkeit zwischen Tatsachen- und Rechtsfragen zugrunde.[528] Dass das aber oft nicht möglich ist, zeigt bspw. die Sachverständigentätigkeit von psychiatrischen Sachverständigen in Bezug auf § 20 StGB oder die Beurteilung der Fahruntüchtigkeit i. S. d. § 315c StGB, die Feststellung von Kausalität und erlaubtem Risiko[529] oder auch im Wirtschaftsstrafrecht, wo z. B. die Feststellung der Zahlungsunfähigkeit nicht ohne § 17 InsO oder die Ansatzpflicht einer Rückstellung nicht ohne § 249 HGB und die hierzu ergangene Rechtsprechung und Literaturmeinung beantwortet werden kann.[530] So wird als Beweisfrage an den IT-Sachverständigen in Bezug auf §§ 184b ff. StGB häufig nach dem Vorsatz gefragt, weil der

---

523 Der Grundgedanke kann gleichermaßen für die StPO herangezogen werden, vgl. *Alsberg/Nüse/Meyer*, Der Beweisantrag im Strafprozess, S. 138.

524 Gewohnheitsrecht lässt sich durch soziologische Erhebungen ermitteln.

525 Der Sachverständigenbeweis in Bezug auf ausländisches Recht wird damit begründet, dass dem Gericht diese Quellen nicht in gleicher Weise zugänglich sind wie inländisches Gesetzesrecht und jede Rechtsordnung ihre eigene Interpretationskultur entwickelt hat.

526 A. A. noch RGSt 42, 54 (56): Schließen eine förmliche Beweiserhebung in Bezug auf ausländisches Recht aus.

527 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 127, S. 136: De lege ferenda wäre die erneute Einführung einer Möglichkeit, Sachverständige in Bezug auf Fragen des inländischen Gesetzesrechts zu hören, zu befürworten. Bei der heute sehr weit vorangetriebenen Spezialisierung einzelner Rechtsgebiete erscheint die Annahme immer wirklichkeitsferner, jeder Richter könne alle Fragen des inländischen Rechts hinreichend beherrschen. Im Strafprozess ergibt sich das Problem insb., wenn der Strafrichter komplizierte Vorfragen des Steuer-, Verwaltungs-, oder Wirtschaftsrechts berücksichtigen muss. Es wäre hier sehr nützlich, wenn Sachverständige zur Verfügung stünden, die gemäß § 75 StPO zur Gutachtenerstattung verpflichtet wären und deren Vergütung gem. JVEG sichergestellt wäre.

528 Siehe dazu vertiefend *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 128 f.

529 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 133.

530 Dem folgend scheint die Zusammenfassung in *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 134 in Bezug auf die Trennung zwischen Tatsachen- und Rechtsfragen schlüssig.

Sachverständige bei seiner Analyse nach vielen solchen digitalen Indizien suchen und diese interpretieren kann, wie z. B. bestimmte Suchbegriffe im Browserverlauf, Ablagestruktur, Dateibezeichnungen, Format, Fundort und Format der Datei, etc.

Die Konsequenz der Beauftragung eines IT-Sachverständigen zur Klärung rein juristischer Fragen in Bezug auf inländisches Gesetzesrecht ist, dass ein Antrag der Prozessbeteiligten oder eine „Ladung" des Gerichts, um eine Aussageperson zu einem derartigen Thema zu hören, grds. nicht nach den Sachverständigenvorschriften beurteilt werden kann. Mangels eines zulässigen Beweisthemas kann keine Sachverständigenposition entstehen. So sind die §§ 72 ff. StPO weder direkt anwendbar, noch analog, soweit das Gericht durch die Vorschriften zu Eingriffen in Rechtspositionen ermächtigt wird.[531] Es muss also weder einer Ernennung nach § 75 Abs. 1 StPO Folge geleistet werden, noch erfolgt die Vergütung nach dem JVEG, das Gericht hat einem Antrag auf Vernehmung der Aussageperson in solchen Fällen auch nicht stattzugeben und muss darüber auch keinen Beschluss fassen. Gibt das Gericht einem Antrag statt, handelt es sich jedenfalls nicht um einen Beweisantrag bzw. um eine Anordnung der Beweiserhebung auf Bestellung eines Sachverständigen. Folge soll allerdings auch nicht sein, dass Urteile erfolgreich mit einer Revision angegriffen werden könnten, wenn sich Experten freiwillig dazu bereit erklären, das Gericht in solchen Fällen in der Hauptverhandlung zu instruieren. Richter könnten ebenso außerhalb der Hauptverhandlung per Anruf Rechtsrat einholen (sofern sie nicht gegen ihre Schweigepflicht verstoßen). A fortiori kann es auch nicht verboten sein, wenn sich das Gericht dazu entschließt, sich öffentlich in der Hauptverhandlung belehren zu lassen und z. B. die Verteidigung auf diese Weise bessere Kontrollmöglichkeiten besitzt.[532] Anzuknüpfen ist daher an die nachvollziehbare Begründung im Urteil (i. S. v. §§ 261, 267 StPO), indem das Gericht auf die Ausführungen der gehörten Aussageperson verweist (wie auch beim Sachverständigenbeweis in Bezug auf sonstige Tatsachen).[533]

Oft verwischen die Grenzen der Tatsachenkategorien und die Komplexität des Sachverhalts lässt eine eindeutige Trennung nicht zu. Auch, wenn die Gerichtsperson daran scheitert, das Beweisthema in der Sprache des Sachverständigen zu formulieren, soll es ausnahmsweise gerechtfertigt sein, im Auftrag direkt die Frage nach dem Rechtsbegriff zu stellen bzw. die Frage „ganz allgemein zu halten".[534] Bspw. wird Psychiatern im Auftrag oft die Frage nach der „Schuldfähigkeit" oder „Schuldminderung" gestellt. Bei der Gutachtener-

531 Dazu *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 136, S. 287 f.
532 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 137.
533 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 137.
534 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 127.

stattung soll dann aber lediglich festgestellt werden, dass „aus medizinischer Sicht“ die „Voraussetzungen“ zur Anwendung der §§ 20, 21 StGB gegeben sind. In der Beweiswürdigung muss das Gericht dann klar erkennen lassen und berücksichtigen, dass der Sachverständige in seiner Antwort (tentativ) zu Rechtsfragen Stellung nehmen muss, für deren Beurteilung er eigentlich nicht die erforderliche Sachkunde besitzt.[535] So geht die Auftragserledigung der Vorsortierung digitaler Speichermedien in Bezug auf kinder- und jugendpornografische Dateien wohl in der Natur der Sache mit einer vorweggenommenen rechtlichen Beurteilung einher (nicht zuletzt aufgrund der Herausforderung, sich in der immensen Datenmenge zurecht zu finden und die verschiedenen Spuren zu finden, geschweige denn, diese richtig zu interpretieren). Rechtsausführungen sollen durch den Sachverständigen noch nicht dessen Befangenheit begründen, so lange der Sachverständige nicht offenkundig einseitig tätig ist, wofür zu Lasten einer Partei ausfallende Ergebnisse allein nicht ausreichen.[536]

IT-Sachverständige können sich damit helfen, dass sie bei ihrer Gutachtenerstattung deutlich machen, dass die rechtliche Beurteilung letztlich nur vom juristischen Entscheider vorgenommen werden kann. Im Gutachten selbst wären diese rechtlichen Schlussfolgerungen („aus technischer Sicht“) explizit als solche zu kennzeichnen. Eine allgemeine Klarstellung am Ende des Gutachtens im Anhang reicht aus Sicht der Verfasserin jedenfalls nicht.[537] So würden im Lesefluss des Gutachtens bereits die rechtlichen Wertungen (Stichwort „priming“, „bias“) auf den Auftraggeber übergehen und er wäre dann ggf. in seiner rechtlichen Bewertung nicht mehr „frei“.

cc) Die verschiedenen Tatsachentypen im Rahmen der Gutachtenerstattung

Innerhalb der Gutachtenerstattung wird – abgesehen von Rechts- und sonstigen Tatsachenfragen – zwischen weiteren, für das Gutachten relevanten, Tatsachentypen unterschieden.[538] Dabei sind Anknüpfungstatsachen, die wahrgenommenen Untersuchungsergebnisse und auch die zugrundeliegende

---

[535] Die gängige Praxis, dass psychiatrische Sachverständige oft aufgefordert werden unmittelbar zur Schuldfähigkeit Stellung zu nehmen, scheint damit vertretbar.

[536] LG Bielefeld v. 9.12.2009 – 3 O 557/04, juris; OLG Nürnberg v. 1.8.2001 – 4 W 2519/01, MDR 2002, 291; zu Rechtsfragen auch Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 12.

[537] Diese „Praxis“ konnte auch bei der von der Verfasserin durchgeführten Akteneinsicht beobachtet werden.

[538] Der Unterschied ist wichtig für die Art, wie diese Informationen in den Prozess eingeführt werden können.

Methode zu unterscheiden und nachvollziehbar und lückenlos darzulegen,[539] sodass es dem Gericht möglich ist, das Gutachten selbstständig zu würdigen. Das gilt insbesondere deshalb, weil das Gericht in rechtlich nachprüfbarer Weise darzulegen hat, warum es dem Gutachten folgt bzw. es ablehnt.[540] So können Transparenz und Nachvollziehbarkeit gewährleistet werden.[541]

Anknüpfungstatsachen sind Tatsachen, die dem Gutachten zugrunde gelegt werden.[542] Sie müssen dem Sachverständigen bei der Auftragserteilung so umfassend wie möglich durch das Gericht oder die Staatsanwaltschaft mitgeteilt werden.[543] Das wären z. B. Zeugen- oder Beschuldigtenvernehmungen und ein digitales Abbild des Mobiltelefons der beschuldigten Person, wenn der IT-Sachverständige diese auf Übereinstimmung miteinander abgleichen soll. Hält der Sachverständige die Anknüpfungstatsachen nicht für ausreichend, kann er von seinem Auftraggeber gem. § 80 StPO weitere Aufklärung verlangen.

Befundtatsachen sind solche Tatsachen, die nur aufgrund oder mithilfe besonderer Sachkunde wahrgenommen werden können. Der Sachverständige ermittelt sie im Rahmen seiner Auftragsausführungen.[544] Das Gericht kann diese Informationen mangels eigener Sachkunde nicht selbst wahrnehmen[545]. Dem Wortlaut des § 85 StPO unterfallen sie grundsätzlich dem Zeugenbeweis, können aber auch im Wege der gutachterlichen Stellungnahme in die Hauptverhandlung eingeführt werden.[546] In der forensischen Informatik wären das bspw. Ergebnisse, die mithilfe von Datenverarbeitungs- und -analysemethoden erzeugt oder durch manuelle forensische Arbeit erlangt werden, und

---

539 *Zimmermann*, DS 2006, 304 (313 f.); *Tondorf/Tondorf*, Psychologische und psychiatrische Sachverständige im Strafverfahren, S. 67 ff. zu den Gutachtenstandards; SK-StPO/*Rogall*, Vor § 72 Rn. 111 ff.; mit ausführlichen Ausführungen zum Inhalt und Aufbau des Gutachtens. Weitere Nachweise siehe später in Teil 3, B. III. 4.

540 BGHSt 12, 311 f.; BGH StV 1982, 210; *Eisenberg*, Beweisrecht der StPO, Rn. 1508. Vertiefter dazu in Teil 4, A. 5.

541 Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 7; *Ulrich*, Der gerichtliche Sachverständige, Rn. 8.

542 Vgl. nur Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 7; KK/*Senge*, Vor § 72 Rn. 3; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 11.

543 BGH NStZ 1995, 282; vgl. auch BGH StV 1986, 138; Meyer-Goßner/*Schmitt*, § 80 Rn. 1; SK-StPO/*Rogall*, Vor § 72 Rn. 61; § 78 Rn. 10; *Ulrich*, Der gerichtliche Sachverständige, Rn. 317.

544 BGHSt 9, 292, 293; 107, 108; 22, 268, 272 f.; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 11; KK/*Senge*, Vor § 72 Rn. 4; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 238.

545 Wobei es regelmäßig nicht auf die Wahrnehmung, sondern auf die Interpretation der Wahrnehmung ankommt.

546 BGHSt 9, 292, 293; 107, 108; 22, 268, 272 f.; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 11; SK-StPO/*Rogall*, Vor § 72 Rn. 83; KK/*Senge*, Vor § 72 Rn. 4.

Schlussfolgerungen in Bezug auf die Beantwortung der Beweisfrage: Z. B. auf dem betroffenen System wurde Schadsoftware festgestellt, die durch eine unsichere Verbindung heruntergeladen wurde. Dadurch wurden sensible Daten des Unternehmens kompromittiert und auf einen externen Server übertragen.

Zusatztatsachen sind solche Tatsachen, die zwar im Zuge der Gutachtenerstellung ermittelt werden, aber auch ohne besondere Sachkunde wahrgenommen und ausgewertet werden könnten.[547] Das Gericht könnte diese Tatsachen grundsätzlich selbst mit den ihm zur Verfügung stehenden Kenntnismitteln feststellen, wie mglw. auch Hilfsdienste von untergeordneter Bedeutung (siehe unter 2. f)) .[548] Nimmt der Sachverständige diese wahr, können sie ausschließlich in Form des Zeugenbeweises in die Hauptverhandlung eingeführt werden. Sie sind nicht Bestandteil der Sachverständigenaussage.[549] Im Bereich der Tätigkeit des IT-Sachverständigen könnten das Kommunikationsinhalte oder Bild- und Videoinhalte sein, deren Inhalte (nachdem sie visualisiert wurden) auch ohne technologische besondere Sachkunde wahrnehmbar sind; so z. B. bei der Beurteilung, ob es sich bei den aufbereiteten Dateien durch den IT-Sachverständigen um jugend- oder kinderpronografische Abbildung i. S. v. §§ 184b ff. StGB handelt (vorausgesetzt die zur Entscheidung berufenen Richterinnen haben ausreichend Sachkunde das beurteilen zu können).

Weiter kennt die Literatur[550] noch die sogenannten Zufallsbeobachtungen, die in keinem unmittelbaren Zusammenhang mit dem Gutachten stehen. Eine klare Grenze zu den Zusatztatsachen sieht Toepel[551] nicht, weshalb der Begriff aus seiner Sicht überflüssig erscheint.

Über alle nicht im Rahmen des Auftrags getroffenen Beobachtungen muss der Sachverständige als Zeuge vernommen werden.

---

547 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 238; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 21; Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 7; *Pfeiffer*, Vor §§ 72–93 Rn. 1; SK-StPO/*Rogall*, § 85 Rn. 31.

548 Wie bspw. ein Geständnis, das der Beschuldigte im Zuge seiner Untersuchung dem medizinischen Sachverständigen gegenüber ablegt, vgl. BGH NJW 1959, 828; BGH NJW 1965, 827; *Pfeiffer*, Vor §§ 72–93 Rn. 1.

549 Vgl. nur BGHSt 13, 1, 3; 13, 250; 18, 107, 108; 20, 164 (166); 22, 268 (271); BGH NStZ 1993, 245; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 11; KK/*Senge*, Vor § 72 Rn. 5; *Vynálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 21; a. A. *Peters*, Strafprozess, S. 343: Er ist der Ansicht, dass die ohne Sachkunde gemachten Wahrnehmungen und getroffenen Feststellungen so eng mit dem Gutachten verknüpft sind, dass sich der Charakter der Aussage nicht ändern würde; vgl. auch OLG Schleswig SchHA 1972, 159; einschränkend *Ligges*, Die Stellung des Sachverständigen, S. 17; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 281.

550 AK/*Wassermann*, § 79 Rn. 10; Meyer-Goßner/*Schmitt*, § 79 Rn. 12; Löwe/Rosenberg/*Krause*, § 79 Rn. 17.

551 Grundstrukturen des Sachverständigenbeweises, S. 281.

Mithilfe der Grenzziehung zwischen Rechts- und sonstigen Tatsachen auf der ersten Ebene und auf einer weiteren Ebene durch die Differenzierung weiterer Tatsachentypen kann Transparenz und eine gemeinsame Verständigungsebene zwischen den Verfahrensbeteiligten geschaffen werden. An dieser kann dann sowohl der IT-Sachverständige mit seinen wissenschaftlichen Fachbegriffen anknüpfen, als auch der juristische Auftraggeber mit seiner rechtlichen Bewertung.

c) Die Formulierung des Beweisthemas im Untersuchungsauftrag

Wichtig bei der Auftragserteilung ist eine genaue Ausformulierung des Gutachtensauftrages und seines Umfangs. Die Praxis, Aktenkopien mit dem Ersuchen, „Befund aufzunehmen und ein Gutachten zu erstatten" an Sachverständige zu verschicken, fördert unnötig umfangreiche, langwierige und kostspielige Gutachten, die oftmals wichtige Fragestellungen gar nicht oder nur unzureichend beantworten oder Unerhebliches erörtern. Ergänzungsaufträge bewirken im Regelfall Zusatzkosten und Verfahrensverzögerungen. An die Staatsanwaltschaften und Gerichte ist zu appellieren, den Gutachtenauftrag klar und deutlich auszuformulieren, die Thematik bzw. den Umfang des Auftrages einzugrenzen und auch angemessene Fristen für die Erledigung zu setzen.[552]

Aus Nr. 72 Abs. 2 S. 1 RiStBV ergibt sich, dass dem IT-Sachverständigen ein genau umgrenzter Auftrag zu erteilen ist und ihm nach Möglichkeit konkrete Fragen zu stellen sind. Auch aus der Verpflichtung zur Leitung des Sachverständigen in § 78 StPO lässt sich ableiten, dass zumindest das Gericht einen möglichst präzisen Auftrag erteilen muss.[553] Das ergibt sich bspw. auch aus der Gesetzesbegründung des § 110 StPO in Bezug auf die Durchsicht von digitalen Speichermedien, wonach sachkundigen Dritten die Durchsicht nicht vollständig und eigenverantwortlich übertragen werden darf, sondern nur im Hinblick auf klar umgrenzte und formulierte einzelne Fragen.[554] In der Praxis wird dieser Aufforderung häufig nicht hinreichend nachgekommen. So wird ein Arzt bspw. oft nur nach einem „Kunstfehler" oder einem „Verschulden" gefragt.[555] Aufträge an einen IT-Sachverständigen lauten häufig wie folgt: „Gutachterliche Untersuchung und Beurteilung sichergestellter Datenträger

---

552 Auch unter dem Aspekt der Wirtschaftlichkeit, Sparsamkeit und Zweckmäßigkeit; *Schirhakl*, Der Sachverständigenbeweis im neuen Strafprozessrecht, S. 152.

553 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 62.

554 Vgl. MüKo-StPO/*Hauschild*, § 110 Rn. 11; KK/*Bruns* § 110, Rn. 4.

555 Ein Arzt wird bspw. oft nur nach einem „Kunstfehler" oder einem „Verschulden" gefragt, vgl. *E. Müller*, in: FS-Lüke, 493, 498; *Wolf*, ZWH 2012, 125 (129 f.). vertiefend zu den sehr offen formulierten Aufträgen.

hinsichtlich strafrechtlich relevanter Handlungen insb. zu Verdacht des Besitzes und/oder der Verbreitung von KIPO“ oder „die Asservate gutachterlich nach inkriminierten Inhalten zu untersuchen“.[556] Diese unzureichende Praxis ergibt sich wohl nicht zuletzt aus dem Mangel an Grundkenntnissen der forensischen Informatik („Was kannst du mir geben?“).[557]

Im Verlauf der Arbeit soll deutlich werden, dass die für den Bereich des IT-Sachverständigen formulierten Beweisfragen Bezug zu den Assoziationen i. S. d. forensischen Informatik nehmen. Für die Formulierung der Beweisfragen ist es deshalb hilfreich, sich eine gewisse Grundkenntnis bzgl. des forensischen Prozesses zu verschaffen. So kann man viele Ermittlungsaufgaben auf Fragen nach Assoziationen reduzieren. Die strikte Anwendung der Theorie von Transfer und Assoziation zwingt den Forensiker, einzelne präzise Aussagen über seine Befunde zu formulieren. Da der Begriff des Transfers so grundlegend und bereits aus anderen forensischen Disziplinen bekannt ist, sind die Aussagen, welche am Ende des Prozesses zur Assoziation getroffen werden, auch für technisch meist weniger versierte Personen leicht verständlich.[558] Das Konzept der Assoziation wird später an den Beispielen „USB-Speichergerät A war an Computer B angeschlossen“ und „Computer A hat Website B aufgerufen“ noch näher erläutert (siehe im 3. Teil, B. III. 3.).[559]

In Bezug auf die IT-Forensik, könnten die Fragen an einen IT-Sachverständigen im Auftrag z. B. wie folgt lauten:[560]

- Wurde E-Mail A (Absender, Empfänger, Datum, Betreff, Inhalt, Datei-Anhänge) auf diesem Rechner verfasst und an Rechner B verschickt?
- War USB-Stick A einmal an Rechner B angeschlossen?
- Wurde Datei A (bitweiser Vergleich oder Hash-Vergleich) auf Rechner B kopiert oder heruntergeladen?
- Findet sich Stichwort A in Dokumenten auf Rechner B?
- Befinden sich auf Rechner A Videos mit Inhalt B?

---

556 Beispiele aus der von der Verfasserin durchgeführten Akteneinsicht.

557 Zu diesem praktischen Blickwinkel wurde damals schon kommentiert „Ob man aber nur allgemeine, oder specielle Fragen stellen soll, hängt weniger vom herrschenden Gebrauche, als von den Kenntnissen des Inquirenten in der gerichtlichen Medicin ab; wer auf diesem Boden keinen festen Fuß hat, enthalte sich lieber aller detaillirten Fragen, damit er sich nicht einer Beschämung aussetze“, vgl. *Poppen*, Die Geschichte des Sachverständigenbeweises, S. 248 m. w. N.

558 *Dewald/Freiling*, Forensische Informatik, S. 94 f.

559 *Dewald/Freiling*, Forensische Informatik, S. 95.

560 Beispiele aus *Dewald/Freiling*, Forensische Informatik, S. 94 f.

- Wurde auf Rechner A Software B, wie bspw. eine bestimmte Filesharing- oder Datenvernichtungssoftware, eingesetzt?
- Wurde Rechner A durch Malware B, wie bspw. einen Banken-Trojaner, kompromittiert?
- Wurde mit Rechner A eine Instant Messenging-/VoIP- Kommunikation mit folgender/m Person/Synonym B geführt?

Gleichwohl ist offensichtlich, wie schwierig die Formulierung der richtigen Beweisfrage ist. An der Stelle der Formulierung des Untersuchungsauftrages besteht zum ersten Mal die Notwendigkeit einer Kommunikation zwischen dem IT-Sachverständigen und seinem Auftraggeber. Hier tritt das oft diskutierte Problem der Verständnisschwierigkeiten zu Tage, welches sich aus den unterschiedlichen Begrifflichkeiten der einzelnen Wissenschaftszweige ergibt, die sich in manchen Fällen nicht direkt in die Sprache der Juristinnen übersetzen lassen.

Freiling und Safferling verbildlichen dieses Problem gerne mit dem „Ping-Pong Spiel“ zwischen IT-Sachverständigen und den Auftraggebern – „was willst du?/was kannst du mir geben?“[561]

So kommt es an der Schnittstelle zwischen der juristischen und technischen Sphäre häufig zu Missverständnissen: Wenn der Jurist gerne „alle Dokumente“ von der Festplatte haben möchte, dann ist dem Informatiker unklar, was damit gemeint ist: nur Word-Dateien, oder auch E-Mails, Chat-Protokolldateien und wenn, in welcher Darstellungsform, usw.[562]

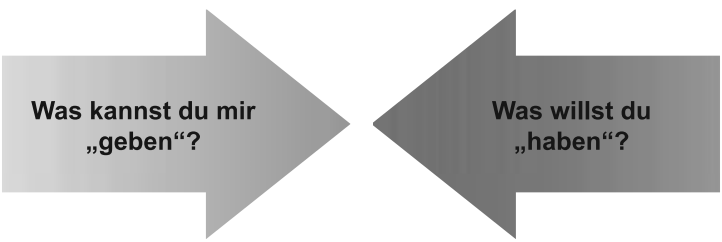


Abbildung 2: „Ping-Pong Spiel“

561 https://www.fau.de/2017/04/news/wissenschaft/nicht-alles-was-technisch-moeglich-ist-ist-auch-rechtlich-zulaessig/ [26.6.2023].

562 https://www.fau.de/2017/04/news/wissenschaft/nicht-alles-was-technisch-moeglich-ist-ist-auch-rechtlich-zulaessig/ [26.6.2023].

Im Laufe der Zeit verfestigt sich zwar die Beobachtung, dass die Strafverfolgungsbehörden langsam ein ganz gutes Gefühl dafür bekommen, was die IT – und auch die Experten der forensischen Informatik – alles kann. Nach wie vor ist jedoch viel Hilfestellung durch die IT-Sachverständigen nötig, um zu konkretisieren, welche Fragen in diesem „Datenwust" beantwortet werden können. Zudem gilt dieses „gute Gefühl" wohl auch nicht für neue Technologien und Datenverarbeitungs- und -analysemethoden; auch hier bedarf es einer offenen Kommunikation zwischen beiden Seiten. Die Bedeutung eines klar formulierten Auftrages kann gar nicht genug hervorgehoben werden.[563]

Wie schwierig das ist, ergibt sich auch aus der Einschätzung, dass die Formulierung der durch forensische Wissenschaftler zu beantwortenden Fragen einen Teil forensischer Informatik darstellt, der durch entsprechend geschulte Polizeibeamte und Juristen durchgeführt werden muss. Diese Aufgabe erfordert ein gewisses Maß an Wissen über Verbrechen (Modus Operandi, Kriminologie usw.) und ein Basiswissen im Bereich der elektronischen Datenverarbeitung.[564] Die Schwierigkeit der Formulierung der Beweisfrage ergibt sich v. a. daraus, dass der Auftraggeber bzgl. des Beweisthemas wenig Sachkunde hat, interdisziplinäre Verständigungsschwierigkeiten existieren, man bei der Fragestellung vermeiden muss, dass diese tendenziös wirkt und man im Bereich der forensischen Informatik keine „Muster"/„Vorlagen" oder „Formulierungshilfen" findet, an denen man sich orientieren könnte.

Konsequenzen einer schlecht formulierten Beweisfrage wären bspw., dass ein falsches Beweisthema erörtert wird, der Verlust der Vergütung, die Gefahr, dass der Sachverständige wegen Unverständnis den Prozess entscheidet, der Vorwurf der Befangenheit, ein Beweisverwertungsverbot oder die Prozessrolle als Zeuge und nicht als Sachverständigenbeweis.

aa) Das Problem der Kommunikation und Übersetzung

So wird ausgeführt, dass viele spektakuläre Fehlurteile, wie die Fälle Rohrbach, Hetzel und Meinberg, auf eine mangelhafte gemeinsame Verständigungsbasis zwischen Richter und Sachverständigen und daraus entstandenen falschen Schlussfolgerungen zurückzuführen sei.[565] Das liegt wohl in dem besonderen Verhältnis zwischen der Strafrechtsdogmatik und den um die Bestätigung oder Widerlegung des Dogmas bemühten empirischen Wissenschaften.[566] So sind die Ziele und Fragestellungen beider Bereiche grundsätzlich

563 *Sunde*, Non-technical Sources of Errors, S. 62.

564 *Dewald/Freiling*, Forensische Informatik, S. 95 f.

565 Vgl. etwa *Arbab-Zadeh*, NJW 1970, 1217 m. w. N.

566 Vgl. dazu *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 48 f. m. w. N.

verschieden: In einem Rechtsstreit geht es ausschließlich darum, rechtliche Fragen zu beantworten. Diese beziehen sich darauf, ob ein Rechtsverstoß stattgefunden hat und falls ja, welcher. Schlussendlich kann die rechtlichen Fragen nur das Rechtssystem bzw. der Richter beantworten. Die Aufgabe forensischer Gutachter ist es, die rechtlichen Fragen in wissenschaftliche Fragen zu übersetzen. Die Frage, ob ein Beschuldigter tatsächlich einen Mord begangen hat, kann bspw. in die Frage übersetzt werden, welche genetischen Sequenzen in den Blutspuren am Tatort gefunden werden können. Eine Antwort auf die wissenschaftliche Frage kann anschließend helfen, eine Antwort auf die rechtliche Frage zu finden. Allerdings hilft nicht jede wissenschaftliche Frage bei der Wahrheitsfindung. Der Nachweis, dass sich Blutspuren des Tatverdächtigen an seinen eigenen Schuhen befinden, hilft nicht notwendigerweise bei der Beantwortung der Frage, ob der Tatverdächtige den Mord begangen hat. Genauso wenig hilft es herauszufinden, dass sich auf der Tatwaffe mikroskopische Fasern aus der Kleidung des Opfers befinden, wenn der Tatverdächtige Kleidung trägt, die auch aus diesen Fasern besteht. Übersetzt man die rechtliche Frage in eine wissenschaftliche Frage, verliert man jeden Bezug zu den Begriffen Schuld und Unschuld. Forensische Wissenschaften suchen immer nach Verbindungen zwischen Objekten, beispielsweise zwischen dem Blut, das sich am Tatort und der Tatwaffe befindet, und dem Blut des Opfers und des Tatverdächtigen. Über die Relevanz und Bewertung und damit über Schuld oder Unschuld entscheidet ausschließlich das Gericht.[567] Dieses Spannungsverhältnis gipfelt in oft beobachteten emotionalen Äußerungen, Überheblichkeiten oder Borniertheiten gegenüber den anderen Wissenschaften.[568]

Diese Schwierigkeit ergibt sich zum einen aus der Unübersetzbarkeit zweier unabhängig voneinander für verschiedene Zwecke entwickelter Sprachsysteme. Zum anderen liegen den verschiedenen Rationalitätskonzepten der Richterinnen und der Sachverständigen irreduzible Vagheiten zugrunde, die zusätzlich die Übertragbarkeit der Ergebnisse der Sachverständigen in die richterliche Sachverhaltsermittlung und Würdigung erschweren.[569]

Ein Verständnis der Kommunikation zwischen Sachverständigem und Gericht setzt präzise Vorstellungen darüber voraus, dass einerseits geklärt werden muss, wie es dem Gericht möglich ist, dem Sachverständigen die Aufgabe zu übertragen, zu ermitteln, ob bestimmte Tatsachen vorliegen. Andererseits ist zu untersuchen, wie der Sachverständige diese Aufgabe in das Begriffssystem seines Wissenschaftszweiges übersetzt. Zuletzt muss umgekehrt klar sein,

---

567 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 26.

568 Vgl. *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 50 f. mit Beispielen und w. N.

569 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 1; vgl. zur Kommunikation auch *Mysegades*, Software als Beweiswerkzeug, S. 141.

wie das Gericht die durch den Sachverständigen ermittelten Tatsachen im Rahmen der Beweisaufnahme und -würdigung verwerten kann.[570]

Im Bereich der forensischen Informatik kommt noch die zusätzliche Anforderung der Übersetzung der Ergebnisse der Datenverarbeitungs- und -analysemethoden bzw. des Binärsystems in eine menschenlesbare Form.[571]

Die einzelnen Anforderungen kann man bildlich so darstellen:

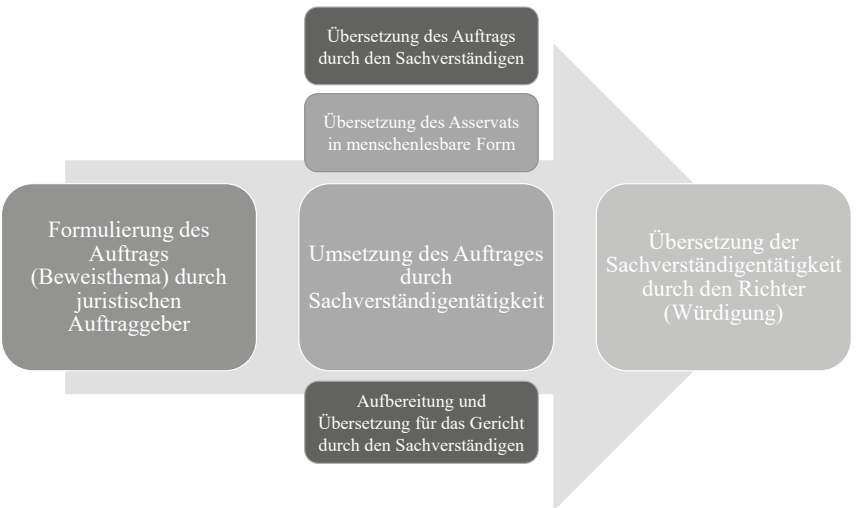


Abbildung 3: „Prozess des Auftrags“

Der Auftrag an den Sachverständigen ist möglichst so zu formulieren, dass der IT-Sachverständige mit seinem Begriffssystem daran anknüpfen kann. Bereits bei der Festlegung des Beweisthemas und noch mehr nach der Erhebung des Sachverständigenbeweises, ist es wichtig, dass die Gerichtspersonen und der Sachverständige „dieselbe“ Sprache sprechen, sonst scheitert die daran anknüpfende Kommunikation und damit auch die Umsetzung des Auftrages durch den Sachverständigen und die anschließende Übersetzung der Sachverständigentätigkeit durch die Gerichtsperson. Sie müssen Aussagen über denselben Gegenstand treffen.[572]

570 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 63.

571 Im Anschluss an die Formulierung des Beweisthemas im Auftrag erfolgen also vier Übersetzungsvorgänge. Das verdeutlicht die Relevanz einer interdisziplinären Kommunikationsbasis.

572 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 62.

Zumindest muss ein „Wörterbuch“ oder eine Art „Translater“ geschaffen werden, wie bestimmte Fachbegriffe in die Sprache des anderen übersetzt werden. Ein Beispiel aus einer anderen forensischen Disziplin wären die Störungs-Begriffe der §§ 20, 21 StGB. Diese sind keine medizinischen Begriffe. Der juristische Begriff der „krankhaften seelischen Störung“ ist im medizinischen Sinne eine Psychose, eine Neurose, ein pathologischer Rauschzustand oder eine organisch bedingte cerebrale Wesensveränderung. Analoges muss von den Verfahrensbeteiligten im Bereich der forensischen Informatik ebenso geschaffen werden. In anderen Rechtsordnungen gibt es für die Überbrückung dieser Sprachbarriere auch sog. Liasons, die beide Sprachen „sprechen“.[573] Für den Bereich der forensischen Informatik könnte das in einem ersten Schritt heißen, z. B. ein gemeinsames Verständnis für Spurenarten und deren Bedeutung zu schaffen. In diesem Rahmen gilt es zunächst Schlüsselbegriffe ausfindig zu machen, die von beiden Seiten gleich verstanden werden müssen (bspw. „Tatsache“; „Daten“; „Informationen“; „Beweis“; „Bits“; „Hashwerte“, „Zeitstempel“, etc.). Das ergibt sich nicht zuletzt aus der Besonderheit der Technologie – der Universalität und der Abgekoppeltheit von der physischen Welt – in der sich ständig neue Möglichkeiten der digitalen Welt auftun: Hochkomplexe Rechenmodelle müssen etwa bei virtuellen Währungen, wie Bitcoin, nachvollzogen werden. Ohne tiefes technisches Verständnis für die Abläufe kommt hier kein Strafverfolger weiter.[574] In der Praxis hat sich durchgesetzt, dass der Staatsanwalt im Rahmen eines Vorabgesprächs versucht, dem IT-Sachverständigen zu erklären, welche juristischen Kriterien für die Fallsachbearbeitung dienlich wären, vgl. auch Nr. 72 Abs. 2 S. 2 RiStBV. Der IT-Sachverständige versucht dann durch gezieltes Nachfragen, die konkreten juristischen Anforderungen in seine Domäne zu übersetzen, um das exakte Ziel des Auftrages und die dafür notwendigen technischen Mittel zur Erreichung des Ziels festlegen zu können.[575]

In rechtlich komplizierten Fällen erweist es sich zudem als nützlich, im Gutachtenauftrag kurz auf die rechtliche Problematik einzugehen bzw. wesentliche Tatbestandsmerkmale und Rechtsbegriffe zu erläutern, so wird bspw. im Zusammenhang mit einem psychiatrischen Gutachten zur Frage der Voraussetzungen der §§ 63 ff. StGB in einem Unterbringungsverfahren auf die erforderliche Gefährlichkeitsprognose näher eingegangen.[576]

---

573 Vgl. *Sunde*, Non-technical Sources of Errors, S. 62.

574 https://www.fau.de/2017/04/news/wissenschaft/nicht-alles-was-technisch-moeglich-ist-ist-auch-rechtlich-zulaessig/ [26.6.2023].

575 So auch die Einschätzung von Johannes Pollach M. Sc., IT-Forensiker bei der ZCB.

576 *Schirhakl*, Der Sachverständigenbeweis im neuen Strafprozessrecht, S. 152 f.

Auch hat man ein gemeinsames gültiges Kriterium, an dem man sich versuchen sollte zu orientieren: Das wichtigste Prinzip wissenschaftlichen Vorgehens (sowohl in der Rechtswissenschaft als auch in der Informatik und anderen) ist den Zweifel voranzustellen – das immer wieder Infragestellen scheinbar gesicherter Erkenntnis.[577] In der Wissenschaft darf es keine Dogmen geben, sie muss auf ständige Selbstkorrektur angelegt sein. So muss jede wissenschaftliche Annahme (Theorien, Modelle, Gesetze, usw.) so formuliert sein, dass sie an der Realität überprüft werden kann. Es müssen sich also objektive Daten gewinnen lassen, die die Aussage stützen oder widerlegen. Wissenschaft muss sich demnach öffentlich vollziehen: Empirische Beobachtungen müssen grundsätzlich für jedermann überprüfbar sein.[578] In diesem Sinne müssen die einzelnen Erkenntnisschritte des eigenen Gutachtens deutlich gemacht und dadurch ein „Optimum an Bedingungen für die Kommunikation“[579] hergestellt werden.

bb) Das Problem des „Primens“

Das Problem des „Primens“[580] besteht darin, dass schon die Fragestellung die (sachverständige) Beantwortung des Beweisthemas beeinflussen kann. Der Auftraggeber sollte also schon hier eine Idee haben, was er mit der Frage intendiert. Denn sie kann durchaus suggestiv wirken und damit die Unabhängigkeit des Sachverständigen einschränken. Auch ist natürlich möglich, dass mit der Fragestellung relevante alternative Hypothesen ausgeschlossen werden.

In diesem Hinblick hat der Auftraggeber also den richtigen Grad an „allgemein und speziell“ bzw. „offen und richtungsweisend“ zu finden.[581]

Um ein „Priming“ zu vermeiden, sollte der Auftraggeber immer auch explizit die Bearbeitung von Alternativhypothesen verlangen.[582] Die Wahrscheinlichkeit für ein gutes und weniger angreifbares Gutachten erhöht, wer die Sachverständigen aktiv Gründe suchen lässt, die gegen die eigene Hypothese

---

577 Vgl. auch *Köller/Nissen/Rieß/Sadorf*, Probabilistische Schlussfolgerungen im Schriftgutachten, S. 1.

578 *Köller/Nissen/Rieß/Sadorf*, Probabilistische Schlussfolgerungen im Schriftgutachten, S. 1.

579 So *Thomae*, Prinzipien und Formen der Gestaltung psychologischer Gutachten, S. 753.

580 Vgl. vertiefter dazu *Thaler/Sunstein*, Nudge, S. 29 ff.; *Kahnemann/Sibony/Sunstein*, Noise, S. 19 ff., 47 ff.

581 Vgl. dazu auch *Sunde*, Non-technical Sources of Errors, S. 62 f.

582 Siehe auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 385 f.: Bildung von Alternativhypothesen zur Vermeidung des Confirmation Bias; *Vogel/Volkmann*, GesR 2021, 753 (758 f.).

sprechen (was wissenschaftlich eigentlich ein Selbstverständnis sein sollte), und damit den Blick für Informationen schärft, die der ersten Erklärung widersprechen. Vorhandene Informationen werden so ausgewogener gewichtet; den Ursachen von Bestätigungstendenzen wird so besser entgegengewirkt.[583]

cc) Fazit

Die Wichtigkeit eines konkret formulierten Auftrags für den weiteren Verfahrensverlauf kann gar nicht genug hervorgehoben werden. Die Pflicht der genauen Umgrenzung und konkreten Fragestellung ergibt sich aus Nr. 72 Abs. 2 S. 1 RiStBV und § 78 StPO. Bei der Formulierung stellt sich der Bezug zu den Assoziationen i. S. d. forensischen Informatik als hilfreich dar. Auch sollte immer explizit die Bearbeitung von Alternativhypothesen verlangt werden.

Um der unzureichenden Praxis entgegnen zu können, müssen die Auftraggeber die Lücke in ihren Grundkenntnissen der forensischen Informatik schließen, dann konkretisiert sich auch die Frage nach dem „Was kannst du mir geben?“. Eine wichtige interdisziplinäre Aufgabe besteht auch darin ein gemeinsames Sprachverständnis zu schaffen, Schlüsselbegriffe ausfindig zu machen und einen „Translater“ für beide Seiten zu entwerfen.

d) Die verschiedenen Aussagekategorien des Sachverständigenbeweises

Entsprechend den drei Arten von Sätzen des Syllogismus sind drei verschiedene Kategorien von Beweisthemen denkbar, die von Hegler[584] und im Anschluss daran von Mezger[585] in der folgenden Reihenfolge genannt werden: 1) Das Bestehen von Erfahrungssätzen/Normen (als erste Aussagekategorie, Oberprämisse des Syllogismus)[586] bzw. Mitteilung abstrakter Ergebnisse aus dem Gebiet besonderer Sachkunde, 2) Schlussfolgerungen (zweite Aussagekategorie, Konklusion des Syllogismus)[587] bzw. Mitteilung von Schlussfolgerungen aus feststehenden konkreten Tatsachen des Prozesses mithilfe von Sachkunde, 3) Beobachtungen (dritte Aussagekategorie, Unterprä-

583 *Vogel/Volkmann*, GesR 2021, 753 (760).

584 AcP 104 (1909), 151 (165 ff.).

585 AcP 117 (1918), Beilageheft, S. 1 (8 ff.) // AcP 117 (1918), Beilageheft, 1, 10 ff.

586 Wenn er dem Gericht einzelne Erfahrungssätze seines Wissensbereichs ohne eigene Würdigung mitteilt.

587 Sachverständige werden wohl am häufigsten dafür eingesetzt, um aufgrund ihrer fachlichen Qualifikation Tatsachen in einem Gutachten zu beurteilen. Hier fehlt die Vertrauenswürdigkeit der Gerichtspersonen auch in Bezug auf eine eigenständige Auswertung des Datenmaterials.

misse des Syllogismus) bzw. Wahrnehmung von Tatsachen und Feststellung der Tatsachen, wenn dazu besondere Sachkunde erforderlich ist.[588]

In der Praxis werden die verschiedenen Kategorien häufig miteinander kombiniert.

Abbildung 4: „Die verschiedenen Aussagekategorien"

Aus dem eben Geschilderten wird umso deutlicher, wie wichtig es ist, dass der Sachverständige in den Teilen seines Gutachtens klar erkennen lässt, wie er Befunde ermittelt hat, Befundtatsachen, (3. Kategorie), von welchen wissenschaftlichen Annahmen er dabei ausgegangen ist, Erfahrungssätze, (1. Kategorie), und durch welche Schritte er bspw. die Verknüpfung seiner Untersuchung mit dem juristischen Begriff im Sinne der Beweisfrage ableitete, Schlussfolgerungen, (2. Kategorie ggf. mit juristischer Schlussfolgerung bzw. was aus Expertensicht Voraussetzung für eine entsprechende Schlussfolgerung wäre).

588 Vgl. *Stinshoff*, Operative Fallanalyse, S. 108; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 104 ff. v. a. S. 107 das Toulmin'sche Schema; SK-StPO/*Rogall*, Vor § 72 Rn. 80; *Hegler*, AcP 104 (1909), 151 (168); *Kühne*, Strafprozessrecht, Rn. 858.

Je nachdem, um welche Kategorie es sich handelt und welche Methode dabei gewählt wurde, müssen die Gerichte den Beweiswert einschätzen und entsprechend würdigen (d. h. mehr oder weniger ausführlich auf die Kausalbeziehungen und Ergebnisse des vom Sachverständigen untersuchten Beweisthemas und seiner Methodik eingehen). Deshalb ist es wichtig, die Kategorie schon so früh wie möglich festzulegen.

aa) Die erste Kategorie: Die Mitteilung von abstrakten Erfahrungssätzen

Die erste Kategorie ist die Mitteilung abstrakter Erfahrungssätze in Form allgemeiner Sätze einer Wissenschaft oder Kunst als generelle Oberprämisse.[589]

Dabei überliefert der Sachverständige generelle, theoretische Erkenntnisse[590] und praktische Erfahrungen[591]. Eine Beziehung zum verfahrensgegenständlichen Sachverhalt gibt es nicht. Das Erfahrungswissen wird vielmehr abstrakt angewendet.[592]

Allg. Erfahrungssätze umfassen bspw. Definitionen, Erklärungen von Fachausdrücken[593], Aussagen über das Wesen allgemeiner Erscheinungen, Überlieferung mathematischer Sätze, Übermittlung von Kausalgesetzen der Naturwissenschaften[594], Forschungsergebnisse und technisches Wissen[595], Buchführungsgrundsätze[596], Erkenntnisse oder praktische Regeln aus dem Wissens- und Erfahrungsgebiet des Sachverständigen, abstrakte Ergebnisse der

---

589 Vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 109 ff. mit einer sehr ausführlichen Beschreibung und Erklärung der syllogistischen Struktur, die in einem Urteil darzustellen ist, und den daran ausgerichteten Arten der Sachverständigenaussagen; SK-/StPO-*Rogall*, Vor § 72 Rn. 1; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 5; Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 6; KMR/*Neubeck*, Vor § 72 Rn. 7; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 371; *Hegler*, AcP 104 (1909), 151 (166 ff.); *Mezger*, AcP 117 (1918), Beilageheft, 1, 10 ff.; *Eb. Schmidt*, *II*, Vor § 72 Rn. 7; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 120.

590 Vor *Hegler*, AcP 104 (1909), 151 (166 ff., 166, Fn. 40 m. w. N.) bestand vielfach die Ansicht, Sachverständige würden ausschließlich solche abstrakten Erfahrungssätze liefern.

591 *Hegler*, AcP 104 (1909), 151 (167).

592 Vgl. auch Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 371.

593 *Hegler*, AcP 104 (1909), 151 (168); Stein, S. 22 ff.

594 *Hegler*, AcP 104 (1909), 151 (168).

595 Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 6; LR-Krause, Vor § 72 Rn. 1.

596 Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 6.

Geschichtswissenschaften[597] und die Mitteilung von Handelsbräuchen (vgl. auch § 114 GVG)[598].

Auch die Erläuterung ausländischen Rechts oder inländischen Gewohnheitsrechts kann eine Aussage der ersten Kategorie sein[599], nicht dagegen Aussagen über inländisches Gesetzesrecht (B. II. 3. b) bb)).[600]

Die Mitteilung erfolgt zur Feststellung der konkreten unmittelbar erheblichen Tatsachen des zugrundeliegenden Sachverhalts.[601] Sie soll dem Gericht ermöglichen, bestehende Tatsachen im Rahmen der Beweiswürdigung auszuwerten.[602] Bspw. ein bereits von einem anderen Sachverständigen erstattetes Gutachten, wissenschaftliche Veröffentlichungen oder etwa Allgemeines zu den Standards oder Begriffen der forensischen Informatik (vgl. dazu B. IV. 3.).[603] Aus den Entscheidungsgründen des LG Hamburgs (siehe B. IV. 3. c)) geht bspw. hervor, dass darunter auch Erklärungen, Lesehinweise und Definitionen im Gutachten des IT-Sachverständigen fallen können.

Im Zusammenhang mit der Mitteilung dieser Erfahrungssätze wird der Sachverständige regelmäßig sowohl die Verwendungsweise im konkreten Fall erklären, als auch aus welchen Hintergrundannahmen sich die Schlussregeln – der Erfahrungssatz – ergibt.[604]

Von Puppe wird in Bezug auf die erste Aussagekategorie kritisiert, dass ein allgemeingültiger Satz nicht vor Gericht bewiesen werden könne, da die dort zur Verfügung stehenden Mittel nicht zu seinem Beweis geeignet seien. Damit läge kein forensisch geführter Beweis, sondern lediglich eine Information über anderweitig geführte Beweise in den Fällen vor, in denen sich das

---

597 *Hegler*, AcP 104 (1909), 151 (169 ff.); *Mezger*, AcP 117 (1918), Beilageheft 1, 11; *Ulrich*, Der gerichtliche Sachverständige, Rn. 5; SK-StPO/*Rogall*, Vor 72, Rn. 81.

598 SK-StPO/*Rogall*, Vor § 72 Rn. 81; Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 6; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 371; *Hegler*, AcP 104 (1909), 151 (168).

599 Vgl. bspw. SK-StPO/*Rogall*, Vor § 72 Rn. 81; Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 6; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 12; KMR/*Neubeck*, Vor § 72 Rn. 2; *Eisenberg*, Beweisrecht der StPO, Rn. 1501; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 371; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 112; *Hegler*, AcP 104 (1909), 151 (184 ff.); *Mezger*, AcP 117 (1918), Beilageheft 1, 12 Fn. 20.

600 *Hegler*, AcP 104 (1909), 151 (191); *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 128; SK-StPO/*Rogall*, Vor § 72 Rn. 81; Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 6; *Eisenberg*, Beweisrecht der StPO, Rn. 1501; weitergehend Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 12; *Peters*, Strafprozess, S. 366.

601 *Mezger*, AcP 117 (1918), Beilageheft 1, 12.

602 *Mezger*, AcP 117 (1918), Beilageheft 1, 13; *Hegler*, AcP 104 (1909), 151 (182).

603 *Mezger*, AcP 117 (1918), Beilageheft 1, 11 f.

604 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 110.

Gericht mithilfe des Sachverständigenbeweises die Kenntnis von der Gültigkeit eines zweifelhaften Kausalgesetzes verschaffe. Das Kausalgesetz sei eine offenkundige Tatsache und mit den Mitteln des Prozessrechts könne man nur singuläre Tatsachen beweisen.[605] Wie Toepel dagegen zutreffend ausführt, besteht zwar eine große Nähe zwischen den mitgeteilten Erfahrungssätzen und offenkundigen Tatsachen. Das Gesetz sieht aber vor, dass ein Beweisantrag wegen Offenkundigkeit gem. §§ 244 Abs. 3 S. 3, 245 Abs. 2 S. 3 StPO abgelehnt werden *darf bzw. kann*.[606] Daraus folgt, dass ein Beweisantrag gerade nicht abgelehnt werden *muss* und eine Beweiserhebung dazu grds. möglich ist. Demnach kann mit den von Puppe angeführten Argumenten nicht hinreichend begründet werden, dass offenkundige Tatsachen nicht vor Gericht bewiesen werden könnten, z. B. durch wissenschaftliche Sekundärliteratur.[607]

bb) Die zweite Kategorie: Das Ziehen von Schlussfolgerungen aus konkreten Tatsachen des Prozesses mithilfe von Sachkunde

Die zweite Aussagekategorie umfasst die Mitteilung von Schlussfolgerungen aus konkreten Tatsachen des Prozesses mithilfe von Sachkunde.[608] Dabei kann der Sachverständige das Tatgericht bspw. bei deren Bewertung des vorhandenen Tatsachenstoffes unterstützen (Sachverhaltsbewertung).[609] Es handelt sich wohl um die häufigste und wichtigste Kategorie der Sachverständigenaussagen.[610] In diesem Fall wendet der Sachverständige seine Expertise

---

605 *Puppe*, JZ 1996, 318 (320).

606 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 111.

607 *Stinshoff*, Operative Fallanalyse, S. 110 f.; vertiefend dazu *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 111.

608 *Hegler*, AcP 104 (1909), 151 (195); *Mezger*, AcP 117 (1918), Beilageheft 1, 13; *Eb. Schmidt*, II, Vor § 72 Rn. 8; SK-StPO/*Rogall*, Vor § 72 Rn. 82; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 10; KK/*Senge*, Vor § 72 Rn. 3; Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 7; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 371; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 120; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 114.

609 *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 57.

610 *Mezger*, AcP 117 (1918), Beilagenheft 1, 13 ff.; *Eb. Schmidt* II, Vor § 72 Rn. 8; SK-StPO/*Rogall*, Vor § 72 Rn. 82; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 10; KK-*Senge*, Vor § 72 Rn. 3; Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 7; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 371; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 120. Grundlegend dazu auch *Hegler*, AcP 104 (1909), 151 (192 ff.), der diese Aussagekategorie als Aussage über das Resultat einer mithilfe besonderen Sachkunde vorgenommenen Denkoperation oder Schlussfolgerung bezeichnet; im Gegensatz zur bloßen Tradierung der Resultate besonderer Sachkunde und der reinen Übermittlung von Tatsachenwissen.

auf den konkreten, als feststehend vorausgesetzten Sachverhalt[611] an und zieht mithilfe seiner Sachkunde Schlussfolgerungen.[612] Er begutachtet den Einzelfall. Es handelt sich um das Ergebnis eines Denkprozesses.[613] Diese Kategorie umfasst daher ein „Mehr" gegenüber der ersten Aussagekategorie.[614]

Unter diese Kategorie fallen z. B. Mitteilungen über die Echtheit eines Gemäldes[615], die Beurteilung, ob ein neugeborenes Kind während oder nach der Geburt noch gelebt hat, die Beurteilung seiner Lebensfähigkeit außerhalb des Mutterleibes (vgl. § 90 StPO)[616] oder die Beurteilung, wie lange der Bremsweg eines Fahrzeugs mit bestimmten Defekten ist[617].

In der forensischen Informatik wären das bspw. Mitteilungen darüber, ob eine Bild- oder Textdatei manipuliert wurde oder ob die Cryptocurrency-Adresse der Person A zugeordnet werden kann[618].

Der zu bewertende Sachverhalt muss dem Sachverständigen vom Auftraggeber in Form von Anknüpfungstatsachen (siehe B. II. 3. b) cc)) mitgeteilt werden.[619] Soll der Sachverständige die Anknüpfungstatsachen selbst ermitteln, handelt es sich um eine Kombination der zweiten und dritten Aussagekategorie.[620] Beispiele dafür sind: Der psychologische Sachverständige, der von einem Strafverfolgungsorgan beauftragt wurde und eine Exploration durchführt, um die Glaubwürdigkeit eines Zeugen zu bestimmen; der medizinische Sachverständige, der den Beschuldigten zur Beurteilung von dessen physischem oder psychischem Zustand untersucht, um die für die Beurteilung erforderlichen Tatsachen zu erlangen, und der technische Sachverständige, der durch Untersuchung des Unfallwagens aufdecken soll, ob der Unfall auf dem

---

611 Bei psychiatrischen Gutachtern ist es deshalb wichtig, den Prozessverlauf zu verfolgen, da hier „feststehende Sachverhalte" (aus den Akten) häufig variieren oder sogar entscheidend verändert werden.

612 *Hegler*, AcP 104 (1909), 151 (193).

613 SK-StPO/*Rogall*, Vor § 72 Rn. 82.

614 Vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 114; SK-StPO/*Rogall*, Vor § 72, Rn. 82.

615 *Hegler*, AcP 104 (1909), 151 (198); *Henkel*, Strafverfahrensrecht, S. 217; SK-StPO/*Rogall*, Vor § 72 Rn. 82.

616 *Hegler*, AcP 104 (1909), 151 (198); SK-StPO/*Rogall*, Vor § 72 Rn. 82.

617 *Henkel*, Strafverfahrensrecht, S. 217; SK-StPO/*Rogall*, Vor § 72 Rn. 82.

618 Vgl. hierzu auch Auch *Deuber et al.*, Argumentation Schemes for Blockchain Deanonymization (vorgestelltes Paper bei JURISIN 2022), https://doi.org/10.48550/arXiv.2305.16883 [26.6.2023].

619 Z. B. durch Akteneinsicht, Zuziehung zu der Inaugenscheinnahme oder Anhörung der Zeugenvernehmung, vgl. auch schon *Hegler*, AcP 104 (1909), 151 (194) m. w. N.

620 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 114.

Zustand des Fahrzeugs beruhe.[621] Oder im Bereich der forensischen Informatik z. B. die Untersuchung dahingehend, ob eine bestimmte Hardware überhaupt in der Lage ist, ein bestimmtes Netzwerk aufzubauen.

Der zu beurteilende Sachverhalt wird bei der Mitteilung von Schlussfolgerungen als wahr vorausgesetzt. Demnach handelt es sich bei den Schlussfolgerungen um hypothetische Aussagen.[622] Das Sachverständigengutachten dient in dieser Aussagekategorie dazu, die Richtigkeit der Schlussfolgerung unter der als richtig vorausgesetzten Prämisse zu verifizieren. Die Richtigkeit der Prämisse zu beurteilen soll dagegen nicht Aufgabe des Sachverständigen sein, es sei denn, die Prüfung der Prämisse ist auch Teil der Fragestellung.[623]

Die Schlussfolgerungen können in dem Prozess zum einen der Feststellung prozesserheblicher Tatsachen dienen. Das soll z. B. dann der Fall sein, wenn der Sachverständige auf das Vorhandensein einer tatsächlichen psychischen Erkrankung schließt oder erklärt, dass ein bestimmtes Verhalten nach psychiatrischer Erfahrung nicht vorgetäuscht sein kann.[624]

Zum anderen (und i. d. R.) dienen die Schlussfolgerungen der Subsumtion konkreter, rechtserheblicher Tatsachen unter die abstrakten Rechtssätze. So z. B. Diagnosen im weitesten Sinne[625] derart, dass die vorliegende Handlung eine unwiderstehliche Zwangshandlung, das gelieferte Öl mangelfreie Ware, eine Operation indiziert, die Steuerungsfähigkeit einer Person eingeschränkt sei, oder der Angeklagte die kinder- und jugendpornographischen Dateien wissentlich besessen hat.

Auch hier kann aber die juristische Sachkunde nicht Gegenstand des Sachverständigenbeweises sein – jedenfalls in Bezug auf inländisches Recht (s. o. bei II. 3. b) bb)).

---

621 Beispiele aus Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 10; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 372; *Toepel*, Grundstrukturen des Sachverständigenbeweises S. 114.

622 *Bennecke/Beling*, Lehrbuch des Deutschen Reichs-Strafprozessrechts, S. 363; *Hegler*, AcP 104 (1909), 151 (194); *Mezger*, AcP 117 (1918), Beilageheft 1, 14 f. Kritisch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 114, der die Ausdrucksweise irreführend findet und unter Verweis auf „Toulmins Backing" ausführt, dass sich die Schlussregeln immer nur relativ zu bestimmten Hintergrundannahmen verhalten.

623 So muss erst die Prämisse „hat jemand eine bestimmte Störung" geprüft werden, um die Folgerung zu ziehen, ob er dadurch in seiner Steuerungsfähigkeit eingeschränkt sein könnte; vgl. dazu auch *Hegler*, AcP 104 (1909), 151 (194); vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 114.

624 *Mezger*, AcP 117 (1918), Beilageheft 1, 15.

625 *Hegler*, AcP 104 (1909), 151 (199); *Mezger*, AcP 117 (1918), Beilageheft 1, 13 ff.

Werden bei der Schlussfolgerung aus den konkreten Tatsachen gleichzeitig auch abstrakte Erfahrungssätze mitgeteilt, handelt es sich um eine Kombination der ersten und zweiten Aussagekategorie.[626]

Hier werden v. a. Unterschiede zu anderen Beweismitteln deutlich: Die Zeugenvernehmung sowie der Augenscheins- und Urkundenbeweis liefern lediglich Tatsachen, aus denen die Gerichtspersonen selbst Schlüsse ziehen. Solche Informationen füllen damit Lücken in dem Datenmaterial, welches den Ausgangspunkt für die Beurteilung des Sachverhalts bildet.[627]

cc) Die dritte Kategorie: Die Ermittlung konkreter Tatsachen, zu deren Wahrnehmung bzw. Feststellung besondere Sachkunde benötigt wird

Bei der dritten Aussagekategorie handelt es sich um die Mitteilung über konkrete Tatsachen mit Beziehung auf den Prozess (sog. Befundtatsachen)[628], zu deren Wahrnehmung bzw. Feststellung besondere Sachkunde benötigt wird.[629] Der Sachverständige hilft im Sinne dieser Kategorie u. a. dabei den Beweisstoff zu generieren, der als Ergebnis der Beweisaufnahme für die tatgerichtliche Sachverhaltsfeststellung zur Verfügung steht (Sachverhaltsaufklärung).[630] Der Unterschied zur zweiten Kategorie besteht darin, dass eine sachverständige Bewertung bzw. Würdigung dieser Wahrnehmungen unterbleibt.[631]

Unter diese Kategorie sind bspw. Mitteilungen darüber zu fassen, dass einer Leiche entnommene Teile bestimmte Giftstoffe enthalten, Feststellungen zur BAK[632] oder dass eine Röntgenaufnahme bestimmte Unregelmäßigkeiten zeigt.[633] Im Bereich der forensischen Informatik wären das z. B. die Feststellung von Schad- oder sonstiger Software oder das Auffinden von „unüblichem“ Datenmaterial in nicht unerheblicher Menge auf einem Datenträger (wie fragwürdige Bildersammlungen von Kindern).

---

626 *Hegler*, AcP 104 (1909), 151 (202) mit weiteren, vertiefenden Ausführungen zu unterschiedlichen Konstellationen.

627 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 58.

628 Siehe in diesem Teil, B. II. 3. b) cc).

629 *Hegler*, AcP 104 (1909), 151 (207 ff.); *Mezger*, AcP 117 (1918), Beilageheft 1, 16 ff.; SK-StPO/*Rogall*, Vor § 72 Rn. 82; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 9; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 370; KMR/*Neubeck*, Vor § 72 Rn. 6; *Eb. Schmidt*, II, Vor § 72 Rn. 2; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 116.

630 *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 57.

631 *Mezger*, AcP 117 (1918), Beilageheft 1, 14.

632 SK-StPO/*Rogall*, Vor § 72 Rn. 83.

633 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 116.

Dem Richter fehlt für eine selbstständige Wahrnehmung die erforderliche Sachkunde.[634] Der Sachverständige untersucht deshalb für das Gericht und übernimmt insofern den gerichtlichen Augenschein.[635] Die erforderliche Sachkunde umfasst in diesen Fällen neben den überdurchschnittlichen Kenntnissen im Bereich der Wissenschaft und Kunst insbesondere die zur Wahrnehmung erforderlichen Fähigkeiten in Form von Vorkenntnissen für eine gesteigerte Aufmerksamkeit für das Wesentliche oder dessen Bloßlegung.[636] Die besondere Sachkunde befähigt somit zur besonderen Wahrnehmung und zum Bericht über den damit erhobenen Befund.[637]

So ist ein Arzt zu bestimmten Feststellungen in Bezug auf eine Röntgenaufnahme deutlich befähigter als ein Laie.[638] Als Beispiel wird ein Bericht von Pupillenstarre und von Reflexstörungen von Paralytikern angeführt.[639] Über die Pupillenstarre oder die Abbildungen auf dem Röntgengerät könnten wahrscheinlich auch Laien berichten, allerdings wäre die Wahrscheinlichkeit, dass relevante Vorgänge oder Interpretationen missachtet oder übersehen würden, viel höher. Es kann deshalb nicht ausschließlich nur auf die Wahrnehmung bestimmter Tatsachen mit besonderer Sachkunde ankommen. Vielmehr kann damit nur die Interpretation und Fixierung des Wahrgenommenen gemeint sein.[640] Eben das gilt regelmäßig auch für die oft umstrittene Durchsicht von Datenträgern durch IT-Sachverständige (dazu später bei B. IV. 3.).

Auch diese Wahrnehmungen enthalten bis zu einem gewissen Grad Schlussfolgerungen (siehe dazu B. III. 2.). In Abgrenzung zur zweiten Kategorie ist eine reine Tatsachenwahrnehmung (dritte Kategorie) dann gegeben, wenn die denkende Verarbeitung lediglich etwas Selbstverständliches, ohne Weiteres als zutreffend zu Unterstellendes, Nebensächliches ist.[641] Eine Kombination aus zweiter und dritter Aussagekategorie ist dagegen immer dann gegeben,

---

634 *Hegler*, AcP 104 (1909), 151 (193 ff., 209).

635 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 116.

636 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 277; *Hegler*, AcP 104 (1909), 151 (193 f., 209 f.); *Mezger*, AcP 117 (1918), Beilageheft 1, 16.

637 *Mezger*, AcP 117 (1918), Beilageheft 1, 16.

638 Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 5; *Gössel*, DRiZ 1980, 363 (364).

639 *Mezger*, AcP 117 (1918), Beilageheft 1, 16.

640 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 277; Siehe dazu auch *Stinshoff*, Operative Fallanalyse, S. 115; oder SK-StPO/*Rogall*, § 85 Rn. 7; RGSt 44, 11, 14, der von „Wahrnehmung und Erkenntnis“ spricht.

641 *Hegler*, AcP 104 (1909), 151 (193 ff., 207); weitere Beispiele dazu in *Mezger*, AcP 117 (1918), Beilageheft 1, S. 14 f.: Teilt der Sachverständige lediglich seine Wahrnehmungen aus einem Gespräch mit einem Patienten mit, die er aufgrund seiner Sachkunde in Erfahrung bringen konnte (ohne diese zu bewerten), handelt es sich um die dritte Aussagekategorie. Bewertet er diese Tatsachen schließlich und stellt eine Diagnose, handelt es sich um eine Aussage aus der zweiten Kategorie.

wenn der Sachverständige sowohl den Sachverhalt feststellt als auch sachverständig würdigen soll.

Ein Angriff gegen das Gutachten in Bezug auf die dritte Aussagekategorie kann nur erfolgreich sein, wenn gerügt wird, dass nicht richtig oder nicht vollständig beobachtet/wahrgenommen (ausgewertet) wurde.[642]

Da auch der Zeuge Tatsachen unter Zuhilfenahme besonderer Sachkunde wahrnehmen und darüber vom Gericht vernommen werden kann (sog. sachverständige Zeugen), führt eben diese Aussagekategorie zu der Schwierigkeit einer deutlichen Abgrenzung des Sachverständigen vom sachverständigen Zeugen.[643] Darauf wird an späterer Stelle vertieft eingegangen (B. III. 2.).

dd) Die Vornahme bloßer Verrichtungen

Ein großer Teil der Literatur[644] ist der Ansicht, dass auch die Vornahme bloßer Verrichtungen zur Tätigkeit des Sachverständigen gehören könnte, wenn diese Tätigkeit eine Sachkunde voraussetzt, die dem Gericht fehlt, wie etwa die Entnahme von Blutproben und Röntgenuntersuchungen.[645]

Eine bloße Verrichtung ist dann gegeben, wenn der Sachverständige im Anschluss an diese Handlung keine weitere Wahrnehmung, Begutachtung oder Auswertung vornimmt.[646]

Ein anderer Teil der Literatur[647] lehnt diese Ansicht mit der Begründung ab, dass, auch wenn diese Verrichtungen eine gewisse fachliche Kompetenz erfordern, sie lediglich der Vorbereitung eines Gutachtens dienen.[648] In diesen Fällen kommt es dem Gericht nicht auf das Blutabnehmen oder die Erstellung der Röntgenaufnahmen für die Beurteilung des Beweisthemas an, sondern

---

642 *Hegler*, AcP 104 (1909), 151 (218); SK-StPO/*Rogall*, Vor § 72 Rn. 83.

643 Vgl. *Stinshoff*, Operative Fallanalyse, S. 116; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 116.

644 Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 7; Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 4; KK/*Senge*, Vor § 72 Rn. 2; KMR/*Neubeck*, Vor § 72 Rn. 5; *Pfeiffer*, Vor §§ 72–93 Rn. 1; *Dippel*, Die Stellung des Sachverständigen im Strafprozess), S. 119; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 369.

645 Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 4; KK/*Senge*, Vor § 72 Rn. 2; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 7; *Pfeiffer*, Vor §§ 72–93 Rn. 1.

646 Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 369.

647 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 274; *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 28; SK-StPO/*Rogall*, Vor § 72 Rn. 79, 82; vgl. auch *Stinshoff*, Operative Fallanalyse, S. 116.

648 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 274; *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 28; SK-StPO/*Rogall*, Vor § 72 Rn. 79 vgl. auch *Stinshoff*, Operative Fallanalyse, S. 116.

vielmehr auf den zweiten Schritt, auf die Beurteilung der Blut- und Röntgenergebnisse durch den Sachverständigen.[649] Dem Gericht fehlt hier also lediglich der *Zugang* zum Tatsachenstoff. Erst der zweite Schritt des Blutabnehmens, die Beurteilung der Blutergebnisse durch den Sachverständigen,[650] versetzt das Gericht in die Lage den Sachverhalt zu bewerten.[651] Nur wenn das Ergebnis aus sich selbst heraus verständlich ist, braucht es keine Begutachtung mehr. Dann muss aber der durch die Vornahme erzeugte Gegenstand als Augenscheinsobjekt in das Verfahren eingeführt werden.[652]

Bei der forensischen Informatik ist jedoch besonders, dass bereits der erste Schritt (der Zugang) zu den Informationen, also die Sicherung und „Entnahme" von Datenmaterial die Auswertung erheblich beeinflussen kann, während man annimmt, dass eine Blutentnahme zur BAK in der Regel sachgerecht vorgenommen wurde. D. h. insbesondere für die sachverständige Tätigkeit im Bereich der forensischen Informatik können auch bloße Verrichtungen im Einzelfall Sachverständigentätigkeit sein. Es ist zu differenzieren, ob eine Person aufgrund ihrer besonderen Fähigkeiten mit der Wahrnehmung eines Sachverhalts beauftragt wird, weil dem Gericht diese Fähigkeit fehlt, sich den Zugang zur Wahrnehmung zu verschaffen, z. B. weil eine Tür nur mit Spezialkenntnissen geöffnet werden kann.[653] Das soll nicht automatisch zu einer Sachverständigenposition der Beweisperson führen. Sie kann vielmehr auch Augenscheinsgehilfe sein.[654] Es ist darauf abzustellen, ob für die Vornahme dieser Verrichtung eine „einfache"[655] Sachkunde ausreichend ist (dann Augenscheinsgehilfe).[656] Wenn dagegen eine besondere Sachkunde für die Wahrnehmung erforderlich ist und dem Gericht diese fehlt, handelt es sich um eine Aussage der dritten Kategorie.[657]

---

649 *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 28.

650 Beispiel bei SK-StPO/*Rogall*, Vor § 72 Rn. 79.

651 *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 28; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 274; SK-StPO/*Rogall*, Vor § 72 Rn. 79, 82.

652 *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 28.

653 Beispiel aus SK-StPO/*Rogall*, Vor § 72 Rn. 92.

654 SK-StPO/*Rogall*, Vor § 72 Rn. 92, 97; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 274.

655 Siehe in diesem Teil B. II. 2. c) bb).

656 Die in der Literatur aufgeführten Beispiele, wie die Blutabnahme oder die Erstellung eines Röntgenbildes, können zwar in der Regel keine Richter, aber doch ein Großteil der Vertreter des entsprechenden Berufsstandes vornehmen, was aber für die Begründung einer besonderen Sachkunde nicht ausreicht.

657 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 274 f.

ee) Fazit

So ergeben sich für den IT-Sachverständigen im Strafverfahren grundsätzlich *vier* konkrete Aufgabenfelder: Die Aufgabe des Sachverständigen kann 1) in der Vornahme einer bloßen Verrichtung, wie etwa im Falle einer Blutprobenentnahme oder Röntgenuntersuchung bestehen, wenn hierfür eine besondere (im Beispielsfall: medizinische) Qualifikation erforderlich ist und daher die Tätigkeit bereits dem Grunde nach nicht seitens der Ermittlungsbehörden selbst erbracht werden kann (vgl. § 81a Abs. 1 S. 2 StPO). Das gilt v. a. für die IT-forensische Sicherung von Datenträgern, die z. T. technologisch besondere Sachkunde erfordern (Stichwort: „selective imaging", Vermeidung „antiforensischer Maßnahmen", siehe dazu auch später im 3. Teil) und erhebliche Auswirkungen auf die spätere Analyse haben kann. Nach derselben Maßgabe kann 2) auch die Feststellung von Tatsachen bzw. Befundermittlung (z. B. die Bestimmung der Blutalkoholkonzentration) Gegenstand der Sachverständigentätigkeit sein. Ein Beispiel für die forensische Informatik ist das Auflisten aller sich auf einem Datenträger befindlichen inkriminierten Dateien. Ferner kann sich die Sachverständigentätigkeit 3) auf die Übermittlung von bloßem Fachwissen beschränken; wie z. B. die Erläuterung von Begriffen aus der forensischen Disziplin. Der letzte (und häufigste) Fall einer Sachverständigentätigkeit ist 4) die Beurteilung von Tatsachen eines bestimmten (im Wege der Leitung nach § 78 StPO bereitgestellten) Sachverhalts auf der Grundlage besonderen Fachwissens; ob bspw. eine Datenveränderung mithilfe von (Schad)-Software vollzogen wurde i. S. d. §§ 303a, b StGB.

Doch sind von der Bereitstellung besonderer Sachkunde durch den Sachverständigen solche Tätigkeiten zu unterscheiden, die sich funktional als Ermittlungshandlungen darstellen. Regelmäßig lassen sich diese daran erkennen, dass sie gerade keine besondere Sachkunde erfordern und/oder mit einer wertenden Initiative zugunsten oder zulasten des Beschuldigten verbunden sind.

III. Die Abgrenzung zu anderen Prozessrollen

Die bisher herausgearbeitete Funktion des Sachverständigen muss nun von derjenigen anderer im Prozess auftretenden Personen und Beweismittel abgegrenzt werden. Eine Abgrenzung ist deshalb so wichtig, weil die Grundsätze des Strengbeweisverfahrens eine eindeutige Bestimmung der Auskunftsperson erfordern. Das Gesetz unterscheidet dabei streng zwischen den verschiedenen (persönlichen) Beweismitteln und ordnet jeweils unterschiedliche Rechtspflichten an.[658] Ist keine Sachverständigenposition entstanden, können

die Vorschriften des Sachverständigenbeweises auch keine analoge Anwendung finden.[659] Deshalb ist eine Abgrenzung von vornherein sehr wichtig. Es haben sich zwar schon andere Arbeiten im Zusammenhang mit dem Sachverständigenbeweis ausführlich mit den Abgrenzungsfragen beschäftigt.[660] Aufgrund der Aktualität und der Besonderheiten der IT sollen in dieser Arbeit jedoch die wichtigsten Ausführungen zur Abgrenzung dargestellt und auf den IT-Sachverständigen übertragen werden. Auch scheint das Thema – trotz der stattgefundenen wissenschaftlichen Aufarbeitung – zumindest in Bezug auf den IT-Sachverständigenbeweis – noch nicht einheitlich beantwortet werden zu können. So wird derzeit eine Auseinandersetzung vor deutschen Strafgerichten und in der Literatur über die Prozessrolle des IT-Sachverständigen in Abgrenzung zum Zeugenbeweis im Hinblick auf die Qualitätsanforderungen und Vielseitigkeit ihrer Tätigkeit geführt (siehe dazu in diesem Teil, B. IV.).

Die seit Inkrafttreten der Rechtsstrafprozessordnung im Jahr 1877[661] bis heute bestehenden Schwierigkeiten bei der Abgrenzung zwischen Sachverständigen und Zeugen sind insbesondere der historischen Entwicklung des Sachverständigenbeweises geschuldet.[662] Die sog. arbitri (die Sachverständigen des 19. Jahrhunderts) konnten vom Richter beauftragt werden, diesen nicht nur zu unterstützen, sondern den ganzen Prozess an seiner Stelle zu entscheiden.[663] Damals scheinen die Sachverständigen also die Stellung von Richtern innegehabt zu haben.[664] Als Nachwirkung sprachen auch einige Autoren vom „Richter des Faktums", wenn es um den Sachverständigenbeweis ging.[665] Andererseits wurde der Begriff „sachverständige Person" auch mit der prozessualen Position des Zeugen in Verbindung gebracht.[666] Aus dieser historischen Entwicklung wurde zum einen der Schluss gezogen, es handle sich um einen Beweis eigener Art, der in engem Zusammenhang mit der rich-

---

658 Vgl. auch *Ulrich*, Der gerichtliche Sachverständige, Rn. 19; *Eb. Schmidt*, II, Vor § 72 Rn. 4 ff.; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 377.

659 Näher dazu *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 284 ff.

660 Vgl. v. a. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 257 ff.; *Stinshoff*, Operative Fallanalyse, S. 61 ff.

661 Zur Entstehung vgl. auch *Glaser*, Handbuch, S. 188 ff.

662 Vgl. auch *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 7, 11; *Pawlak*, Ablehnung des Sachverständigen, S. 55; SK-StPO/*Rogall*, Vor § 72 Rn. 2; Löwe/Rosenberg/*Krause*, Vor § 72 StPO Rn. 1; vertiefend dazu auch *Stinshoff*, Operative Fallanalyse, S. 85 ff., 171 ff.

663 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 260.

664 *Glaser*, Handbuch, S. 677 f.

665 Auch „iudex facti", vgl. *Gönner*, Handbuch des gemeinen Prozesses Bd. 2, S. 432; *Grolman*, Theorie des gerichtlichen Verfahrens, § 84b; *Mittermaier*, AcP 2 (1819), S. 119 (221 ff.).

666 So in Art. 147 CCC; vgl. dazu auch *Zachariae*, Handbuch Bd. 2, S. 425, Fn. 12.

terlichen Augenscheinseinnahme stehe,[667] und zum anderen wurde die Forderung laut, die Beurteilung des Sachverständigen nach den Grundsätzen des Zeugenbeweises zu handhaben[668] – so wie es auch im angloamerikanischen Recht der Fall ist.[669] Die Schwierigkeit, die Rolle des Sachverständigen zu fassen, wird also schon aus der historischen Betrachtung deutlich. Eine entsprechende Charakterisierung zeichnet sich ab, wenn zwischen den Entstehungsbedingungen für die Sachverständigenposition und den daran geknüpften Rechten und Pflichten getrennt wird. Deshalb wird im Folgenden auf die Frage eingegangen, wann neben der Rolle des Sachverständigen eine Person Richterin, Zeugin oder Augenscheinsgehilfin ist, um dann die jeweiligen Tätigkeiten der IT-Sachverständigen einordnen zu können.

1. Die Abgrenzung zu Richterinnen

Zunächst kann die Sachverständigenposition (wie die Auffassung eines „iudex facti") im Hinblick auf die Entstehungsgeschichte nicht mit der Stellung des Richters verglichen werden, da insoweit das Recht auf den gesetzlichen Richter i. S. d. Art. 101 Abs. 1 S. 2 GG entgegenstünde. Daraus wird abgeleitet, dass der zur Entscheidung berufene Richter im Voraus durch generelle Regelungen festgelegt wird.[670] Ob ein Sachverständiger bestellt werden soll und welche Beweisthemen er zu bearbeiten hat, bestimmt hingegen erst die Staatsanwaltschaft im Ermittlungsverfahren bzw. das erkennende Gericht in der Hauptverhandlung – und zwar aus Anlass des Einzelfalls.[671]

Daran ändern auch die Verweisungen bspw. auf § 24 StPO nichts. Der Sachverständige steht dem Richter hinsichtlich seiner Tätigkeit zwar sehr nahe, indem er dessen Überzeugung durch Informationen über die möglichen Schlussfolgerungen und die anzuwendenden Erfahrungssätze vorbereitet. Aus diesem Grund soll Mängeln an der Objektivität in ähnlichem Umfang vorgebeugt werden wie bei Richterinnen selbst. Der Verweis ist also mit der Bedeutung der Informationen für die jew. Gerichtspersonen zu erklären und gerade nicht damit, dass die Sachverständigenposition selbst als Richterposition betrachtet werden soll.[672]

Auch bzgl. der Rechte hinsichtlich der Urteilsfindung unterscheidet sich die Richterposition erheblich von der des Sachverständigen. Der zuständige Rich-

---

667 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 261 m. w. N.

668 Vgl. *Schneider*, Lehre vom Beweise, § 176.

669 Vgl. *Zuckerman*, Principles, S. 62 ff.

670 St. Rspr.: BVerfGE 17, 294 (298 ff.); 19, 52 (59); 30, 149 (152); 40, 268 (271); 48, 246 (253); 63, 77 (79); 82, 286 (298); *Maunz/Dürig/Maunz*, Art. 101 Rn. 5.

671 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 262.

672 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 263.

ter ist nach der Konzeption des § 261 StPO *allein* dazu berufen, an der konstitutiv den Sachverhalt feststellenden Entscheidung mitzuwirken. Nicht ganz so eindeutig scheint das in den Fällen zu sein, in denen für eine richterliche Überzeugungsbildung kein Raum bleibt. So bspw. bei der zwangsweisen Anwendung von gesicherten wissenschaftlichen Erkenntnissen, die nach dem gegenwärtigen Stand der Forschung zum gesicherten Wissen gezählt werden können (dazu später im 4. Teil, A. III. 4. b) cc) (2) (a)). Allerdings ist auch hier das Gericht nicht an die Autorität des Sachverständigen gebunden – vielmehr folgt das Tatgericht in solchen Fällen dem Zwang des übermittelten Stands der Forschung (der auch nicht mit der Ansicht des jeweiligen Sachverständigen übereinstimmen muss). Die Person des Sachverständigen ist für den Entscheidungsprozess unmaßgeblich. Das ergibt sich deutlich daraus, dass der Sachverständige dem Richter bei auftretenden Vagheitsintervallen[673] Unsicherheiten berichten muss. Er ist nicht zur selbstständigen Auflösung von Unklarheiten befugt. Das Gericht sollte sogar von sich aus nach Unsicherheiten fragen.[674] Auch wenn die Praxis diesen Anforderungen oft nicht nachzukommen scheint, wenn sie bspw. Gutachten in Bezug auf das Vorliegen rechtlicher Merkmale in Auftrag gibt (siehe oben bei II. 3. b) bb)),[675] ändert sich nichts an der alleinigen Autorität zur Entscheidungsfindung durch das Gericht. Der Sachverständige stellt eine Durchgangsstation für den Fluss der Informationen zum Gericht dar. Im Urteil erscheint diese nicht als selbstständige Entscheidungsposition. Wenn sich in der Praxis eingebürgert hat, die Formulierung zu wählen, „nach den überzeugenden Ausführungen des Sachverständigen Cooper“[676] sei das Gericht zu einem bestimmten Ergebnis gelangt, so besitzt diese Floskel keinerlei Bedeutung, die etwa einer Revisionsrüge vorbeugen könnte. Es kommt nicht darauf an, dass der Sachverständige Cooper Ausführungen zu dem Beweisthema getroffen hat, sondern allein darauf, dass und v. a. warum seine Darlegungen überzeugend waren.[677]

2. Die Abgrenzung zu (sachverständigen) Zeugen

Nicht als ganz so eindeutig gestaltet sich eine Grenzziehung zwischen der Sachverständigen- und Zeugenrolle im deutschen Strafverfahren.

---

673 Vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 153 f., 211, 232.

674 Vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 214 f.

675 So häufig in Bezug auf die Schuldfähigkeit; vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 132, 218.

676 Vgl. auch Kemptener Bitcoin Fall im 4. Teil.

677 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 263 f.

a) Die Rolle des (sachverständigen) Zeugen im Strafverfahren

Zeuge i. S. d. §§ 48 ff. StPO ist nach der wohl herrschenden Definition eine Beweisperson, die in einem nicht gegen sie selbst gerichteten Strafverfahren Auskunft über die Wahrnehmung von Tatsachen gibt.[678] Gem. der Manifestation des Willens der Strafverfolgungsbehörden bzgl. der Prozessstellung, soll in der Ladung kenntlich gemacht werden, dass die Person als Zeuge geladen wird, vgl. Nr. 64 Abs. 1 S. 1 RiStBV.[679]

Gegenstand des Zeugenbeweises ist (entsprechend der oben dargelegten Definition) die Bekundung von wahrgenommenen Tatsachen. Der subjektive Personalbeweis ist dabei die wichtigste Funktion des Zeugen. Er kann aber auch Gegenstand des objektiven Personalbeweises sein, wie einer Augenscheinseinnahme oder körperlichen Untersuchung.[680] Der Zweck der Vernehmung ist die Abschöpfung des gesamten verfahrensrelevanten Wissens des Zeugen[681], der über exklusives Tatsachenwissen verfügt.[682]

Beweisaufgabe und Pflicht des Zeugen ist es, seine Tatsachenwahrnehmungen zu der verhandelten Straftat wahrheitsgemäß zu bekunden, §§ 153 ff. StGB, § 57 S. 1 StPO.[683] Entsprechend des hier zugrunde gelegten Tatsachenbegriffs (siehe B. I. 2.) kann der Zeuge nur über Begebenheiten und Zustände aussagen, die sinnlich wahrnehmbar sind.[684] Die Tatsachen können positiv bzw. negativ oder äußerlich bzw. innerlich sein.[685] Auch Hypothesen können Tatsachenwahrnehmungen sein, aber nur, sofern sie auf das eigene Denken und Handeln bezogen sind.[686] Nicht erfasst vom Zeugenbeweis sind hingegen reine Prognosen, Meinungen, Schlussfolgerungen (bspw. auf ein

---

678 RG DStrR 1934, 345, 346; BGHSt 22, 347 f.; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 303; Löwe/Rosenberg/*Ignor/Bertheau*, Vor § 48 Rn. 3; Meyer-Goßner/*Schmitt*, Vor § 48 Rn. 1; KMR/*Neubeck*, Vor § 48 Rn. 1; AwK-*Krekeler/Werner*, Vor § 48 Rn. 1; *Kindhäuser*, Strafprozessrecht, § 21 Rn. 6; *Eisenberg*, Beweisrecht der StPO, Rn. 1003, 1005; SK-StPO/*Rogall*, Vor § 48 Rn. 11.

679 *Stinshoff*, Operative Fallanalyse, S. 63.

680 SK-StPO/*Rogall*, Vor § 48 Rn. 128 ff.

681 SK-StPO/*Rogall*, Vor § 48 Rn. 164.

682 SK-StPO/*Rogall*, Vor § 48 Rn. 86.

683 SK-StPO/*Rogall*, Vor § 48 Rn. 134; Löwe/Rosenberg/*Ignor/Bertheau*, Vor § 48 Rn. 16; KK/*Senge*, Vor § 48 Rn. 3; *Pfeiffer*, Vor §§ 48 – 71 Rn. 1.

684 So auch Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 336.

685 Löwe/Rosenberg/*Ignor/Bertheau*, § 48 Rn. 5; SK-StPO/*Rogall*, Vor § 48 Rn. 16; KK/*Senge*, Vor § 48 Rn. 1; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 337 ff.

686 Meyer-Goßner/*Schmitt*, Vor § 48 Rn. 2; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 340.

bestimmtes weiteres Geschehen aus den Wahrnehmungen) oder Werturteile.[687] Auch Fragen danach dürfen vom Zeugen verweigert werden.[688] Problematisch insoweit ist jedoch, dass eine klare Trennung von Tatsachen und Wertungen bzw. Schlussfolgerungen nicht immer möglich ist. So beurteilt der Verstand fast jede Wahrnehmung bis zu einem gewissen Grad, um sie verarbeiten zu können,[689] womit im Ergebnis ein Werturteil steht.[690] Deshalb müssen notgedrungen auch Werturteile und Bewertungen Gegenstand der Zeugenaussage sein.[691] Bspw. liegt in der Aussage, es sei in der Tatnacht sehr kalt oder der Beschuldigte sei nicht be- sondern nur angetrunken gewesen, eine Bewertung der Situation.[692] Um aber den Inhalt des Zeugenbeweises (insb. im Hinblick auf die Beweisaufgaben des Sachverständigen) nicht zu sehr auszuweiten, darf der Zeuge nur über solche Werturteile oder Schlussfolgerungen aussagen, die ihm nach seiner allgemeinen Lebenserfahrung ohne weiteres möglich sind bzw. sich dem verständigen Betrachter ohne weiteres aufdrängen.[693] Das Bewerten von Tatsachen soll dem Sachverständigen vorbehalten sein.

Somit dient der Zeuge der Aufklärung eines nicht feststehenden Sachverhalts und er hilft dem Gericht einen Sachverhalt zu erkennen, zu rekonstruieren und zu beurteilen. Der Unterschied des Sachverständigen zum einfachen Zeugen besteht also v. a. im Innehaben einer besonderen Sachkunde.

Allerdings bestimmt § 85 StPO in diesem Zusammenhang, dass auch eine Bekundung von Tatsachen und Zuständen möglich ist, die nur mit besonderer Sachkunde wahrgenommen werden kann, und ordnet solche Aussagen dem

---

687 Löwe/Rosenberg/*Ignor/Bertheau*, Vor § 48 Rn. 4; KK/*Senge*, Vor § 48 Rn. 1; Meyer-Goßner/*Schmitt*, Vor § 48 Rn. 2 f.; *Eisenberg*, Beweisrecht der StPO, Rn. 1003; *Kindhäuser*, Strafprozessrecht, § 21 Rn. 22.

688 Löwe/Rosenberg/*Ignor/Bertheau*, Vor § 48 Rn. 4.

689 Vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 236, der darstellt, dass seit Kant jede Beobachtung als theorieimprägniert und daher zumindest zu einem großen Teil als konzeptabhängig betrachtet werden muss.

690 Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 346 f.; Löwe/Rosenberg/*Ignor/Bertheau*, Vor § 48 Rn. 6; *Ranft*, Strafprozessrecht, Rn. 479; vgl. auch *Hegler*, AcP 104 (1909), 151, 193 f.

691 Vgl. *Eisenberg*, Beweisrecht der StPO, Rn. 1003 mit weiteren Beispielen und Nachweisen; BGH bei *Holtz*, MDR 79, 807.

692 Beispiele aus *Stinshoff*, Operative Fallanalyse, S. 80.

693 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 236; RGSt 37, 371, 372; RGSt 57, 412, 413; SK-StPO/*Rogall*, Vor § 48 Rn. 18 ff.; Löwe/Rosenberg/*Ignor/Bertheau*, Vor § 48 Rn. 6; KK/*Senge*, Vor § 48 Rn. 1; *Eisenberg*, Beweisrecht der StPO, Rn. 1003; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 347.

Zeugenbeweis zu.[694] Ein Unterfall[695] des Zeugenbeweises ist somit der sog. sachverständige Zeuge. Der Begriff findet sich zwar nicht (mehr[696]) im Gesetz, ist aber allgemein anerkannt.[697] Die Norm beschreibt eine sachkundige Person, die nach den Vorschriften über den Zeugenbeweis zu vernehmen ist, soweit sie zum Beweis vergangener Tatsachen oder Zuständen aussagen soll, zu deren Wahrnehmung eine besondere Sachkunde erforderlich war, wie z. B. die Befragung eines Kfz-Meisters, in dessen Werkstatt ein Unfallverursacher am Tage vorher mit seinem Auto zur Inspektion war. Auf ihn finden die Vorschriften über den einfachen Zeugen wie bspw. die Vereidigung und Entschädigung unmittelbare Anwendung. Eine Ablehnung nach §§ 74 Abs. 1, 22 Nr. 1 – 4 StPO oder wegen Besorgnis der Befangenheit ist nicht möglich.[698] Er kann nicht vom Gutachtenverweigerungsrecht Gebrauch machen aus § 76 StPO und kann nicht zur schriftlichen Vorbereitung seiner Aussage verpflichtet werden.[699]

So kann der Sachverständige ebenso wie der Zeuge über unmittelbar wahrgenommene Tatsachen (i. S. d. dritten Kategorie) berichten, und auch der Zeuge zieht aus Tatsachen unbeabsichtigt Schlussfolgerungen[700], regelmäßig aber weniger als der Sachverständige. So erscheint eine Abgrenzung nach unmittelbarer Wahrnehmung und sachkundiger Beurteilung schwierig, wenn man an das Konstrukt des sachverständigen Zeugen denkt (siehe weiter unter III. 3.).[701]

b) Die Abgrenzung zu Ermittlungspersonen

Eine häufig anzutreffende Konstellation bei der Verwertung und Würdigung digitaler Spuren als Beweismittel ist diejenige, dass ein sachkundiger Polizeibeamter oder eine IT-Forensikerin der sachbearbeitenden Polizeidienststelle

694 SK-STPO/*Rogall*, Vor § 48 Rn. 1.

695 Weitere Kategorien sind bspw. der „unmittelbare" bzw. der „mittelbare" Zeuge oder der sog. Kronzeuge, vgl. SK-StPO/*Rogall*, Vor § 48 Rn. 24 ff.

696 Früher wurde der Begriff in § 5 S. 1 ZSEG verwendet. In das heute geltende JVEG wurde der Begriff nicht übernommen; vgl. auch Löwe/Rosenberg/*Krause*, § 85 Rn. 12.

697 Vgl. nur Meyer-Goßner/*Schmitt*, § 85 Rn. 1; KK/*Senge*, § 85 Rn. 1 ff.; BeckOK-StPO/*Ritzert*, § 85 Rn. 2; *Pfeiffer*, § 85 Rn. 1; *Hegler*, AcP 104 (1909), 151, 155 f.; kritisch zu dem Begriff siehe Löwe/Rosenberg/*Krause*, § 85 Rn. 12.

698 Meyer-Goßner/*Schmitt*, § 85 Rn. 1; Löwe/Rosenberg/*Krause*, § 85 Rn. 12; KK/*Senge*, § 85 Rn. 2; SK-StPO/*Rogall*, § 85 Rn. 35, 37.

699 Vgl. *Stinshoff*, Operative Fallanalyse, S. 81.

700 Siehe dazu auch unter B. II. 3. d) cc).

701 So auch schon *Walter*, Sachverständigenbeweis, S. 9. Dieser hat Zeugen von Sachverständigen, sachverständigen Zeugen und Beweismittlern abgegrenzt.

oder der zuständigen Staatsanwaltschaft (gerade die Schwerpunktstaatsanwaltschaften der Länder für den Bereich Cybercrime beschäftigen regelmäßig eigene Expertinnen der forensischen Informatik)[702] die im Verfahren verwerteten Daten erheben oder die Daten im Ermittlungsverfahren ohne einen spezifischen Gutachtenauftrag untersuchen. In diesen Fällen kommt anstelle der Beauftragung eines IT-Sachverständigen durch das Gericht auch die Vernehmung des sachkundigen Polizeibeamten oder der IT-Forensikerin der Staatsanwaltschaft als sachverständiger Zeuge i. S. d. § 85 StPO in Betracht.[703] Insbesondere in diesen Fällen geht es also um die oben bereits angedeutete Abgrenzung zwischen dem Sachverständigen- und Zeugenbeweis. Die forensische Tätigkeit muss zwischen einer Sachverständigen- und einer reinen Ermittlungstätigkeit abgegrenzt werden; das beschäftigte nicht zuletzt die Richterinnen in aktuellen Strafverfahren aus dem Deliktsbereich der §§ 184b ff. StGB und Wirtschaftsstrafverfahren (dazu sogleich in IV. 3. vertiefter).

Ermittlungspersonen gehören der Strafverfolgungsbehörde an (§§ 161 StPO; 152 Abs. 2 GVG, StAErmPV[704]). Gem. § 160 StPO *ermitteln* diese; ihre Tätigkeit ist also durchaus auch mit wertenden Initiativen zugunsten oder zulasten des Beschuldigten verbunden. Im Gegensatz dazu darf der Sachverständige (wie ein „Automat") lediglich das auswerten, was er vorgegeben bekommt – ohne eigene Initiativen ergreifen zu dürfen.[705] Dass eine Grenzzie-

---

[702] So auch der gesetzgeberische Wille in Bezug auf die Auswertung von digitalen Speichermedien nach § 110 StPO, vgl. MüKo-StPO/*Hauschild*, § 110 Rn. 11; KK/*Bruns* § 110, Rn. 4.

[703] *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 664; *Jahn/Brodowski*, in: FS Rengier, S. 409 (412).

[704] Verordnung über die Ermittlungspersonen der Staatsanwaltschaft, StAErmPV: § 1 Ermittlungspersonen der Staatsanwaltschaft – Bürgerservice (gesetze-bayern.de [20.5.2023]).

[705] Man könnte die Anforderungen eines IT-Sachverständigen im Strafverfahren vllt. auch „mathematischer" erklären und den IT-Sachverständigen als einen „Algorithmus" beschreiben. Dieser ist eine festgelegte Handlungsweise, um klar definierte mathematische Probleme zu lösen. Das mathematische Problem legt dabei fest, welche Informationen der Problemlöser kennt und welche Eigenschaften das Resultat haben muss, um als Lösung des Problems zu gelten. Das Problem definiert also die Beziehung zwischen Input (eingegebene Informationen) und Output (gewünschte Lösung). In der Informatik wird immer davon gesprochen, was „gegeben" ist (welche Information vorliegt) und was „gesucht" ist: Input = Anknüpfungstatsachen und Output = Antwort auf Beweisfrage unter Einhaltung der forensischen Schritte und Standards mithilfe von Werkzeugen und Sachkunde. Innerhalb dieser forensischen Schritte werden nicht immer die gleichen Werkzeuge und Erfahrungssätze (im Rahmen der besonderen Sachkunde) zur Beantwortung der Beweisfrage führen. Hierbei muss der IT-Sachverständige „herumprobieren", arbeitet dabei also (auch) wie eine Heuristik. Dieser Vergleich soll den Unterschied zur Ermittlungsperson verdeutlichen: Bei der Tätigkeit von Ermittlungspersonen sind Input und Output gerade noch nicht vorgegeben, diese müssen erst noch *ermittelt* werden.

hung hier im Einzelfall schwierig ist, geht mit den zugrundeliegenden unumgänglichen Wertungen und der anzuwendenden kriminalistischen Erfahrung einher, um die Beweisaufgabe beantworten zu können. Diese Kompetenzen des Sachverständigen, die ja auch für die Lösung der Beweisaufgabe notwendig sind, lassen sich natürlich im Denken nicht bewusst aus- und anschalten.

Ein großer Unterschied besteht darin, dass Ermittlungspersonen weisungsgebunden sind; also gerade nicht unabhängig und selbstständig, wie es die Sachverständigen sind.

Wichtig ist eine Unterscheidung – über die prozessuale Stellung der Beweisperson hinaus – v. a. wegen der Frage der Befangenheit, der Verjährungsunterbrechung, und der Kostentragung der Gutachtenerstellung. Auf die Abgrenzungskriterien wird sogleich bei B. III. 3. eingegangen.

c) Die Abgrenzung zum Augenscheinsgehilfen

Eine weitere Beweisperson, die vor Gericht über die Wahrnehmung von Tatsachen aussagt, ist der Augenscheinsgehilfe.

Eine Einordnung der IT-Sachverständigen als Augenscheinsgehilfen ist grundsätzlich denkbar, weswegen ein kurzer Überblick über die Prozessrolle und die Abgrenzung zum Sachverständigen erfolgen soll.[706]

Der sog. Augenscheinsgehilfe ist zwar gesetzlich nicht geregelt, die ganz h. M. erkennt dieses Rechtsinstitut jedoch an.[707] So weisen auch gesetzliche Vorschriften wie bspw. § 81d Abs. 1 oder § 87 Abs. 2 S. 1 StPO darauf hin, dass eine andere Möglichkeit als die richterliche Augenscheinnahme gem. § 86 StPO existieren muss.[708]

Augenscheinsgehilfe ist, wer vom Gericht mit der sinnlichen Wahrnehmung eines Beweisobjekts beauftragt wird und im Anschluss in der Hauptverhandlung über diese Wahrnehmung berichtet, ohne besondere Sachkunde zu haben.[709]

---

706 Vertiefend auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 285.

707 Vgl. nur BGHSt 27, 135, 136; Löwe/Rosenberg/*Krause*, § 86 Rn. 7; KK/*Senge*, § 86 Rn. 3; Meyer-Goßner/*Schmitt*, § 86 Rn. 4; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 400 ff.; *Rogall*, in: GS-Meyer S. 391 ff.

708 So auch in *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 18; *Stinshoff*, Operative Fallanalyse, S. 169.

709 KK/*Senge*, § 86 Rn. 3; *Eisenberg*, Beweisrecht der StPO, Rn. 2262; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 18; *Kindhäuser*, Strafprozessrecht, § 21 Rn. 109.

Die Beauftragung erfolgt aufgrund tatsächlicher Notwendigkeit (bspw. Besichtigung eines Dachfirsts oder eines Gegenstands unter Wasser)[710] oder weil sie gesetzlich vorgeschrieben ist, z. B. in § 81d StPO. Auch aus Zweckmäßigkeitserwägungen darf ein Richter einen Augenscheinsgehilfen bestimmen.[711] Auf eine besondere Sachkunde kommt es beim Augenscheinsgehilfen gerade nicht an (vgl. auch die Ausführungen bei B. II. 3. d) dd)).[712]

Die verfahrensrechtliche Stellung des Augenscheinsgehilfen ist umstritten.[713] Es bestehen unterschiedliche Auffassungen darüber, ob der Augenscheinsgehilfe während des Stadiums der Wahrnehmung Zeuge[714], Sachverständiger[715], ein Beweismittel eigener Art[716] oder ein freiwillig handelndes bzw. nach Amtshilfegrundsätzen herangezogenes bloßes Hilfsmittel des mittelbaren Augenscheins ist, wie Stinshoff[717] auch nach hiesiger Überzeugung plausibel dargelegt hat. Gegen die Anwendung der Vorschriften über den Zeugenbeweis spricht, dass der Augenscheinsgehilfe die Tatsachen aufgrund eines gerichtlichen Auftrags wahrnimmt.[718] Die Kriterien des Sachverständi-

---

710 Meyer-Goßner/*Schmitt*, § 86 Rn. 4; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 402.

711 RGSt 47, 100, 106; BGHSt 27, 135, 136; BGH NStZ 1994, 227; Löwe/Rosenberg/*Krause*, § 86 Rn. 5; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 402; kritisch dazu *Eisenberg*, Beweisrecht der StPO, Rn. 2264; a. A. *Wenskat*, Der richterliche Augenschein im deutschen Strafprozess, S. 228 ff., 231 ff.

712 Statt vieler vgl. nur *Eb. Schmidt*, II, Vor § 72 Rn. 18; *Girnth*, Der Augenscheinsmittler, S. 71 f.

713 Vertiefend dazu *Rogall*, in: GS-Meyer, S. 391 ff.; *Girnth*, Der Augenscheinsmittler, S. 10 ff.; *Harms*, Das Augenscheinsersatzobjekt im Strafprozess, S. 17 ff., 81 ff.; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 403; vgl. auch *Eb. Schmidt*, II, Vor § 72 Rn. 20.

714 AK/*Schreiber*, Vor § 73 Rn. 36, wenn der Augenscheinsgehilfe keine besondere Sachkunde hat; KMR/*Neubeck*, Vor § 72 Rn. 14; *Henkel*, Strafverfahrensrecht, S. 226; *Gössel*, Strafverfahrensrecht, S. 244; *Wenskat*, Der richterliche Augenschein im deutschen Strafprozess, S. 223 ff.; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 67.

715 *Eb Schmidt*, II, Vor § 72 Rn. 21, § 86 Rn. 8 f.; *Schlüchter*, Das Strafverfahren, Rn. 526 Fn. 424a; Löwe/Rosenberg/*Krause*, § 86 Rn. 7; Meyer-Goßner/*Schmitt*, § 86 Rn. 4; *Volk/Engländer*, § 21 Rn. 36; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 403; *Ranft*, Strafprozessrecht, Rn. 565; *Kindhäuser*, Strafprozessrecht, § 21 Rn. 109.

716 *Goldschmidt*, Der Prozess als Rechtslage, S. 434 ff. Fn. 2288; vgl. auch *Lent*, ZZP 60 (1936/1937), 9, 44.

717 *Stinshoff*, Operative Fallanalyse, S. 170; SK-StPO/*Rogall*, Vor § 72 Rn. 178 f. mit weiteren Ausführungen; zu den Problemen des Augenscheinsgehilfen im Strafprozess ferner ausführlich *ders.*, in: GS-Meyer, S. 391 ff.; *Eisenberg*, Beweisrecht der StPO, Rn. 2277 ff.; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 285 ff.; ausführlich auch *Girnth*, Der Augenscheinsmittler, S. 91 ff., 101 ff.

718 *Stinshoff*, Operative Fallanalyse, S. 170.

gen können jedenfalls auch keine Anwendung finden, weil eine besondere Sachkunde für die Wahrnehmung gerade nicht erforderlich ist.[719] Eine analoge Anwendung scheitert an der fehlenden Regelungslücke.[720] Eine Einordnung als Beweismittel sui generis scheidet aus, da der numerus clausus der Beweismittel dieses nicht vorsieht.[721]

Überwiegend Einigkeit besteht jedoch darüber, dass der Augenscheinsgehilfe während seiner Aussage über die Tatsachenwahrnehmung wie ein Zeuge zu behandeln ist.[722]

d) Unterschiedliche Rechte- und Pflichtenkataloge

So wurde eben angesprochen, dass die verschiedenen prozessualen Stellungen mit unterschiedlichen Rechte- und Pflichtekatalogen einhergehen. Deshalb ist eine Grenzziehung im Einzelfall notwendig. Im Folgenden sollen nun die wichtigsten Unterschiede der Zeugen- und Sachverständigenrolle dargestellt werden, die die StPO vorsieht.

Das Gesetz ordnet im Zusammenhang mit dem Sachverständigenbeweis an, dass dieser gem. § 74 Abs. 1 S. 1 StPO i. V. m. §§ 22 Nr. 1 – 4, 24 StPO abgelehnt werden kann.[723] Dagegen besteht gegen einen Zeugen kein Ablehnungsrecht.

Weiter kann ein Beweisantrag auf Vernehmung eines Sachverständigen zusätzlich zu den Kriterien des § 244 Abs. 3 StPO dann abgelehnt werden, wenn das Gericht selbst die nötige Sachkunde besitzt oder das Gegenteil der behaupteten Tatsache durch ein früheres Gutachten schon bewiesen ist, vgl. § 244 Abs. 4 StPO. Wird dagegen eine Beweisperson als Zeuge vernommen, muss bei fehlender Sachkunde des Gerichts einem Antrag auf Einholung eines Gutachtens stattgegeben werden, vgl. § 244 Abs. 4 StPO. Das Gericht darf die

---

719 Ausführlich vgl. *Girnth*, Der Augenscheinsmittler, S. 71 ff.

720 *Girnth*, Der Augenscheinsmittler, S. 77 f.

721 *Girnth*, Der Augenscheinsmittler, S. 70 f.; *Harms*, Das Augenscheinsersatzobjekt im Strafprozess, S. 98 f.

722 RGSt 47, 100 (106); BGHSt 27, 135 (136); OLG Frankfurt VRS 58, 368, 369 f.; Löwe/Rosenberg/*Krause*, § 86 Rn. 7; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 403; *Eisenberg*, Beweisrecht der StPO, Rn. 2281; KK/*Senge*, § 86 Rn. 3; KMR/*Neubeck*, Vor § 72 Rn. 14; AwK-*Krekeler/Wener*, Vor § 72 ff. Rn. 11; *Volk/Engländer*, § 21 Rn. 36; *Ranft*, Strafprozessrecht, Rn. 565; *Kindhäuser*, Strafprozessrecht, § 21 Rn. 109; *Hellmann*, Strafprozessrecht, Rn. 758; *Harms*, Das Augenscheinsersatzobjekt im Strafprozess, S. 177 ff., 184; *Girnth*, Der Augenscheinsmittler, S. 109, 120; so auch schon in den Motiven zur RStPO bei *Hahn*, Die gesamten Materialien zur Strafprozessordnung, S. 122 f.; a. A. *Eb. Schmidt*, II, Vor § 72 Rn. 21; *Schlüchter*, Das Strafverfahren, Rn. 526, Fn. 424a.

723 Vgl. in diesem Teil, B. V. 2. c).

Einholung des Gutachtens nicht mit der Begründung ablehnen, es habe aufgrund der Zeugenaussage selbst ausreichende Sachkunde. Es darf sich also die erforderliche besondere Sachkunde nicht aus der Zeugenaussage aneignen, sondern muss sie sich aus einem sachverständigen Gutachten erarbeiten. Spricht sich das Gericht die Sachkunde zu, ist es verpflichtet, im ablehnenden Beschluss oder dem Urteil genau darzulegen, woher er diese nimmt.[724]

Dem Sachverständigen steht darüber hinaus nach § 80 Abs. 2 StPO ein Akteneinsichtsrecht zu. Das Akteneinsichtsrecht dient der (Nach-)Ermittlung weiterer Anknüpfungstatsachen. Weil der Zeuge nur über die von ihm wahrgenommenen, für den Prozess relevanten Tatsachen aussagt,[725] besteht für ihn ein solches Recht nicht.

Auch sind die Ungehorsamsfolgen bei Zeugen und Sachverständigen unterschiedlich. Gegen einen Sachverständigen kann ein Ordnungsgeld als Zwangsmittel festgesetzt werden, vgl. § 77 Abs. 1 StPO. Gegen Zeugen dagegen können zusätzlich zum Ordnungsgeld auch Zwangsvorführung und Ordnungshaft angeordnet werden, vgl. § 51 StPO. Grund der Unterscheidung ist, dass ein gegen den Willen eines Sachverständigen erzwungenes Gutachten bzgl. der Sorgfalt und Objektivität sehr zweifelhaft ist.[726] Eine Erzwingung wird wohl auch in den seltensten Fällen notwendig sein, nachdem Sachverständige frei gewählt und i. d. R. ersetzt werden können. Dagegen kann bei einem Zeugen eine Aussageerzwingung durchaus notwendig sein, weil dieser gerade nicht austauschbar ist und die Gefahr besteht, die zu bekundende Tatsachenwahrnehmung könnte ansonsten für den Prozess verloren gehen.[727]

Ferner wird der Sachverständige, anders als der Zeuge, nicht nur entschädigt, sondern auch vergütet, vgl. §§ 1 Abs. 1 S. 1 Nr. 1 und 3, 5 ff., 8 ff. JVEG.[728]

Darüber hinaus werden die Kosten der Gutachtenerstattung und die Kosten der Ermittlungspersonen im Rahmen des Verfahrens unterschiedlich getragen: Handelt es sich um Ermittlungstätigkeit, verbleibt die Verantwortung für die

---

724 Vgl. SK-StPO/*Rogall*, Vor § 72 Rn. 21; *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 136.

725 Vgl. *Stinshoff*, Operative Fallanalyse, S. 172.

726 *Schmidhäuser*, ZZP 72 (1959), 365 (384); vgl. auch Motive bei *Hahn*, Die gesamten Materialien zur Strafprozessordnung, S. 122, der ausführt, dass einem erzwungenen Gutachten nur in den seltensten Fällen der volle Wert beigemessen werden könne.

727 Vgl. *Stinshoff*, Operative Fallanalyse, S. 173.

728 Rechtsgrundlage ist § 84 StPO i. V. m. dem JVEG. Voraussetzung ist, dass der Sachverständige vom Gericht oder der Staatsanwaltschaft herangezogen worden ist (§ 1 Abs. 1 Nr. 1 JVEG) oder von der Polizei im Auftrag oder mit vorheriger Billigung der Staatsanwaltschaft (§ 1 Abs. 3 JVEG). Die Vergütung richtet sich nach Honorargruppen (Honorargruppe 1 bis 10, M1 bis M3) und umfasst ein Honorar je Stunde zwischen 50 € bis 95 € (§ 9 Abs. 1 JVEG), zzgl. erstattungsfähiger Nebenkosten.

entstandenen Kosten bei der Staatsanwaltschaft („innerbetriebliche Kosten" der Strafverfolgungsbehörde) und die Staatskasse trägt die Kosten der „Berichterstattung". Handelt es sich dagegen um Sachverständigentätigkeit, ist der Auslagentatbestand regelmäßig § 3 Abs. 2 GKG i. V. m. Nr. 9015, Nr. 9005 KV GKG[729] i. V. m. JVEG. So werden die von der Staatskasse an einen Sachverständigen nach dem JVEG zu zahlende Vergütung für ein zur Vorbereitung der öffentlichen Klage eingeholtes Sachverständigengutachten (unter Beachtung des Verhältnismäßigkeitsgrundsatzes, Art. 2 Abs. 1 i. V. m. Art. 20 Abs. 3 GG[730]) dem Verurteilten i. S. d. §§ 465, 464a StPO auferlegt.[731]

Auch unterscheiden sich die Eidesformeln der zwei Beweispersonen: Eine Eidesleistung nach § 79 StPO („Sachverständigeneid") oder Vereidigung als Zeuge nach §§ 59 ff. StPO. Gem. § 79 Abs. 2 StPO hat der Sachverständige das Gutachten unparteiisch und nach bestem Wissen und Gewissen zu erstatten,[732] im Gegensatz zum Zeugen, der gem. § 64 Abs. 2 StPO „nur" den Eid darauf beziehen muss, dass er die reine Wahrheit gesagt und nichts verschwiegen hat. Der Sachverständige beeidet also nicht nur seine Wahrhaftigkeit bzgl. des Gutachtens, sondern auch seine Wahrhaftigkeit bzgl. seiner Bemühungen um Objektivität.[733] Andersherum geht der Zeugeneid weiter als der Sachverständigeneid: Der Sachverständigeneid beschränkt sich auf das Gutachten und die zugrundeliegenden Aussagekategorien. Der Zeugeneid dagegen deckt unbeschränkt jede Tatsachenbehauptung der Aussageperson ab.[734]

Der Sachverständige besitzt außerdem eine größere Manipulationsmöglichkeit – v. a. unter dem „Mantel der Objektivität" – als der Zeuge, weil er die richterliche Überzeugung auf einem Gebiet vorbereitet, auf dem sich die

729 Für die bei Strafverfolgungsbehörden angesiedelte Sachverständige sind die Kosten nach Nr. 9005 Abs. 2 S. 2 KV GKG vom Kostenschuldner als (fiktiver) Betrag in identischer Höhe zu erheben.

730 BVerfG, Beschl. der 2. Kammer des Zweiten Senats v. 28.12.2020 – 2 BvR 211/19, Rn. 34 f.

731 Nachdem es sich bei den Gutachterkosten teilw. um sehr hohe Beträge handelt, die oft vom Verurteilten zu tragen sind (siehe dazu Rechtsprechung in diesem Teil, B. IV.), muss letztlich sogar über eine Reform der PKH nachgedacht werden. So lässt sich feststellen, dass das JVEG nicht auf IT-Sachverständige ausgelegt ist: Bspw. können elektronische Dateien zu je 1,50 € abgerechnet werden, jedoch nur bis zu insgesamt 5 €, § 7 Abs. 3 JVEG. Jedes Verfahren in Bezug auf §§ 184b ff. StGB hat erfahrungsgemäß weitaus mehr Daten. Des Weiteren werden die Daten meistens auf Festplatten angeliefert, deren Kosten sich kaum durch 5 € decken lassen.

732 Waren die Darstellungen unparteiisch und leistet der Sachverständige einen Eid i. S. d. § 79 Abs. 2 StPO, kann es sich um ein falsches Schwören i. S. d. § 154 StGB hinsichtlich der Unparteilichkeit der Aussage handeln.

733 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 265, 282.

734 Zur Erörterung des Überzeugungsbegriffs siehe *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 153 ff.

Richter selbst nicht vertrauen dürfen. Der Sachverständige ist hier durch seine Information nicht nur in der Lage, dem Gericht eine Basis für eine selbstständige Entscheidung zu verschaffen, sondern durch geschicktes Arrangement der vertretenen Ansichten und Argumente eine bestimmte Lösung nahezulegen. Das Gutachten kann in Zweifelsfragen eine zutreffende und vollständige Schilderung enthalten und dennoch infolge seiner tendenziellen Darstellung das Gericht zu einer bestimmten Schlussfolgerung hinleiten.[735] Dabei ist es wohl naturgegeben, dass man (als Wissenschaftlerin) bestimmte Auffassungen bevorzugt, was dann unbewusst in der Darstellung zum Ausdruck kommt.

Weiter sind die Vorschriften der § 243 Abs. 2 S. 1 StPO und § 58 Abs. 1 S. 1 StPO, wonach der Zeuge nicht der Hauptverhandlung beiwohnen darf, nicht entsprechend auf den Sachverständigen anwendbar.[736] So darf der Sachverständige gem. § 80 StPO grundsätzlich der gesamten Hauptverhandlung sowie der Vernehmung des Beschuldigten und Zeugen beiwohnen und es kann ihm gestattet werden, unmittelbare Fragen an sie zu stellen und die Akten einzusehen.[737]

Materiellrechtlich ergibt sich die Besonderheit, dass die Beauftragung eines Sachverständigen die Verfolgungsverjährung gem. § 78c Abs. 1 Nr. 3 StGB unterbrechen kann. Die Vernehmung des Zeugen hat dagegen keine verjährungsunterbrechende Wirkung.[738]

Neben den prozessrechtlichen unterschiedlichen Rechte- und Pflichtenkatalogen, die an die jeweiligen Verfahrenspositionen geknüpft sind, ergeben sich v. a. bei der Abgrenzung zwischen Ermittlungspersonen als (sachverständige) Zeugen und IT-Sachverständigen Bedenken bzgl. der Auslagerung genuiner Ermittlungstätigkeit an externe Dritte – anders gesprochen, wenn die Strafverfolgung, die teils mit intensiven Grundrechtseingriffen verbunden ist, privatisiert wird. Dieses Problem tritt ist derzeit im Zusammenhang mit der Beauftragung von IT-Sachverständigen in der Praxis zu beobachten. Es wird kritisiert, dass wohl nicht wenige „Ermittlungsaufgaben“ gleichsam auf IT-Sachverständige „ausgelagert“ werden.[739] Natürlich muss dies in einem ersten Schritt theoretisch eine Trennung der beiden Rollen „Sachverständige“ und

735 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 283.

736 RGSt 22, 434; *Eisenberg*, Beweisrecht der StPO, Rn. 1590.

737 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 338.

738 Wenn während des Verfahrens ein Sachverständiger beauftragt wird, dann führt das zu einer Unterbrechung der Verjährung, das heißt die Tat kann länger verfolgt werden; man spricht hier von einem verjährungsunterbrechenden Gutachtenauftrag nach § 78c Abs. 1 Nr. 3 StGB; wenn es sich dagegen nicht um Sachverständigenqualität handelt, sondern um reine Ermittlungstätigkeit, dann führt das eben nicht zu einer Verjährungsunterbrechung, vgl. auch *Stinshoff*, Operative Fallanalyse, S. 173.

739 Siehe dazu sogleich unter IV.

„Ermittlungsgehilfe“ nach sich ziehen. Für die Praxis dürfte aber durchaus zu vermuten sein, dass eine ursprünglich als IT-Sachverständige bestellte Person im Verfahren dann ganz überwiegend auch innerhalb dieser Rolle (und damit immerhin als „Gehilfe des Gerichts“ und nicht als Gehilfe der Polizei) auftritt. Deshalb ist eine Differenzierung der Rollen schon vor einer möglichen Beauftragung, bspw. i. R.d Vorüberlegungen zur Formulierung der Beweisfrage i. R.d § 78 StPO, von außerordentlicher Bedeutung. Wenn hier bereits auffällt, dass eigentlich erst noch „ermittelt“ werden muss oder aber gar keine besondere Sachkunde gebraucht wird, dann darf schon gar keine Sachverständigenbestellung erfolgen. Auch wichtig erscheint in einer solchen Situation die Auswirkung auf die Verringerung des Beweiswertes der so gewonnenen Ermittlungsergebnisse und die Folge einer verfassungswidrigen „faktischen“ Beleihung (ggf. sogar ein Beweisverwertungsverbot). In Bezug auf den Beweiswert wird zu bedenken gegeben, dass Sachverständige im Vergleich zu staatlichen Strafverfolgungsbehörden, die zur Wahrheitserforschung verpflichtet und verschiedenen Kontrollmechanismen unterworfen sind, ein geringeres Interesse an der Aufklärung des wahren Sachverhalts haben. Sie verfügen i. d. R. über keine kriminalistische oder juristische Ausbildung, die sie für entsprechende Entscheidungen qualifizieren, sondern eben über in anderen Gebieten liegende Expertise.[740]

3. Abgrenzungskriterien

Im Laufe der Zeit wurden verschiedene Versuche unternommen, ein allgemeingültiges Abgrenzungskriterium zu finden, die aber alle nicht überzeugen können. Auch an der heutigen h. M. lässt sich Kritik ausüben[741].

Einig sind sich zunächst alle dahingehend, dass die Bezeichnung als „Zeuge“ oder „Sachverständiger“ in der Ladung nicht entscheidend dafür sein soll, in welcher Funktion die Aussageperson vernommen werden soll. Die prozessuale Stellung der Aussageperson ergibt sich zunächst nicht von selbst. Es bedarf einer Einbeziehung in das Strafverfahren durch ein Strafverfolgungsorgan (formelles Element).[742] So sind Prozesshandlungen (wie die Ladung oder der Beweisbeschluss) auslegungsbedürftig.[743]

---

740 *Momsen/Rackow/Schwarze*, NStZ 2018, 625 f.; *Beukelmann*, NJW-Spezial 2008, 280.

741 Wie *Stinshoff*, Operative Fallanalyse, S. 188 ff., 191 ff.

742 SK-StPO/*Rogall*, Vor § 48 Rn. 11; *Stinshoff*, Operative Fallanalyse, S. 62.

743 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 279; BGH 2 StR 213/55 v. 15.12.1955; BGH NStZ 1985, 182; LG Osnabrück JurBüro 1998, 463; Alsberg/Nüse/Meyer, Der Beweisantrag im Strafprozess, S. 213; *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, Rn. 13; KK/*Senge*, Vor § 72 Rn. 7; Löwe/Rosenberg/*Krause*, § 85 Rn. 1; KK/*Senge*, Vor § 72 Rn. 7; *Eisenberg*, Beweisrecht der StPO,

So wird zur Abgrenzung bspw. am Zeitpunkt der Wahrnehmung[744] oder an dem historisch entwickelten Begriff des Sachverständigen als „Gehilfe des Richters“[745] angeknüpft. Wieder andere ziehen die Austauschbarkeit des Sachverständigen[746] oder den Inhalt der Bekundung[747] für einen Abgrenzungsversuch heran. Daneben gibt es Auffassungen, die sich am Zweck der Beauftragung[748] orientieren oder die Natur der Beweismittel[749] betrachten.

Rn. 1513; Alsber/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 377; *Ulrich*, Der gerichtliche Sachverständige, Rn. 19, der aber davon spricht, dass die Bezeichnung in der Ladung nicht entscheidend für die „endgültige“ Einordnung sei; mit Einschränkungen SK-StPO/*Rogall*, § 85 Rn. 11; *Eb. Schmidt*, II, Vor § 72 Rn. 15; *Mezger*, AcP 117 (118) Beilagheft, 1, 6; zur Abgrenzungsproblematik siehe auch vertiefend *Stinshoff*, Operative Fallanalyse, S. 61 ff.; KMR/*Neubeck*, Vor § 48 Rn. 1.

744 Wonach der Zeuge über vergangene und der Sachverständige über gegenwärtige Tatsachen aussagt. Vgl. dazu auch *Stinshoff*, Operative Fallanalyse, S. 174 f.: Aber vielmehr unterliegt es dem Zufall, ob ein Zustand beendet ist oder noch andauert, vgl. auch *Mezger*, AcP 117 (1918), Beilageheft, 1, 18; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 30. Eine juristische Einordnung der Aussage soll sich durch eine solche Zufälligkeit nicht ändern, vgl. auch *Hegler*, AcP 104 (1909), 151, 233 f.

745 Dagegen soll der Zeuge bloßes Beweismittel sein, vgl. *Stinshoff*, Operative Fallanalyse, S. 176 f. Aber schon die Tatsache, dass auch der Zeuge dem Richter hilft, wie bei der Rekonstruktion des Sachverhalts, spricht gegen dieses Abgrenzungskriterium, vgl. auch Meyer-Goßner/*Schmitt*, Vor § 72 Rn. 8; Löwe/Rosenberg/*Krause*, § 85 Rn. 5; *Gössel*, DRiZ 1980, 365; Peters, S. 342.

746 Wonach der Sachverständige immer auswechselbar sei, der Zeuge dagegen nicht, vgl. auch *Stinshoff*, Operative Fallanalyse, S. 177 f. Jedoch kann dieses Kriterium bzgl. der Abgrenzung zwischen Sachverständigen und Augenscheinsgehilfen nicht weiterhelfen, weil auch dieser austauschbar ist.

747 Vgl. auch *Stinshoff*, Operative Fallanalyse, S. 179 f. Wobei hier zwei Ansätze erkennbar sind: Einerseits die Anforderungen an die Denkleistung, wonach diese beim Sachverständigen qualitativ höherwertiger sein soll. Es gibt jedoch auch Schlussfolgerungen, die keine schwierige Denkleistung erfordern und Tatsachen, deren richtige Wahrnehmung und Wiedergabe hohe intellektuelle Anforderungen stellen, vgl. *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 36 f.; vgl. *Mayer*, in: FS-Mezger, S. 455, S. 464. Andererseits wird nach der Bildung von Ober- und Untersätzen unterschieden. Hier wird entgegnet, dass auch Zeugenaussagen Schlussfolgerungen und Werturteile enthalten können.

748 Hier sei der Grund entscheidend, warum die Beweisperson im Prozess aussagen soll (die „Hegler’sche Formel“), vgl. *Hegler*, AcP 104 (1909), 151, 247, 249; *Stinshoff*, Operative Fallanalyse, S. 182 f. m. w. N. Dabei soll der Zeuge aufgrund seiner historischen, individuellen Beziehung zum Sachverhalt (mit oder ohne besondere Sachkunde) über für den Prozess erhebliche wahrgenommene Tatsachen berichten und der Sachverständige wegen seiner generell-rationalen Beziehung seines besonderen Sachverstandes im Rahmen der drei Aussagekategorien aussagen. Hier fehlt es jedoch an einem unmittelbaren Vergleichsmoment, da das Motiv der Bestellung nicht immer eindeutig bestimmbar nach außen tritt.

749 Dabei bestehe die charakteristische Eigenschaft des Zeugen darin, dass er durch die Mitteilung seiner Wahrnehmungen das Beweismaterial vermehrt, wogegen der

Darüber hinaus gibt es die Meinung, dass für die Abgrenzung allein der Auftrag[750] entscheidend ist.[751] Nach Toepel[752] soll für die Abgrenzung zwischen Zeugen- und Sachverständigenposition auch die Zuständigkeit für die Auftragserteilung[753] herangezogen werden können.

Die wohl h. M.[754] zieht zur Abgrenzung der Beweispersonen zwei Kriterien heran: Die besondere Sachkunde und den Auftrag. Danach soll Sachverständiger sein, wer über Tatsachen aussagt, die er unter Zuhilfenahme besonderer Sachkunde und aufgrund eines Auftrages wahrgenommen hat. An dieser „Kriterienkombination"[755] kann jedoch kritisiert werden, dass für die prozessuale Stellung der Beweisperson nicht ausschließlich der Wille des Gerichts ausschlaggebend sein darf.[756]

Überzeugender ist es, auch unter dem Gesichtspunkt der Methodenlehre, auf den *Zweck* abzustellen, zu dem die Aussageperson herangezogen wurde. Dieser ergibt sich aus dem Beweisthema, zu dem die Aussageperson gehört werden soll. Bei Ermittlung des Zwecks ist zwar auch das Interesse des An-

---

Sachverständige bereits vorhandenes Beweismaterial verwertbar mache, vgl. auch *Stinshoff*, Operative Fallanalyse, S. 183 f. m. w. N. Jedoch kann dieses Kriterium hinsichtlich der Bekundung von Befundtatsachen nicht weiterhelfen.

750 Ausschlaggebend ist in diesem Zusammenhang, ob die Beweisperson eine Wahrnehmung gemacht hat oder gutachterlich tätig geworden ist, weil sie von dem zuständigen Strafverfolgungsorgan dazu beauftragt wurde. Besteht ein solcher Auftrag, sei die Person Sachverständiger, so insb. *Stinshoff*, Operative Fallanalyse, S. 184 f., S. 191 f.; KK/*Senge*, § 85 Rn. 1; *Ulrich*, Der gerichtliche Sachverständige, Rn. 20; *Eb. Schmidt*, II, Vor § 72 Rn. 15; *Ditzen*, ZStW 10 (1890), 111 (163); *Glaser*, Handbuch, S. 687. Allerdings ist der Auftrag zwingende Folge, nicht die Voraussetzung für die Ernennung einer Beweisperson zum Sachverständigen im Prozess, vgl. auch *Pawlak*, Ablehnung des Sachverständigen, S. 42.

751 Für eine vertiefende Auseinandersetzung vgl. *Stinshoff*, Operative Fallanalyse, S. 171 ff.; auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 250 ff.

752 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 265 f.

753 Der Sachverständige wird jeweils von derjenigen Autoritätsposition herangezogen, deren mangelnder Sachkunde er abhelfen soll. Relativ zu dieser Autoritätsposition soll er Sachverständiger sein.

754 Löwe/Rosenberg/*Krause*, § 85 Rn. 11; Meyer-Goßner/*Schmitt*, § 85 Rn. 2 f.; AwK-*Krekeler/Werner*, § 85 Rn. 4; KMR/*Neubeck*, Vor § 48 Rn. 40, § 85 Rn. 2; *Pfeiffer*, § 85 Rn. 1; *Roxin/Schünemann*, § 27 Rn. 3; *Gössel*, DRiZ 1980, 363, 365; *Krekeler*, wistra 1989, 52; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 275; KK/*Senge*, § 85 Rn. 1; *Ulrich*, Der gerichtliche Sachverständige, Rn. 20; *Eb. Schmidt*, II, Vor § 72 Rn. 15, Rn. 17; *Ditzen*, ZStW 10 (1890), 111 (163); zu dem ganzen auch *Stinshoff*, Operative Fallanalyse, S. 188 f.

755 Vgl. *Stinshoff*, Operative Fallanalyse, S. 189.

756 Vertiefend dazu *Stinshoff*, Operative Fallanalyse, S. 61 ff., 119 ff., 187, 191: So ist auch im Zusammenhang mit der Beschuldigteneigenschaft eines Verdächtigen mittlerweile allgemein anerkannt, dass es zunächst auf den subjektiven Akt der Strafverfolgungsbehörde ankommt, der sich objektiv in einer Maßnahme manifestiert.

tragstellers zu berücksichtigen, wenn dieser Wille jedoch nicht erkennbar ist oder aber (irrtümlich) falsch geäußert wurde, soll auf die Kategorie der Beweisfrage abgestellt werden.[757] Dieses objektive Regulativ (Zweck der Befragung) braucht es schon deshalb, weil der Sachverständige durch sein überlegenes Wissen großen Einfluss auf das Verfahren hat und die Rechte der Verfahrensbeteiligten immer gewahrt bleiben müssen (z. B. Ablehnungsanträge). Das Abstellen auf den Zweck vermag auch das Problem zu lösen, dass Strafverfolgungsbehörden eine besondere Sachkunde zum Zeitpunkt der Auftragserteilung lediglich vermuten können.[758] Das Bestehen oder Nichtbestehen muss jedoch zu einer Veränderung der Verfahrensposition führen können. Wenn sich später also ein Mangel an der ursprünglich erwarteten Sachkunde der als Sachverständige bestellten Personen herausstellt, muss die Verfahrensstellung hin zu einer Zeugenposition geändert werden können. Wird z. B. der zunächst als sachverständige Zeuge Geladene auch über Erfahrungssätze und Schlussfolgerungen vernommen, so ist in der Vernehmung darüber eine konkludente Bestellung als Sachverständiger (mit entsprechender Entschädigung als Sachverständiger[759]) zu sehen.[760] Diese Argumentation wird auch durch § 85 StPO gestützt. Wohl mag die Verortung des § 85 StPO im Abschnitt über den Sachverständigen zunächst die Abgrenzungsschwierigkeiten in der Praxis

---

757 So auch in Vgl. OVG Lüneburg NJW 2012, 1307, das zwar auf den Inhalt der Vernehmung abstellt, aber „insbesondere die gerichtliche Nachfrage" betont; SK-StPO/*Rogall*, Vor § 72 Rn. 32.

758 Vgl. auch *Hegler*, AcP 104 (1909), 151, 153 f., 249; *Mezger*, AcP 117 (1918), Beilageheft, 1, 3, 5; SK-StPO/*Rogall*, Vor § 72 Rn. 7, § 85 Rn. 11 ff.; *Stinshoff*, Operative Fallanalyse, S. 127 ff.

759 Bsp. OLG Bamberg JurBüro 1980, 1221; OLG Hamburg JurBüro1975, 82; OLG München JurBüro 1973, 1206; *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, Rn. 13.

760 Exkurs: Wahrnehmungen aus einem anderen Gerichtsverfahren wegen eines anderen richterlichen Auftrags können nur Gegenstand eines Zeugenbeweises sein. Es handelt sich um vergangene Tatsachen i. S. d. § 85 StPO. Die gegenteilige Ansicht wird damit begründet, die Wahrnehmungen seien Befundtatsachen, die der Sachverständige aufgrund seiner besonders geschulten Beobachtungsgabe festgestellt habe. Hierbei ist jedoch einerseits zu beachten, dass auch sachverständige Zeugen Tatsachen aufgrund einer besonderen Sachkunde bzw. Beobachtungsgabe feststellen. Die Rspr. erkenne auch an, dass der Sachverständige fremde gutachterliche Äußerungen sowie den fachlichen Inhalt von Krankengeschichten mitverwerten dürfe, ohne dass dazu eine gesonderte Beweiserhebung erforderlich wäre. Allerdings komme es dabei darauf an, dass der Sachverständige die von anderen Wissenschaftlern gefundenen Untersuchungsergebnisse selbst prüft und verarbeitet, „also nicht bloß wie ein Zeuge vom Hörensagen ohne eigene Stellungnahme über sie berichtet hat." Die fremden Beobachtungen dürfen nur dann als Indizien dienen, auf die der Sachverständige zurückgreifen darf, wenn sie ordnungsgemäß durch Vernehmung des früheren Sachverständigen als sachverständigen Zeugen in die Hauptverhandlung eingeführt worden sind; vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 273 m. w. N.

zwischen Sachverständigen und Zeugen weiter erschweren.[761] Jedoch liefert genau diese systematische Stellung der Norm ein klares Abgrenzungskriterium: So bestimmt die Norm, dass sich die materielle Stellung der Beweisperson im Prozess nach der Beweisaufgabe richtet. Aus der Vorschrift folgt nämlich einerseits, dass eine Person nicht deshalb automatisch zum Sachverständigen wird, weil sie Wahrnehmungen aufgrund besonderer Sachkunde gemacht hat. Andererseits ergibt sich im Umkehrschluss, dass Schlussfolgerungen, Werturteile und Begutachtungen auch dann nicht mehr zur Aufgabe des Zeugenbeweises gehören, wenn die Person sachkundig ist. Diese Tätigkeiten unterfallen der Beweisaufgabe des Sachverständigen.

Eine Sachverständigenposition ergibt sich eindeutig dann, wenn es sich um Beweisthemen der ersten oder zweiten Aussagekategorien handelt; wenn eine Aussageperson zum Bestehen von Erfahrungssätzen Stellung nehmen oder mit Hilfe solcher Erfahrungssätze Schlussfolgerungen ziehen soll. Der Kritik dieser Auffassung – auch Zeugen nehmen Erfahrungssätze in Anspruch und ziehen Schlussfolgerungen aus Tatsachen[762] – kann entgegnet werden, dass die Erfahrungssätze, derer sich der Zeuge bedient, solche sind, die jeder bei Wahrnehmung benutzt.[763] Dabei ist keine besondere Sachkunde erforderlich, um das Bestehen dieser Erfahrungssätze zu kennen oder mit ihnen Schlussfolgerungen ziehen zu können. Sie werden als bekannt vorausgesetzt und sind deshalb nicht Beweisthema i. S.e. Sachverständigenbeweises.[764]

Hinsichtlich der dritten Aussagekategorie überschneiden sich die Themen von Sachverständigen- und Zeugenbeweis.[765] So können auch singuläre Prämissen eines Syllogismus, die sich aus Beobachtungen ergeben, Gegenstand des Zeugenbeweises sein. Dem „sachverständigen" Zeugen und dem Sachverständigen ist damit gemein, dass sie eine besondere Sachkunde haben, unter deren Zuhilfenahme sie Tatsachen wahrnehmen und darüber aussagen können.

---

761 Vgl. vertiefend dazu *Stinshoff*, Operative Fallanalyse, S. 81 f.

762 Vgl. bspw. *Birkmeyer*, Deutsches Strafprozessrecht, S. 444; ebenso Alsberg/Nüse/Meyer, Der Beweisantrag im Strafprozess, S. 21 ff.; *Henkel*, Strafverfahrensrecht, S. 247; *Hetzer*, Wahrheitsfindung, S. 98; *Mayer*, in: FS Mezger, S. 455 (464); *Sauer*, Allgemeine Prozesslehre, S. 165; *Schmidhäuser*, ZZP 72 (1959), 365 (374); *Wüst*, Richter und psychologischer Sachverständiger, S. 11 f.

763 Insoweit ergibt sich im kontinentaleuropäischen und angloamerikanischen Recht dieselbe Problematik. Besonders deutlich wird das in Section 3 Paragraph 2 des englischen Civil Evidence Act 1972 (Admissibility of expert opinion and certain expressions of non-expert opinion): „It is hereby declared that where a person is called as a witness in any civil proceedings, a statement of opinion by him on any relevant matter on which he is not qualified to give expert evidence, if made as a way of conveying relevant facts personally perceived by him, is admissible as evidence of what he perceived."

764 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 266.

765 Hierauf weist auch *Mezger*, AcP 117 (1918), Beilageheft, S. 1 (21 f.) hin.

Abbildung 5: „Abgrenzung zwischen (sachverständigen) Zeugen und den Sachverständigen"

Dem „einfachen" Zeugen und dem Augenscheinsgehilfen fehlt dagegen diese Sachkunde. Um die übrig gebliebene Abgrenzungslücke zu schließen, wird als weiteres Kriterium der Auftrag herangezogen, um dadurch den „einfachen" Zeugen vom Augenscheinsgehilfen und den „sachverständigen" Zeugen vom Sachverständigen unterscheiden zu können (siehe Abb. 5).[766]

Zeuge ist also, wer unter Zuhilfenahme besonderer Sachkunde, aber ohne Auftrag, oder ausschließlich mit Allgemeinwissen, unabhängig von der Auftragserteilung wahrgenommen hat. Darüber hinaus kann der Zeuge unter Anwendung von Allgemeinwissen beurteilen und schlussfolgern. Augenscheinsgehilfe ist, wer mit Allgemeinwissen auftragsabhängig wahrnimmt. V. a. in Bezug auf die dritte Aussagekategorie muss es darauf ankommen, ob ein

766 SK-StPO/*Rogall*, § 85 Rn. 3; vgl. *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 52; *Stinshoff*, operative Fallanalyse, S. 82; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 279.

Auftrag vorliegt (dann Sachverständiger) oder nicht (dann sachverständiger Zeuge).[767] Ob der Auftrag richtig ergangen ist, ist eine andere Frage.[768]

Für eine Abgrenzung helfen auch die anderen Merkmale, die von den verschiedenen Vertretern herangezogen wurden, wie bspw. die „Austauschbarkeit" oder die „Natur des Beweismittels" in Summe.

4. Fazit

Kriterium für die Entstehung einer Sachverständigenposition ist also der ausdrücklich oder konkludent erteilte Auftrag zu einer Frage i. S. einer der drei Aussagekategorien Stellung zu nehmen, um den Mangel der erforderlichen Sachkunde auf Seiten des Gerichts auszugleichen.[769]

Die Verweisungen auf die Regelungen bzgl. Gerichtspersonen (§ 74 StPO) sollen lediglich verdeutlichen, dass die Objektivitätsproblematik ein ähnliches Gewicht wie bei der Position des Richters besitzt, insofern, als der Sachverständige dem Richter Überzeugungsmöglichkeiten vorlegt, die übernommen werden können.

Die Verweisungen auf die Vorschriften für die Zeugen (§§ 72, 76 StPO) wiederum zeigen, dass die Problematik des Zeugnisverweigerungsrechts ähnlich wie bei der Position des Zeugen auftritt, wenn sich Konflikte der Prozessrolle mit anderen sozialen Rollen ergeben.

Nichtsdestotrotz ist die Sachverständigenposition ein durch ihre Entstehungsbedingungen deutlich zu unterscheidendes Beweismittel.[770]

Wie schwierig diese Abgrenzung im Einzelfall sein kann, zeigt die aktuelle rechtswissenschaftliche Diskussion in Literatur und Rechtsprechung, die im nächsten Abschnitt dargestellt werden soll.

IV. Der Versuch einer Kategorisierung und Bewertung der IT-Sachverständigentätigkeit aus juristischer Perspektive

Wie aktuell die Abgrenzungsfrage zwischen dem IT-Sachverständigen und einem Zeugen bzw. einer Ermittlungsperson ist, zeigt die unterschiedliche Auffassung der Verfahrensbeteiligten und der Rechtsprechung deutscher Strafgerichte im Bereich der Wirtschaftsstrafverfahren und Strafverfahren in

767 *Stinshoff*, Operative Fallanalyse, S. 191 f.
768 Vgl. *Stinshoff*, Operative Fallanalyse, S. 169 ff.
769 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 280.
770 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 281.

Bezug auf §§ 184b ff. StGB (Verbreitung, Erwerb und Besitz kinder- und jugendpornografischer Inhalte).

1. Aus Sicht der Strafverteidiger

So diskutierten zuletzt die Strafverteidiger Wackernagel und Graßie[771], die Anforderungen an die Qualität der IT-Sachverständigentätigkeit. Dabei formulieren sie typische Beweisfragen aus der Praxis und bewerten diese im Hinblick auf die Erforderlichkeit einer besonderen Sachkunde auf dem Gebiet der forensischen Informatik. Im Ergebnis beanstanden die Strafverteidiger die gängige Praxis, dass die Staatsanwaltschaften in Ermittlungsverfahren zur Auswertung von Datenträgern auf die Dienste privater IT-Forensik-Büros zurückgreifen, indem sie diese förmlich als Sachverständige bestellen (§ 161a Abs. 1 S. 2 StPO i. V. m. § 73 Abs. 1 StPO) und in der Regel damit beauftragen, digitale Daten aufzubereiten, strukturiert zusammenzustellen und nach bestimmten Suchkriterien zu untersuchen, obwohl diese Tätigkeiten eigentlich Ermittlungsarbeiten darstellen, und gerade keine besondere Sachkunde erfordern („Outsourcing genuiner Ermittlungstätigkeit").[772]

Die Bewertung im Hinblick auf die Erforderlichkeit einer besonderen Sachkunde i. R. d. Tätigkeit der IT-Sachverständigen erfolgt durch die Autoren dabei wie folgt: Im Grunde soll es zwei in Auftrag gegebene Sachverständigenkategorien geben – die *Vorarbeiten* und die *Hauptaufgaben* eines IT-Sachverständigen.

Die Aufträge lauten dabei wie folgt: 1) Die „Bestandsaufnahme von Kommunikationsdaten", 2) die „Datenaufbereitung", 3) ein „‚strukturiertes' Zusammenstellen von Daten", 4) das „Überprüfen der Daten auf Vollständigkeit" und 5) ein „Durchsuchen von Daten".

Diese Daten „aufzubereiten" i. S. einer „Bestandsaufnahme" bzgl. der Qualifizierung der Daten (z. B. welche Kommunikationsdaten vorhanden sind, E-Mails, Chat-Protokolle, Messenger-Diensten oder Plattformen), festzustellen, welche sonstigen Daten (Home- oder Group-Shares) vorliegen und diese nach Personen und Zeiträumen „strukturiert zusammenzustellen" bzw. zu sortieren und bestimmten Personen zuzuordnen (bereits bekannten oder dem Beschuldigten) und diese letztlich nach bestimmten Kriterien, die von der Staatsanwaltschaft in Rücksprache mit dem IT-Sachverständigen näher spezifiziert werden, zu durchsuchen (Hauptaufgabe), stellen aus Sicht der Autoren triviale Aufgaben dar, die die Kompetenzen eines durchschnittlichen Ermittlungsbeamten nicht übersteigen. Allerdings fasst diese Einschätzung viel zu kurz und

771 *Wackernagel/Graßie*, NStZ 2021, S. 12.

772 Vgl. dazu auch *Schwartz/Faber*, ZWH 2023, S. 123 ff.

ist aus Sicht der Verfasserin falsch. Wie oben schon dargelegt und unten weiter ausgeführt, können bereits diese Vorarbeiten durchaus fehleranfällig sein (insbesondere für Laien) und haben eine durchaus nicht triviale Rolle für die weitere Ermittlungstätigkeit und den Ausgang des Verfahrens.

Die Autoren begründen ihre Einschätzungen zunächst damit, dass man bei der Qualifizierung der (Komunikations-)Daten kein spezifisches Fachwissen benötigt. Für die Zuordnung von Daten zu bestimmten Personen muss lediglich ermittelt werden, welche Personen auf bestimmte Ordner Zugriff hatten. Eine „Datenaufbereitung" ist nur dann eine sachverständige Verrichtung, wenn bestimmte Daten in nicht geläufigen Dateiformaten zunächst lesbar gemacht werden müssen, wie im Falle spezieller Gerätesoftware (z. B. Auslesen bestimmter Mobiltelefone), bestimmter Datenbanklösungen (z. B. Lotus Notes) oder Spezialsoftware (z. B. SAP-Steuerungssoftware), bei denen Vorarbeiten auf Grundlage spezifischer Informatikkenntnisse erforderlich sind, um eine Lesbarkeit herzustellen. Wenn es sich dagegen nur darum handelt, verstreute Daten (aus verschiedenen „Lieferungen" oder von verschiedenen Datenträgern oder aus verschiedenen E-Mail-Postfächern) zusammenzuführen, stellt das reine Ermittlungstätigkeit dar. Auch hinsichtlich der Durchsuchung der aufbereiteten Daten bezweifeln die Autoren, dass es sich um eine Sachverständigenaufgabe handelt. Sie begründen das damit, dass die aufbereiteten Daten mit üblichen – teils frei verfügbaren – Forensikprogrammen (wie Relativity, NUIX, ZyLAB) durchsucht werden könnten. Die Anwendung dieser Programme erfordert keine besondere Sach- oder Fachkunde im Bereich der EDV. Diese Ansicht wird auch von der Rechtsprechung des OLG Schleswig gestützt (dazu sogleich unter IV. 3.).[773]

Diese Bewertung als reine Ermittlungstätigkeit *kann* zutreffend sein. So berichten auch Praktiker, dass die oben genannten Tätigkeiten regelmäßig automatisiert im Hintergrund aufbereitet werden (dafür existiert mittlerweile auch eine große Auswahl an Tools, bspw. „Magnet Axiom"). Auch wird vom Auftraggeber häufig eine Stichwortliste mitgegeben, wonach genau gesucht werden soll, und diese Wörter lediglich in das Programm eingefügt. Die Treffer kennzeichnet das Programm später automatisiert.[774]

Im Einzelfall kann es sich aber durchaus auch um eine Sachverständigentätigkeit handeln, soweit eben schon besondere Sachkunde erforderlich wird: Das beginnt bereits bei einer Sicherung des Asservats am Tatort unter Achtung geltender forensischer Grundprinzipien[775] und gilt v. a. auch im Hinblick auf die Bewältigung von „big data" oder der Anwendung spezieller Datensiche-

773 OLG Schleswig, Beschl. v. 10.1.2017 – 2 Ws 441/16.

774 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

775 Vgl. OLG Saarbrücken, Beschl. v. 20.9.2018 – 1 Ws 104/18.

rungsverfahren wie „selective imaging“ (i. S.e. *verhältnismäßigen* Ermittlungsmaßnahme). Abgesehen davon widerspricht das Argument, dass es sich dabei lediglich um vorbereitende Maßnahmen oder Hilfstätigkeiten handelt, die für sich genommen keine erforderliche Sachkunde benötigen und an Ermittlungsbehörden ausgegliedert werden könnten, wohl auch einer prozessökonomischen forensischen Auswertung (Stichwort aus der aktuellen Rechtsprechung: „Gesamtbetrachtung der forensischen Tätigkeit“, siehe später genauer bei IV. 3.) und den Ausführungen bei B. II. 2. f)), wonach auch Hilfsarbeiten (untergeordnete Verrichtungen) bei der Vorbereitung der sachverständigen Tätigkeit in das Gutachten übernommen werden (wobei die jeweiligen Personen für untergeordnete Hilfstätigkeit nicht explizit genannt werden müssen). Weiter berichtet die Praxis, dass selbst die Untersuchung, welche Personen auf welchen Ordner in einem Unternehmen Zugriff haben, in den allermeisten Fällen die Kenntnisse einer durchschnittlichen Ermittlungsperson übersteigen dürften. Hierbei sind tiefere Kenntnisse im Bereich der „IT-Administration“ notwendig, die von einer „durchschnittlichen“ Ermittlungstätigkeit nicht mehr gedeckt sind. Neben den Berechtigungen für einzelne Personen oder Gruppen, gibt es eine Vielzahl von weiteren Personen, die möglicherweise Zugriff auf die Daten haben könnten: So können im Unternehmen bspw. auch lokale Administratoren, die sich direkt am Server anmelden, Zugriff auf die Daten haben, ohne dass das im Rechtemanagement angezeigt wird. Es besteht auch die Möglichkeit, dass sich ein Administrator/Mitarbeiter temporären Zugriff zu den Daten beschafft und nach erfolgreicher Tatausführung die Berechtigung wieder abgelegt hat. Solche Möglichkeiten wären Personen, die kein besonderes Fachwissen im Bereich der IT haben, wohl eher nicht geläufig.[776]

Weiter führen die Autoren aus, dass es sich bei der Beweisfrage nach Vollständigkeit der Daten, bzw. ob Daten „vorenthalten“[777] wurden, nur dann um eine Sachverständigentätigkeit handelt, wenn eine komplexe Analyse des Quellcodes oder Metadaten erforderlich werden. In den allermeisten Fällen könne man jedoch etwaige Lücken ohne besonderes Fachwissen durch den Abgleich von Daten oder durch eine Plausibilisierung anhand des Inhalts feststellen, bspw. durch Betrachten der Datenfolgen oder des Kontextes.[778]

Festzustellen, ob bspw. Kommunikationsdaten vollständig sind, ist allerdings keine triviale Aufgabe, die von einem „durchschnittlichen“ Ermittler durchgeführt werden kann. Hierfür sind meistens sehr viel Erfahrung der jeweiligen Programmanwendung oder vertieftes technisches Wissen notwendig.

---

776 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

777 Was unter „vorenthalten“ verstanden wird, ist unklar. Dabei kann „gelöscht“ oder „verschlüsselt“ gemeint sein.

778 *Wackernagel/Graßie*, NStZ 2021, S. 12.

M. E. – auch nach Rücksprache mit Praktikern – sollte das (grds.) von einem IT-Sachverständigen durchgeführt werden, da die Tools häufiger fehlerhaft sind[779] und es selbst bei guten Forensikern oftmals ein Glücksfall sein kann, dass sie auf die Fehler aufmerksam werden, insb. wegen der riesigen Datenmenge; ein Abgleich aller Daten ist kaum realisierbar. Im Hinblick auf das Erkennen von verschlüsselten Daten gibt es zwar Heuristiken, die darauf hinweisen, um eine „triviale" Aufgabe handelt es sich dabei allerdings auch nicht. Hier muss regelmäßig manuell mit besonderer Sachkunde der forensischen Informatik vorgegangen werden.[780]

2. Eine Stellungnahme

Wie bereits oben dargestellt, kommt es bei der Abgrenzung zwischen einer Sachverständigen- und Ermittlungstätigkeit immer auf den konkreten Einzelfall an. Eine verallgemeinernde Betrachtung, wie die der Autoren, kann dem nicht gerecht werden. Es wird zwar deutlich, dass ebenfalls ein Mangel in der sehr allgemeinen und offenen Fragestellung der Auftraggeber zu sehen ist (siehe dazu oben B. II. 3. c)); ob es in den jeweiligen Einzelfällen aber dennoch gerechtfertigt war, einen Sachverständigen zu beauftragen, kann so nicht nachvollzogen werden.

Dass aber auch der Gesetzgeber gesehen hat, dass für den Schritt der forensischen Durchsicht von IT-Asservaten umfangreiches Expertenwissen erforderlich ist, zeigt die Novellierung des § 110 Abs. 1 StPO, wonach eine generelle Überlassung von Daten an Spezialisten der gesetzlichen Ermittlungspersonen i. S. d. § 110 Abs. 1 StPO – der Polizei und der Steuerfahndung – zu erfolgen hat, da diese besonders ausgebildete, spezialisierte und erfahrene Ermittlungspersonen im Bereich forensischen Informatik sind.[781] Da es dabei aber durchaus nicht wenige Fälle geben wird, in denen ein sehr spezialisierter, vom präsenten Wissen der Ermittlungspersonen nicht umfasster Umstand und ein nicht regelmäßig wiederkehrender Sachverhalt vorliegt, wird es dennoch häufig angezeigt sein, einen Sachverständigen hinzuzuziehen.

Durch die von den Autoren verwendeten allgemeinen Begriffe, kann kein Rückschluss gezogen werden, was genau die jeweilige (forensische) Tätigkeit beinhaltete und nach welcher Methode vorgegangen wurde. Diese Aspekte wären jedoch für eine Kategorisierung in Sachverständigen- oder Ermittlungstätigkeit erforderlich, da nur durch die Details die Erforderlichkeit einer besonderen Sachkunde festgestellt werden kann. Ein weiteres Augenmerk bei

---

779 Vgl. www.deutschlandfunk.de/probleme-bei-digitalen-ermittlungen-wenn-forensik-software-100.html [27.6.2023].

780 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

781 Vgl. MüKo-StPO/*Hauschild*, § 110 Rn. 11; KK/*Bruns* § 110, Rn. 4.

der Abgrenzung sollte auch auf den Kontext des Deliktsbereiches geworfen werden, da z. B. bei Verfahren in Bezug auf das Deliktsfeld der §§ 184b ff. StGB die Tätigkeit des Sichtens der Daten anders zu bewerten ist als bei dem Sichten eines Asservats, wenn es um den Tatvorwurf des Ausspähens von Daten i. S. v. § 202a StGB geht. Letzteres erfordert weit mehr an Expertise aus dem Bereich der (forensischen) Informatik.[782]

Im Rahmen dieser Arbeit werden im 3. Teil die einzelnen forensischen Schritte (am Beispiel der Datenträgerforensik) dargestellt und beschrieben, um auch in diesem Zusammenhang mehr „Klarheit" in eine versuchte Kategorisierung und Bewertung der Erforderlichkeit einer besonderen Sachkunde zu bringen.

3. Aus Sicht der Strafrichterinnen

In den hier dargestellten Strafverfahren geht es jeweils um die zu entscheidende Frage, ob die forensische Tätigkeit tatsächlich Sachverständigenqualität aufzeigte oder es sich vielmehr um genuine Ermittlungstätigkeit handelte; denn je nachdem hat die Kosten des Verfahrens entweder die verurteilte Person (IT-Sachverständige) oder die Staatskasse (Ermittlungsperson) zu tragen (siehe oben bei III. 2. d.). War der Auslagentatbestand des § 3 Abs. 2 GKG i. V. m. Nr. 9015, Nr. 9005 KV GKG i. V. m. JVEG nicht erfüllt, und hatte die Aufgabenzuweisung damit keine Sachverständigenqualität, wurden die Gutachterkosten zu Unrecht auf den Verurteilten übertragen, was, wie oben dargestellt, im Bereich der forensischen Informatik oft erst „nach getaner Arbeit" festgestellt werden kann.

a) Leitlinien zur Bestimmung der Sachverständigentätigkeit

Die Gerichte knüpften bei der Subsumtion der Tätigkeit unter den Auslagetatbestand an der Definition der Sachverständigentätigkeit an die bisherige Rechtsprechung[783] an. Diese stellten „Leitlinien" für die Abgrenzung zwischen Sachverständigen und Ermittlungspersonen auf: Es handelt sich danach um Sachverständigentätigkeit, wenn das Folgende gegeben ist:

- Sachkunde und eine eigenverantwortliche Tätigkeit, die frei von jeder Beeinflussung ist und zu einem bestimmten Beweisthema erfolgte;

---

782 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

783 KG Berlin, Beschl. v. 23.12.2008 – 1 Ws 1/07 (Bei der StA eingegliederte Wirtschaftsreferentin); OLG Koblenz, Beschl. v. 21.1.2010 – 2 Ws 21/10 (Arzthelferin als Sachverständige); BGH, Beschl. v. 2.3.2011 – 2 StR 275/10 (Ersuchen um technische Unterstützung bei der Wiederherstellung gelöschter Computerdateien).

- diese sich nicht in der bloßen Sichtung der sichergestellten Unterlagen oder dem Geben von Hinweisen für die weitere Ermittlungstätigkeit erschöpfte; es darf sich auch nicht um schlichtes Sammeln EDV-mäßig erfassten Datenmaterials ohne wertende Überprüfung gesicherter Unterlagen auf ihre Bedeutung für das Strafverfahren handeln.
- „Korrektiv": Wenn es sich um die Sichtung und Erhebung von Datenmaterial handelt, muss die Sichtung auf Grund besonderer, nicht jedermann zur Verfügung stehender technischer Möglichkeiten und Kenntnisse erfolgt sein. Indiz dafür ist der Einsatz geeigneter Rechenprogramme, die nicht jedermann zur Verfügung stehen und nicht von jedermann beherrscht werden können oder die Datenerhebung zur Klärung bestimmter sachverständig zu beurteilender Zusammenhänge erforderlich und zur Vorbereitung einer schließlich zu erstellenden gutachterlichen Äußerung ausgeführt wird.

So hatten sich die Richter mit der Abgrenzung zwischen der Sachverständigen- und Ermittlungstätigkeit v. a. aus dem Deliktsfeld der §§ 184b ff. StGB[784] und in Wirtschaftsstrafverfahren[785] ausgiebig zu befassen.

Nachfolgend sollen beispielhaft die jeweiligen Entscheidungsgründe von ausgesuchten Beschlüssen/Urteilen dargestellt werden.

b) OLG Schleswig, Beschluss vom 10.1.2017 – 2 Ws 441/16

Zunächst soll ein Blick in die Entscheidungsgründe des OLG Schleswig vom 10.1.2017 geworfen werden: Bei der Tätigkeit des beauftragten IT-Sachverständigen ging es um die Auflistung kinderpornografischer Dateien in einer Excel-Tabelle, um die Mitteilung von Daten von Absender, Empfänger und Datum sowie die Angabe von Fundstelle und die Auswertung der Kom-

---

[784] Übersicht (Stand Januar 2024): OLG Schleswig, Beschl. v. 10.1.2017 – 2 Ws 441/16; LG Köln Beschl. v. 8.2.2017, Az. 102 Qs 3/17; KG, Besch. v. 25.7.2018 – 1 Ws 65/17; OLG Saarbrücken, Beschl. v. 20.9.2018 – 1 Ws 104/18; Vorinstanz: LG Saarbrücken (1. Strafkammer), Beschl. v. 14.3.2018 – 1 Qs 27/18; LG Hamburg, Beschl. v. 7.8.2019 – 631 Qs 27/19; BVerfG (2. Kammer des Zweiten Senats), Beschl. v. 28.12.2020 – 2 BvR 211/19; Vorinstanzen: LG Düsseldorf, 2.1.2019, 004 Qs-70 Js 6554/12-69/18; LG Düsseldorf, Beschl. v. 26.11.2018 – 004 Qs-70 Js 6554/12-69/18; LG Düsseldorf, Beschl. v. 16.11.2018 – 004 Qs-70 Js 6554/12-69/18; AG Düsseldorf, Beschl. v. 27.9.2018 – 142 Cs-70 Js 6554/12-262/15; OLG Dresden (2. Strafsenat), Beschl. v. 26.8.2019 – 2 Ws 334/19; Vorinstanz: LG Dresden (16. Große Strafkammer als Beschwerdekammer), Beschl. v. 1.4.2019 – 16 Qs 89/18; LG Dresden (16. Große Strafkammer als Beschwerdekammer), Beschl. v. 8.9.2020 – 16 Qs 37/20; Vorinstanz: AG Dresden, Urt. vom 10.4.2018 – 210 Ds 614 Js 47297/15.

[785] Übersicht (Stand Januar 2024): OLG Frankfurt (2. Strafsenat), Beschl. v. 26.5.2020 – 2 Ws 89 – 91/19; OLG Frankfurt a. M. (2. Strafsenat), Beschl. v. 11.11.2021 – 2 Ws 52/19.

munikationsdaten. Die Kosten des Gutachtens beliefen sich auf ca. 10.000 €. Auf Erinnerung des Verurteilten wurde die Kostenrechnung der Staatsanwaltschaft mit Beschluss des AG niedergeschlagen. Die weiteren Beschwerden des Bezirksrevisors hiergegen blieben erfolglos. Auch das OLG Schleswig entschied, dass es sich im zugrundeliegenden Fall um keine Sachverständigentätigkeit handelte.

Die Entscheidung wurde wie folgt begründet: Die bloße Vornahme einer organisatorischen oder technischen Dienstleistung allein reiche nicht für die Qualifikation als Sachverständigentätigkeit, mag auch hierfür umfangreiches Expertenwissen erforderlich sein. So kam zwar eine spezifische Software und begleitendes fachliches Wissen zur Anwendung, allerdings wurde auf diese Weise nicht mehr erbracht als eine technische Sichtbarmachung von Datenmaterial und eine technisch bedingte Vorsortierung von Dateimaterial. Um eine Sachverständigentätigkeit handle es sich vielmehr erst dann, wenn etwa das Beweisthema die Erstellung eines spezifischen Kommunikationsprofils in Bezug auf wiederholten Kontakt zu bestimmten Internet-Adressen sei oder wenn es um die Beantwortung der Beweisfragen nach der Wirksamkeit oder der Provenienz bestimmter Verschlüsselungstechnologien geht. Um Sachverständigentätigkeit handle es sich auch, wenn eine Auswertung mittels eines allein von dem IT-Sachverständigen entwickelten speziellen Verfahrens vorgenommen wird; nicht dagegen mit einem auf dem Markt erhältlichen Produkt, welches nach Erwerb und Schulung grundsätzlich auch von anderen IT-Spezialisten angewendet werden kann.

In Bezug auf die oben aufgelisteten Leitlinien der bisherigen Rechtsprechung kann folgendes festgestellt werden: Die Sichtung und Erhebung vorhandenen Datenmaterials wird dann nicht als Sachverständigentätigkeit angesehen, wenn sich die in Auftrag gegebene Dienstleistung lediglich in einer organisatorischen und technischen Dienstleistung wie der technischen Sichtbarmachung und einer technisch bedingten Vorsortierung von Datenmaterial erschöpft; selbst wenn hierfür umfangreiches Expertenwissen sowie der Einsatz einer spezifischen, allerdings auf dem Markt erhältlichen Software erforderlich ist.[786] So wendet sich das Schleswig-Holsteinische Oberlandesgericht vom o. g. „Korrektiv“ der bisherigen Rechtsprechung ab.

Zunächst ist nochmal darauf hinzuweisen, dass die Grenzen zwischen einfacher und besonderer Sachkunde oft fließend und schwer zu ziehen sind. Für das Merkmal der „besonderen“ Sachkunde kann es jedenfalls nicht ausreichen, dass eine Person mehr Wissen hat als eine andere beliebige Person,

[786] Laut Angaben des Gutachtens wurde die Software EnCase Version 6.16 eingesetzt. Diese sei ein auf dem Markt erhältliches Produkt des Herstellers „Guidance Software“, welches nach Erwerb und Schulung grundsätzlich auch von anderen IT-Spezialisten angewendet werden kann.

wenn dieses z. B. dem allgemeinen Wissen ihres Berufsstandes entspricht. Die Person, die zum Sachverständigen ernannt werden soll, muss sie auch gegenüber anderen ihres Berufsstands oder Wissens- und Erfahrungsstand haben und zwar auch innerhalb eines sehr speziellen Expertengebiets. Denn ansonsten handelt es sich innerhalb dieser Expertengruppe wohl nur um „einfache" Sachkunde, auch wenn es sich für jeden anderen außerhalb um Expertenwissen handelt. Anders als in der Begründung des Gerichts, darf es deshalb nicht auf die freie Verfügbarkeit der Software ankommen, sondern es muss vielmehr auf die dafür erforderliche Kenntnis und Fertigkeit in Bezug auf ihre Anwendung sowie die Bewertung der Ergebnisse für den konkreten Fall und die Mitteilung der relevanten Erfahrungssätze ankommen. Es würde der Definition der „erforderlichen besonderen Sachkunde" widersprechen, würde man diese von der freien Verfügbarkeit der entsprechenden Werkzeuge auf dem Markt abhängig machen. So wird von Medizinern schließlich auch nicht gefordert, ihre Instrumente, die bei der Befundermittlung im Rahmen ihrer sachverständigen Tätigkeit zum Einsatz kommen, selbst „zusammen zu basteln". V. a. im Hinblick auf solch ein Erfordernis eines „self made-Werkzeugs" wird zu bedenken gegeben, dass das eine gegenläufige Entwicklung der geforderten Standardisierung und Nachvollziehbarkeit der forensischen Informatik (Grundsatz der Nachvollziehbarkeit und Transparenz der Informatik, siehe Dritter Teil, A. II.) bedingen würde.

Vom vorherigen LG wird bzgl. vorbereitender Tätigkeiten der Gutachtererstattung im Rahmen der Befundermittlung – wie es die Sichtung von IT-Asservaten ist – der Vergleich zur Entnahme einer Blutprobe nach § 81a StPO gezogen. Einerseits handle es sich um eine bloße medizinische Dienstleistung, die aber – was die Bestimmung etwa des Alkoholgehalts oder des Nachweises von Drogen betrifft – zweifelsohne ebenfalls die Anwendung medizinischen Erfahrungswissens und die Bewertung des gewonnenen Sachverhalts erfordert. Auch bei der Sichtung von IT-Asservaten, dem Sichtbarmachen und der Vorsortierung von Datenmaterial bedarf es durchaus der Anwendung von Erfahrungssätzen der forensischen Informatik sowie Schlussfolgerungen bzw. Bewertungen des Sachverhalts, welche Dateien relevant werden. Auch aus der Sicht von Praktikern ist die Entscheidungsbegründung kritisch zu sehen. Professionelle Forensik-Tools würden z. T. ein „immenses" Expertenwissen im Bereich der (forensischen) Informatik erfordern. Selbst bei Standardwerkzeugen, die regelmäßig zum Einsatz kommen, müssten sich die Praktiker in spezielle IT-Themen einlesen, um die Ergebnisse des Werkzeuges richtig interpretieren zu können.[787]

[787] Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

c) LG Hamburg, Beschluss vom 7.8.2019 – 631 Qs 27/19

Bei der forensischen Tätigkeit, die dem Beschluss aus Hamburg zugrunde lag, war der Auftrag zum obigen Beispiel inhaltlich gleich.[788]

Hier distanzierten sich die Richterinnen jedoch von der Entscheidungsfindung des OLG Schleswig und wollten sich damit auch gar nicht tiefergehend auseinandersetzen, weil sie der Ansicht waren, dass es sich hier gerade nicht auf eine bloße technische Unterstützung und organisatorische Aufarbeitung beschränkte. Die in Auftrag gegebene Leistung erforderte vielmehr besondere Sachkunde und den Einsatz spezieller Technik[789]. Sie kehrten also wieder zurück zu den ursprünglichen Maßstäben.[790]

Die Sachverständigenqualität wurde insbesondere darin gesehen, dass inkriminierte Dateien zunächst überhaupt ausfindig und kenntlich gemacht, ihre strafrechtlich relevante Bedeutung herausgearbeitet sowie festgestellt wurde, wann und von wem der Verurteilte entsprechendes Material bezogen, wann und an wen er es weitergeleitet und welche Kommunikationsprogramme er hierbei verwendet hatte. Vorarbeiten und Dokumentationstätigkeiten, die bloße Hilfstätigkeiten darstellen, ändern nichts an der Sachverständigenqualität unter Vornahme einer „gebotenen Gesamtbetrachtung".

Der Behauptung des Verurteilten, der Sachverständige vermittle in seinem Gutachten keine fachwissenschaftlichen Erfahrungssätze, sondern beschränke sich größtenteils auf die Anfertigung von Übersichtstabellen und erörtere lediglich allgemeine Funktionsweisen von Programmen wie beispielsweise der Tauschbörse „eMule" oder generell oberflächliche Informationen über das Löschen von Dateien, die jedermann unproblematisch über eine Suchmaschine im Internet abfragen könne, entgegnete das Gericht, dass die ergänzenden Hinweise und Ausführungen des Sachverständigen (so etwa zu dessen Auswertungsvorgehen oder etwaigen Lesehinweisen zum Gutachten) mitnichten selbsterklärend seien. Der Sachverständige habe sehr wohl aufgrund eigener besonderer Sachkunde erlangte Erfahrungssätze mitgeteilt. So erläutert der Sachverständige bspw. in Bezug auf die vom Nutzer im Tauschbörsenprogramm „eMule" eingegebenen speziellen Suchbegriffe, dass diese bei der gezielten Suche nach kinderpornografischen Schriften sehr verbreitet sind,[791] dass sich aus der Erfahrung mit bisherigen Auswertungen gezeigt hat, dass im

---

788 Allerdings wurden die Beweisfragen ausführlicher formuliert und mit Beispielen belegt.

789 Auch hier kam die o. g. Software EnCase zum Einsatz.

790 OLG Koblenz, Beschl. v. 21.1.2010 – 2 Ws 21/10 (Arzthelferin als Sachverständige).

791 Sollte das als Indiz für „Kenntnis" gewertet werden, ist anzumerken, dass Suchmaschinen in der Eingabemaske durchaus auch Suchbegriffe „vorschlagen". Von einer

Tauschbörsen-Kontext etwa 60 % der Dateien mit für Kinderpornografie einschlägigen Benennungen tatsächlich kinderpornografische Inhalte haben[792] sowie dass im vorliegenden Fall ausgewertete Dateien des Sachverständigen über eigene Hashwerte bereits aus früheren Verfahren als kinderpornografische Schriften bekannt sind.[793] Dass im Gutachten auch allgemeinere Ausführungen zu Begriffen wie Hardware/Software oder dem Löschvorgang von Dateien enthalten seien, lässt die Einordnung als Sachverständigentätigkeit nicht entfallen, zumal diese Erläuterungen für das Verständnis derartiger Gutachten im Gesamtkontext unerlässlich wären und nicht als allgemeinkundig vorausgesetzt werden könnten. Dass einige dieser allgemeineren Informationen möglicherweise über Suchmaschinen im Internet selbst herangezogen werden könnten, führe zu keiner anderen rechtlichen Bewertung. Entscheidend sei vielmehr die von der besonderen Sachkunde des jeweiligen Sachverständigen getragene Bewertung und Einordnung auch solcher Informationen.

Fortgeführt bzw. spezifiziert haben die Richter des LG Hamburg also die bisherigen Maßstäbe dahingehend, dass die Erhebung und Sichtung von Datenmaterial dann Sachverständigenqualität aufweist, wenn es 1) nicht nur darum geht, Dateien sichtbar zu machen und zu sortieren, sondern insbesondere darum, inkriminierte Dateien ausfindig und kenntlich zu machen, ihre strafrechtlich relevante Bedeutung herauszuarbeiten sowie weitere für die Tatbestandsmerkmale der §§ 184b ff. StGB wichtige Tatsachen festzustellen (bspw. wann und von wem der Verurteilte entsprechendes Material bezogen bzw. wann und an wen er es weitergeleitet und welche Kommunikationsprogramme er verwendet hatte). Weiter ergänzen sie, 2) dass, wenn vom Auftragsumfang auch Vorarbeiten und Dokumentationstätigkeiten umfasst waren, die, wenn sie ausschließlich übertragen worden wären, möglicherweise als bloße Hilfstätigkeit angesehen werden könnten, nichts daran ändern, dass der Schwerpunkt der in Auftrag gegebenen und erbrachten Leistungen in der sachverständigen Analyse und Bewertung bestand; hier ist dann eine Gesamtbetrachtung anzuwenden. Und 3) weiter haben sie verdeutlicht, dass Erklärungen, Lesehinweise und Definitionen im Gutachten auch Sachverständigentätigkeit i. S. d. Ersten Kategorie sein können. Das entspricht auch den obigen Ausführungen der Sachverständigenkategorien (siehe II. 3. d) aa)).

Kenntnis der beschuldigten Person bestimmter Begriffe darf also nicht ohne weiteres ausgegangen werden.

792 Bl 191 d. LA; interessant wären Ausführungen im Hinblick auf die Qualität dieses Erfahrungssatzes gewesen.

793 Bl. 141 d. LA. Insbesondere diese Aussage qualifiziert aus Sicht der Verfasserin die Aussage als „besonders sachkundig“ insbesondere im Vergleich zu anderen „kundigen“ IT-Experten, denen diese Hashwerte nicht zugänglich sind.

d) OLG Saarbrücken, Beschluss vom 20.9.2018 – 1 Ws 104/18

Der Entscheidung des OLG Saarbrücken lagen zwei forensische Gutachten (inhaltlich ähnlich wie die anderen Beispiele zuvor) zugrunde. Die Gutachtenkosten beliefen sich auf ca. 20.000 €.

Zunächst hatte das vorinstanzliche AG Saarbrücken vom 18.12.2017 die forensische Tätigkeit als „technische Hilfstätigkeit" eingeordnet und sich inhaltlich dem OLG Schleswig angeschlossen. Den Beschluss hob die 1. Strafkammer des LG Saarbrücken vom 14.3.2018 auf und wies die Erinnerung des Verurteilten vom 25.10.2016 zurück, wobei sie sich inhaltlich dem LG Hamburg angeschlossen und sich damit für eine Sachverständigentätigkeit entschieden haben. Schließlich bestätigte das OLG Saarbrücken die vorherige Entscheidung und beurteilte die forensische Analyse als Sachverständigentätigkeit und führte die Einschätzungen des LG Hamburg fort im Hinblick auf den Einsatz spezieller Software und begleitendes Fachwissen als Indiz für besondere Sachkunde und die Erläuterungen im Gutachten als sachverständige Erfahrungssätze.

Der Schwerpunkt der forensischen Analyse lag eindeutig bei der Sachverständigentätigkeit, so v. a. in Bezug auf die „Bewertung der verfahrensrelevanten Daten"[794], das „Ausfiltern sicher irrelevanter Multimediadateien", die „Feststellung von Kommunikationsprogrammen und Grobsichtung der Konfigurationen und Datenablage auf relevante Bilddateien", die „Feststellung möglicher eindeutiger Ablagestrukturen und Dateinamen", und die „Feststellung verschlüsselter Datencontainer, sonstiger kryptierter Daten oder z. B. ISO-Images" des Gutachtens.

Die übrigen Punkte des Gutachtens stellten ganz überwiegend hierzu notwendige Vorarbeiten und Dokumentationsmaßnahmen dar und könnten deshalb auch nicht hiervon getrennt als bloße technische Dienstleistung gewertet werden („gebotene Gesamtbetrachtung").

Auch gehen die Richter erstmals näher auf forensische Grundprinzipien im Zusammenhang mit dem IT-Sachverständigen ein, die von Laien auf dem Gebiet der forensischen Informatik nicht umgesetzt werden könnten, bspw. wurden die Datenträger spurenschonend unter Zuhilfenahme spezieller Geräte und von Spezialsoftware ohne Inbetriebnahme ausgewertet.

794 V. a. Ermittlung von Dateien, die vom System automatisch ohne Einfluss des Anwenders erstellt wurden; Dokumentation von Erstellungsdatum, Datum des letzten Zugriffs bzw. Änderungsdatum, etc.

e) Weitere Rechtsprechungsentwicklung

Das LG Dresden (16. Große Strafkammer als Beschwerdekammer) schließt sich in seinem Beschluss vom 8.9.2020[795] dem LG Hamburg und OLG Saarbrücken an und führt damit die Rechtsprechungslinie fort. Dabei gehen sie immer expliziter auf die Sachverständigenqualität unter Bewertung der einzelnen Gutachtenteile ein. Das ist eine positive Rechtsprechungsentwicklung und eine sehr zu empfehlende Lektüre für Interessierte.

Auch in Wirtschaftsstrafverfahren herrscht Uneinigkeit. So schließt sich auch das OLG Frankfurt (2. Strafsenat)[796] in seinem Beschluss vom 26.5.2020 der Rechtsprechungslinie der letztgenannten und damit der Fortsetzung der ursprünglich aufgestellten Leitlinien an. Hervorzuheben ist die Begründung der Sachverständigenqualität mit der umfangreichen Identifizierung, Sicherung, Analyse und Aufarbeitung des immensen und ohne besondere Sachkunde nicht handhabbaren Datenvolumens im Hinblick auf den Verdacht des Betruges.

Der gleiche Strafsenat entschied sich im Folgejahr aber (bei einer ähnlichen zugrundeliegenden Gutachtenerstattung) gegen eine Sachverständigentätigkeit.[797] Die Entscheidungsgründe bezogen sich dabei auf die Rechtsprechung des OLG Schleswig.

Es zeichnet sich aber nichtsdestotrotz ab, dass sich die Rechtsprechung (grds.) in eine richtige Richtung entwickelt und dabei spezifisch auf die einzelnen Punkte des zugrundeliegenden Gutachtens eingeht und diese entsprechend würdigt.

4. Eine Stellungnahme

Der IT- Sachverständige wird tätig, wenn er gerade aufgrund besonderer Sachkunde Tatsachen feststellt und bewertet und relevante Erfahrungssätze mitteilt. Aufgrund dem eben dargestellten ist das v. a. dann anzunehmen, wenn aufgrund spezieller, nicht jedermann zur Verfügung stehender technischer Möglichkeiten und Kenntnisse (teils verborgene oder gelöschte) Daten aufgesucht, wiederhergestellt und sichtbar gemacht oder Erhalt und Weiterleitung bestimmter Dateien nachvollzogen werden sollen. Ob dabei eine am Markt erhältliche Software oder „selbst gebastelte Werkzeuge“ zum Einsatz kommen, darf m. E. nicht ausschlaggebend für die Beurteilung der besonderen

795 LG Dresden (16. Große Strafkammer als Beschwerdekammer), Beschl. v. 8.9.2020 – 16 Qs 37/20.

796 OLG Frankfurt (2. Strafsenat), Besch. vom 26.5.2020 – 2 Ws 89 – 91/19.

797 OLG Frankfurt a. M. (2. Strafsenat), Beschl. v. 11.11.2021 – 2 Ws 52/19.

Sachkunde sein. Es soll vielmehr darauf ankommen, ob die tätig gewordene Person, im Vergleich zu anderen technisch versierten Menschen, zur Beantwortung der Beweisfrage besondere Sachkunde auf dem Gebiet der forensischen Informtik anwenden musste, bspw. um die ermittelten Ergebnisse für das jeweilige Verfahren richtig zu interpretieren und zu bewerten. Wenn es sich zum Teil um bloße unterstützende Tätigkeit handelte, wie Vorarbeiten und Dokumentationstätigkeiten, der Schwerpunkt aber bei Vorgängen liegt, die den drei Aussagekategorien des Sachverständigenbeweises zugeordnet werden können, ohne dass „ermittelt" werden musste, soll eine gebotene Gesamtbetrachtung zugunsten der Sachverständigentätigkeit ausfallen. Das entspricht auch der Kritik der Verfasserin bei B. IV. 1. und den Ausführungen bei B. II. 2. f), wonach auch Hilfsarbeiten (untergeordnete Verrichtungen) bei der Vorbereitung der sachverständigen Tätigkeit in das Gutachten übernommen werden können. Zu fragen ist in diesem Zusammenhang auch, wenn ein Großteil der Arbeit nicht sachverständigengemäß honoriert wird, welcher kompetente Mensch das zukünftig noch übernimmt? Auch die IT-spezialisierten Ermittler haben wohl kaum die Ressourcen, diese „Vorarbeiten" zu leisten, die auch noch zu einer Qualitätseinbuße führen würden. Im psychiatrischen Bereich wird schließlich auch nicht die körperliche Untersuchung, wie die Blutabnahme etc., ausgegliedert.

V. Einflussmöglichkeiten der Verfahrensbeteiligten auf den bestellten Sachverständigen

In diesem Abschnitt soll in einer knappen Übersicht die Verformungen des Modells alleiniger Entscheidungsbefugnis des Gerichts aufgrund von Einflussmöglichkeiten von Staatsanwaltschaft und beschuldigter Person sichtbar gemacht werden.

Die Funktion, die die Einflussnahme der anderen Verfahrensbeteiligten auf die Sachverständigenposition erfüllt, lässt sich am besten durch den Kontrast zum angloamerikanischen Recht verdeutlichen: Dort dominieren die Parteien die Tatsachenbeschaffung und tragen zwei bewusst einseitige Rekonstruktionen des Sachverhalts vor.[798] Im deutschen Strafprozess ist die Aufgabe der Sachverhaltsfeststellung in erster Linie bei einer zum Nachforschen verpflichteten zentralen Stelle konzentriert („Inquisitionsmaxime"). Danach sind die Gerichte innerhalb der durch die prozessuale Tat gesetzten Grenzen zur Be-

[798] Vgl. nur *Zuckerman*, Principles, S. 62 f.: Sachverständige werden dort als eine besondere Art von Zeugen, „expert witnesses" behandelt und wie diese ganz selbstverständlich einer der „Parteien" zugeordnet. Das bringt natürlich kaum zu beseitigende Gefahren der Objektivität der Aussagepersonen mit sich (deshalb strenge Reglementierung).

weiserhebung in Bezug auf alle entscheidungserheblichen und noch nicht bewiesenen Tatsachen verpflichtet, §§ 155 Abs. 2, 244 Abs. 2 StPO. Dementsprechend sollte der Sachverständigenbeweis auch der neutralen Sphäre des Gerichts zuzuordnen sein, und eben nicht als Ent- oder Belastungszeuge dem Beschuldigten oder der Staatsanwaltschaft; das beugt auch einer Interessenkollision und vorurteilsgeleiteten Erstattungen des Sachverständigen vor.

1. Die dominierende Stellung der Staatsanwaltschaft im Ermittlungsverfahren

Allerdings bestellt in den allermeisten Fällen die Staatsanwaltschaft den Sachverständigen schon im Ermittlungsverfahren, § 161a Abs. 1 S. 2 StPO i. V. m. § 73 Abs. 1 StPO. In diesem Stadium kann es sein, dass von der Bestellung weder das an sich zuständige Gericht noch der Beschuldigte und sein Verteidiger erfahren; Nr. 70 RiStBV stellt lediglich Sollvorschrift dar. Mit der Einführung des § 161a StPO wird der von der Staatsanwaltschaft beauftragte Sachverständige zur Gutachtenerstattung verpflichtet, und es besteht für den Sachverständigen die Pflicht zum Erscheinen und die Bezahlung wird durch das JVEG geregelt.[799] Wie unter B. II. 2. b) dargelegt, haben dagegen der Beschuldigte und sein Verteidiger keine prozessuale Möglichkeit, einen Sachverständigen „kraft behördlichen Auftrags“ zu bestellen.

Die noch bedenklichere Praxis und gerichtliche „Gewohnheit“[800] ist aber, dass der von der Staatsanwaltschaft ausgewählte Sachverständige auch der vom Gericht in der Hauptverhandlung gehörte, letztlich nur noch bestätigte, allenfalls bestellte, keineswegs aber (der vom Gericht selbst) ausgewählte Sachverständige ist (siehe dazu bereits oben bei B. II. 2. b)).[801] Die Begründung, dass der Sachverständige bereits im Ermittlungsverfahren im Auftrag der Staatsanwaltschaft tätig geworden ist, reicht jedenfalls nicht für einen

---

[799] Gem. § 1 Abs. 1 JVEG kann die Bezahlung auch den von der StA beauftragten Sachverständigen angeboten werden.

[800] *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 298.

[801] So bereits *Walter*, Sachverständigenbeweis, S. 114; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 334 ff., 337.: Einen Verstoß gegen die Waffengleichheit stellt jedoch die Praxis dar, Sachverständige der Staatsanwaltschaft über im Ermittlungsverfahren gemachte Wahrnehmungen später vor Gericht als Sachverständige zu vernehmen und nicht als sachverständige Zeugen; vgl. aus Österreich *Wess/Rohregger*, JSt 2014/3, S. 200: Nachdem verschiedene Strafsenate des OGH in den letzten Jahren wiederholt die Grundrechtskonformität bzgl. der Bestellung des Sachverständigen aus dem Ermittlungsverfahren zum Gerichtssachverständigen im Hauptverfahren bejaht hatten, wird in der Entscheidung 17 Os 25/14a erstmals die gegenteilige Auffassung, unter ausdrücklicher Ablehnung der bisherigen Rechtsprechung, vertreten.

Befangenheitsantrag, siehe dazu bei B. V. 2. c).[802] Wie bereits dargelegt, bringt diese Bestellung- und Bestätigungspraxis zwischen Staatsanwaltschaft und Gericht zwar Vorteile mit sich, allerdings ergeben sich auch Bedenken und die Frage kommt auf, wie und ob das von der Staatsanwaltschaft in Auftrag gegebene Gutachten, so wie es dann erstellt wird, auch in die Gerichtsakten gelangt.[803] Es passiert einfach schon sehr viel Kommunikation zwischen Auftraggeber und Sachverständigen, die für den Beschuldigten und seinen Anwalt nicht mehr nachvollziehbar sind. Das führt zu einem erheblichen Vorsprung der Ermittlungsbehörde im Ermittlungsverfahren – dadurch entsteht eine faktisch ungleiche Ausgangsposition von Staatsanwaltschaft und Verteidigung. Hinzu tritt die Neigung der Staatsanwaltschaft, besonders für häufig auftretende Fragen[804] immer wieder dieselben Gutachter zu bestellen, sodass eine bedenklich enge Zusammenarbeit mit der Anklagebehörde entsteht.[805]

Eine Ungleichbehandlung ergibt sich auch daraus, dass eine Kontrolle der Einflussnahme der Staatsanwaltschaft auf den Sachverständigen dadurch behindert wird, dass dem Verteidiger nach der StPO kein Anwesenheitsrecht bei der staatsanwaltschaftlichen Vernehmung zusteht und er auch nicht über den Vernehmungstermin benachrichtigt wird.[806]

Um die dominierende und mit Vorteilen ausgestattete[807] Stellung der Staatsanwaltschaft in ihrer Anklägerrolle (als „Herrin des Ermittlungsverfahrens“) im Strafverfahren auszugleichen,[808] muss also entweder nach Rechtfertigungsgründen dafür gesucht werden oder danach, ob das Gesetz durch Gewährung eines entsprechenden favor defensionis das entstandene Ungleichgewicht beseitigt.[809] So sieht die StPO zwar Ausgleichsmechanismen vor: Bspw. ist die Staatsanwaltschaft als Organ der Rechtspflege zur Objektivität ver-

---

802 Siehe auch *Schirhakl*, Der Sachverständigenbeweis im neuen Strafprozessrecht, S. 152 f.

803 Vgl *Sarstedt*, in: FS-Schmidt-Leichner, S. 175; *Walter*, Sachverständigenbeweis, S. 115: zwischenzeitlich neue Anknüpfungstatsachen veranlassen zu Zusatzgutachten bzw. Ergänzungen oder Verbesserungen des ursprünglichen Gutachtens.

804 Wie bei der Schuldfähigkeitsbeurteilung oder bei technischen Einzelheiten von Verkehrsunfällen zu beobachten ist.

805 Dazu *Arndt*, NJW 1962, 25 (26); *Frenken*, DAR 1956, 291; *ders.*, DRiZ 1957, 169; *Hetzer*, Wahrheitsfindung, S. 163; *Lürken*, NJW 1968, 1161 (1162); *Rudolph*, Die Justiz, 24; *Tondorf/Waider*, StV 1997, 493 (496); *Wasserburg*, StV 1989, 332 (335).

806 Vgl. Meyer-Goßner/*Kleinknecht*, § 161a Rn. 3; Löwe/Rosenberg/*Rieß*, § 161a Rn. 31.

807 Aufzählung bei *Birkmeyer*, Deutsches Strafprozessrecht, S. 378 f.

808 Dieses Problem hat schon in der ersten Hälfte des 19. Jhd. Eingang gefunden, vgl. *Wohlers*, Entstehung und Funktion der Staatsanwaltschaft, S. 68 ff.

809 Dazu ausführlich *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 299 f.

pflichtet (§ 160 Abs. 2 StPO) und dadurch auch die zur Entlastung dienenden Umstände zu ermitteln[810] sowie zur Erhebung von Entlastungsbeweisen nach § 163a Abs. 2 StPO. Weiter soll die Verteidigung Gelegenheit zur Stellungnahme haben nach Nr. 70 Abs. 1 RiStBV[811]. Allerdings vermögen die Vorschriften die vorteilhafte Stellung der Staatsanwaltschaft – jedenfalls im Ermittlungsverfahren – nicht auszugleichen, da in Bezug auf all diese Ausgleichsvorkehrungen eine Möglichkeit gerichtlicher Überprüfung (abgesehen von der i. d. R. wirkungslosen Dienstaufsichtsbeschwerde) fehlt.[812]

Das BVerfG hat die nach dem Gesetz gegebene vorteilhafte Stellung der Staatsanwaltschaft ausdrücklich gebilligt[813] und auch Art. 6 EMRK ist nur mit Einschränkungen auf das Vorfahren anwendbar[814]. Nach der Rspr. des EGMR wird der „fair trial"-Grundsatz dann gewahrt, wenn das Verfahren als Ganzes betrachtet – einschließlich der Art, in der die Beweise aufgenommen wurden – fair war.[815] Solange die Verteidigungsrechte gewahrt wurden, ist die Verwendung der im Ermittlungsverfahren erlangten Aussagen als Beweismittel nicht unvereinbar mit Art. 6 Abs. 1 und Abs. 3 EMRK. Ob das der Fall ist, beurteilt der EGMR in einer Gesamtbetrachtung und lässt es ausreichen, wenn der Beschuldigte eine angemessene und geeignete Gelegenheit erhält, die Aussage auch zu einem späteren Zeitpunkt des Verfahrens zu prüfen.[816] Solange es sich also um keine abschließende oder unkorrigierbare Entscheidung der Staatsanwaltschaft handelt, wird diese Praxis toleriert.[817]

---

[810] Auch sehen §§ 296 Abs. 2, 365 i. V. m. § 301 StPO, Nr. 147 Abs. 3 RiStBV ein Ermessen der Staatsanwaltschaft vor zugunsten des Angeklagten Rechtsmittel einzulegen oder die Wiederaufnahme mit dem Ziel eines Freispruchs zu betreiben.

[811] Eine Ansicht hat den Versuch unternommen, § 163a Abs. 2 StPO für die Begründung eines solchen Rechts in Anspruch zu nehmen, vgl. dazu AK/*Achenbach*, § 163a Rn. 8; *Krekeler*, Der Beweiserhebungsanspruch, insb. S. 80 ff., *ders.*, NStZ 1991, 367; Löwe/Rosenberg/*Rieß*, § 163a Rn. 107, 112; *Nelles*, StV 1986, 74 (77); a. A. KK/*Wache*, § 163a Rn. 8; Kleinknecht/Meyer-Goßner, § 163a Rn. 15.

[812] *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 297. Im Gegensatz dazu stehen dem Beschuldigten in erhöhtem Maße durchsetzbare Rechte zu, wenn ein Ermittlungsrichter eingeschaltet wird (§§ 166 Abs. 1, 168c Abs. 5, 168d Abs. 2 StPO). Das ergibt sich daraus, dass ein verstärkter Einfluss richterlicher Vernehmungen auf das erkennende Gericht in der Hauptverhandlung möglich ist (§ 251 Abs. 1 StPO).

[813] BVerfG NStZ 1984, 228.

[814] Vgl. EKMR EuGRZ 1986, 276 (277) „Can", wo Art. 6 Abs. 3b und c EMRK auch in Bezug auf das Vorverfahren für anwendbar erklärt wurden.

[815] Zur Relevanz der EMRK und der Rspr. des EGMR für deutsche Gerichte, vgl. *Mysegades*, Software als Beweiswerkzeug, S. 84 ff. und *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 515 ff.

[816] EGMR StV 1990, 481 (482); 1991, 193 (194).

[817] *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 306.

Ein Unbehagen des Gesetzgebers bzgl. der bisherigen Praxis und der damit einhergehenden Ungleichstellung kann jedenfalls daraus entnommen werden, dass bspw. bei Anordnungen einer DNA-Analyse i. S. d. § 81e StPO der zuständige Richter in der schriftlichen Anordnung schon im Ermittlungsverfahren gem. § 81f Abs. 1 S. 2 StPO den zu beauftragenden Sachverständigen benennt. Insoweit nimmt der Richter (jedenfalls nach dem Gesetz) im Ermittlungsverfahren die Auswahl vor und nicht die Staatsanwaltschaft.[818] In der Praxis wird sich diese Besonderheit jedoch kaum auswirken, da die Richter bereits aus Zeitgründen keine Kapazitäten haben werden, die Qualität des Sachverständigen selbstständig zu überprüfen. Eine weitere Einschränkung ergibt sich daraus, dass der Sachverständige aus dem Kreis der durch § 81f Abs. 2 StPO bestimmten Personen ausgewählt werden muss.[819] Auch das Beweisverwertungsverbot bei einem Verstoß[820], falls Material des Beschuldigten untersucht worden ist, hat in der Praxis kaum Bedeutung.[821]

Nichtsdestotrotz wäre es jedenfalls besser, so wie es im Wortlaut des § 73 StPO auch vorgesehen ist, der Richter würde von der Staatsanwaltschaft um Beauftragung eines Sachverständigen ersucht und darüberhinaus auch der betroffene Be- bzw. Angeschuldigte zwingend dazu gehört werden.[822] Jedenfalls ist dringend eine Verständigung zwischen Staatsanwaltschaft und Verteidigung über Person und Fachrichtung des Sachverständigen angeraten.[823] In Fällen, in denen die Staatsanwaltschaft ohnehin davon ausgeht, dass wegen der besonderen sozialen oder beruflichen Stellung des Angeklagten oder wegen des besonderen Bekanntheitsgrades des Verteidigers von der Verteidigung ein Gutachter benannt oder geladen wird, funktioniert die Verständigung zwischen Staatsanwaltschaft und Verteidigung hinsichtlich der Person des Sachverständigen.[824]

---

818 *Eisenberg*, Beweisrecht der StPO, Rn. 1687i; *Kleinknecht/Meyer-Goßner*, § 81f Rn. 3; SK-StPO/*Rogall*, § 81f Rn. 7; a. A. *Senge*, NJW 1997, 2411: Der Richter sei an die Benennung durch die Staatsanwaltschaft gebunden.

819 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 299.

820 *Eisenberg*, Beweisrecht der StPO, Rn. 1687; *Kleinknecht/Meyer-Goßner*, § 81f Rn. 9; SK-StPO/*Rogall*, § 81f Rn. 18.

821 Weil sich entweder das Spurenmaterial so weit von der Person gelöst hat, dass kein schützenswerter Eingriff mehr vorliegt oder der Beschuldigte, der einen Eingriff rügen würde, damit erklären würde, dass er der Spurenleger sei, wodurch eine DNA-Analyse für die Überzeugungsbildung hinfällig wäre.

822 So auch schon *Walter*, Sachverständigenbeweis, S. 115; *Sarstedt*, NJW 1968, 1174 f.; *Lürken*, NJW 1968, S. 178 ff.; a. A. *Karpinski*, NJW 1968, 1173.

823 Auch das wird schon lange vorgeschlagen. *Lürken*, NJW 1968, S. 1164; *Karpinski*, NJW 1968, 1173.

824 *Walter*, Sachverständigenbeweis, S. 116.

2. Ausgleichsmechanismen

Abgesehen von der eben beschriebenen gängigen Praxis wären auch nach der Konzeption der §§ 73 StPO ff. die übrigen Beteiligten des Strafverfahrens grds. nicht aktiv in den Vorgang der gerichtlichen Beweisaufnahme einbezogen. Die Konzentration der Tatsachenbeschaffung beim Gericht ist aber unter dem Aspekt der möglichst exakten Sachverhaltsermittlung nicht ganz unbedenklich. Die Gefahr einer zu unkritischen Beweisaufnahme entsteht insbesondere beim Sachverständigenbeweis, da das Gericht sich durch die Auswahlbefugnis aus § 73 Abs. 1 S. 1 StPO ein Beweismittel schaffen kann, von dem zu erwarten ist, dass es eine vorgefasste Absicht des Gerichts stützen wird („bewährte Gutachter", die den Richtern von vorangegangenen Prozessen bekannt sind[825]). So besitzen die in hohem Maße motivierten Prozessbeteiligten ein erhebliches Potential, einseitige Informationen zu korrigieren. Um diese positiven Seiten des Potentials auszuschöpfen – ohne Verschleierungstaktiken zu begünstigen oder amerikanische Verhältnisse zu schaffen – sieht die StPO eine Reihe von Ausgleichsmechanismen vor, als Möglichkeit, die Tatsachenermittlung zu beeinflussen.

So darf nicht nur das Gericht Fragen an den Sachverständigen richten (vgl. §§ 238, 240 Abs. 1 StPO), sondern auch die Verfahrensbeteiligten, sobald ihnen das Gericht das Wort erteilt hat (§ 240 Abs. 2 StPO).[826]

Die Staatsanwaltschaft (§ 214 Abs. 3 StPO) und die beschuldigte Person bzw. die Verteidigung (§§ 220 Abs. 1, 245 Abs. 2 StPO) sind zwar zur unmittelbaren Ladung befugt, diese begründet zunächst jedoch nur die Pflicht zum Erscheinen. Auftragserteilung und Ladung sind hier deutlich voneinander zu unterscheiden (siehe bereits bei II. 2. b)).[827]

a) Antragsrechte der Verfahrensbeteiligten

In der Hauptverhandlung können die Staatsanwaltschaft und der Beschuldigte bzgl. des Gegenstandes des Beweises am effektivsten über die Stellung von Beweisanträgen Einfluss gewinnen, §§ 244 Abs. 3, 4 StPO.[828] So wird die Aufmerksamkeit des Gerichts auf bestimmte Aspekte der Beweisaufnahme

---

825 *Detter*, NStZ 1998, S. 57.

826 Unzulässige Fragen an den Sachverständigen kann das Gericht zurückweisen, unangemessene Fragen kann es untersagen (§ 241 Abs. 2 StPO). Siehe auch *Mysegades*, Software als Beweiswerkzeug, S. 106 ff., S. 150 ff.

827 *Eisenberg*, Beweisrecht der StPO, Rn. 1527a; SK-StPO/*Rogall*, § 73 Rn. 16; *Vyhnálek*, S. 60 ff.

828 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 270; vgl. zur besonderen Bedeutung des Beweisantragsrechts auch *Mysegades*, Software als Beweiswerkzeug, S. 74 ff.

gelenkt, indem es zu einer Entscheidung gezwungen wird.[829] Dabei kommt v. a. der „Cyber-Strafverteidigung" wegen ihrer benachteiligten Stellung im Strafverfahren eine besondere Rolle bei der Überprüfung der Reliabilität und Validität sowie daraus folgender Einschätzung von Zulässigkeit und Beweiswert des Sachverständigenbeweises zu.[830]

Antragsrechte zu gewähren ist jedoch mit dem Risiko behaftet, dass ein Antragsberechtigter eine ungleich stärkere Position erlangt. So könnten Antragsberechtigte versuchen, ihre Position zu nutzen, um einen ungleich stärkeren Einfluss auf die Bestimmung der Aussageperson auszuüben als andere Prozessbeteiligte und infolgedessen das Gericht zur Ernennung eines in seiner Objektivität erheblich beeinträchtigen Sachverständigen zu beeinflussen. In letzter Konsequenz kann das zu einer Verzerrung der Tatsachendarstellung führen.[831] Im Interesse einer exakten Sachverhaltsaufklärung müssen Mechanismen bereitstehen, die verhindern, dass einseitig günstige Prozesslagen zugunsten der Staatsanwaltschaft oder des Beschuldigten entstehen, sondern die Inquisitionsmaxime des Gerichts favorisieren, gleichzeitig aber auch letztgenannte zu berichtigen.[832]

Bei den Antragsrechten (und anderen prozessualen Mitwirkungsrechten der Beteiligten) ist daher auf ein strukturelles Gleichgewicht zu achten („Prinzip der Waffengleichheit", Art. 20 Abs. 3 GG, Art. 103 Abs. 1 GG, Art. 6 Abs. 1 EMRK).[833] Waffengleichheit bedeutet dabei keine streng formale Gleichheit[834], sondern einen verfassungsrechtlichen Auftrag zur Ausbalancierung der rechtlichen Positionen der Staatsanwaltschaft und des Beschuldigten. An diesem Auftrag muss sich die gesetzliche Regelung und die Gerichtspraxis messen lassen. Das Recht auf ein faires Verfahren fordert, dass der Beteiligte eines Gerichtsverfahrens eine echte Möglichkeit haben muss, zu einem Beweismittel Stellung zu nehmen. Das gilt besonders, wenn das Beweismittel aus einem technischen Bereich stammt, in dem das Gericht und der Verfahrensbeteiligte nicht über Sachkenntnis verfügen.[835]

---

829 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 291 f.

830 Grundthese 2 von Dr. Uwe Ewalds Vortrag auf dem Erlanger Cybercrime Tag 2020.

831 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 293.

832 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 293.

833 Mehr zur Waffengleichheit nach der Rspr. des EGMR in *Safferling*, NStZ 2004 181; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 291, 339 ff.; *Den Hartog*, in: Forensic expertise and the law of evidence (Hrsg. Nijboer/Callen/Kwak), S. 148 (156).

834 Eine strenge formale Gleichheit ist schon deswegen nicht möglich, weil die Staatsanwaltschaft umfassende Ermittlungsmöglichkeiten besitzt, die dem Beschuldigten nicht zugestanden werden können, vgl. *Roxin*, Strafverfahrensrecht, § 12 Rn. 13.

835 Vgl. LG Berlin, EuGH-Vorlage v. 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22), Rn. 84; Urt. v. 2.3.2021 – C-746/18, Rn. 44; Urt. v. 6.10.2020 – C-511/18 u. a.,

Das Gesetz hält dahingehend eine Vielzahl von Regeln über das „Beweisantragsrecht" bereit, um über die bestehende richterliche Aufklärungspflicht aus § 244 Abs. 2 StPO hinaus die Möglichkeit zur Einflussnahme auf die Sachverhaltsfeststellung auszuüben.[836] Die Überlegungen zur Erstattung von Beweisanträgen sind im Grunde identisch zu den Ausführungen bzgl. der Beauftragung eines Sachverständigen (siehe zu den Ausführungen oben bei B. I. 2. und B. II. 2. a)).[837] In diesem Zusammenhang spielt auch das bereits erwähnte „Verbot der Beweisantizipation"[838] eine wichtige Rolle.[839]

Ob das Gericht verpflichtet ist, einen IT-Sachverständigen mit der Untersuchung einer 1:1-Kopie des Original-Datensatzes zu beauftragen bzw. Beweisanträgen dahingehend stattzugeben, oder ob es sich mit sachferneren Beweismitteln wie Ausdrucken, Bildern oder Videos als Urkunden- oder Augenscheinsbeweis begnügen darf, ist von den konkreten Einzelfallumständen abhängig. Ähnliches gilt auch für Beweisanträge auf Bestellung eines Ober- oder Zweitgutachters zur Plausibilitätskontrolle der Methodik des ersten Gutachtens, wenn den Prozessbeteiligten nach der Befragung des Sachverständigen erhebliche Zweifel an der Zuverlässigkeit des Gutachtens verbleiben.[840] Um noch einmal die Ergebnisse von Rückert[841] hervorzuheben: Aus der Pflicht des Gerichts zur Ermittlung der materiellen Wahrheit (Amtsaufklärungspflicht) nach § 244 Abs. 2 StPO und den Grundsätzen der freien richterlichen

---

Rn. 226 f. und Urt. v. 10.4.2003 – C-276/01 Rn. 77; EGMR, Entsch. v. 18.3.1997 („Mantovanelli/Frankreich").

836 Zum Verhältnis zwischen gerichtlicher Aufklärungspflicht und dem Beweisantragsrecht bzw. zum „Beweisantizipationsverbot", vgl. ausführlich *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 308 ff. m. w. N.: Grds. sind die Maßstäbe identisch, Ausn.: in besonders schweren Fällen psychiatrischer Beurteilungen (BGHSt 23, 8 (11); 23, 176 (187 ff.)) oder Schriftsachverständigen (BGHSt 10, 116 (118); BGH StV 1986, 376). Nach dem BGH zwinge die Aufklärungspflicht bei möglichem Einfluss auf die Überzeugungsbildung weitere Sachverständige auch dann anzuhören, wenn § 244 Abs. 4 S. 2 StPO die Ablehnung eines Beweisantrags gestatte. Demnach ginge die Aufklärungspflicht aus § 244 Abs. 2 über das Beweisantragsrecht hinaus. Kritisiert wird diesbezüglich, dass das Gericht verkenne, dass das Gegenteil der behaupteten Tatsache eben noch nicht erwiesen sein darf i. S. d. § 244 Abs. 4 S. 2 StPO, wenn erhebliche abweichende Stellungnahmen noch einbezogen werden müssen.

837 Vertiefender dazu siehe auch *Schneider*, NStZ 2023, 65; *Trück*, NStZ 2007, 377.

838 Wurde vom RG entwickelt, um Beweisanträge in der ersten historischen Phase zu begünstigen, vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 309.

839 Vertiefend dazu auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 662 ff.

840 Vgl. zu diesem Punkt auch *Mysegades*, Software als Beweiswerkzeug, S. 160 f. Gründe nach § 244 Abs. 4 S. 2 HS. 2 StPO wären z. B. Zweifel an der Sachkunde des Sachverständigen, falsche Anknüpfungstatsachen, Widersprüche im Gutachten oder Existenz überlegener Forschungsmittel.

841 Digitale Daten als Beweismittel im Strafverfahren, insb. S. 673 ff.

Beweiswürdigung nach § 261 StPO und insbesondere deren Einschränkung durch das Erfordernis einer objektiv tragfähigen Tatsachengrundlage folgt, dass das Tatgericht bei der Entscheidung dieser Frage folgende Rechtssätze zugrunde legen muss: 1) Die Beweiswürdigung ist lücken- und damit fehlerhaft, wenn – entgegen des Prinzips der vollständigen und erschöpfenden Beweiswürdigung – die Heranziehung weiterer Beweismittel nach den bekannten oder erkennbaren Umständen naheliegt oder zumindest die Möglichkeit besteht, dass das Beweismittel die Perspektive des Gerichts auf den Sachverhalt verändert. 2) Nach dem Grundsatz des bestmöglichen und sachnächsten Beweismittels muss das Tatgericht außerdem das beste und das im Verhältnis zum jeweiligen Beweisthema unmittelbarste Beweismittel heranziehen; und 3) nach dem Verbot der Beweisantizipation muss das Tatgericht außerdem, wenn es von der Heranziehung eines erreichbaren Beweismittels absehen will, in einer rational nachvollziehbaren Argumentation, die sich auf bereits erwiesene Tatsachen und bereits verwendete Beweismittel stützt, begründen, warum aus dem neuen Beweismittel keine weiteren Erkenntnisse zu gewinnen sind.

Bei Berücksichtigung der vorstehenden Rechtssätze ergibt sich hinsichtlich der Pflicht zur Beauftragung eines IT-Sachverständigen mit der Untersuchung einer 1:1-Kopie der Originaldaten anstelle oder zusätzlich zur Einführung der Informationen mittels Urkunden oder Augenscheinsobjekten folgendes: 1) Die Untersuchung einer 1:1-Kopie des Originaldatensatzes durch einen IT-Sachverständigen ist regelmäßig dann notwendig, wenn von der Auswertung weitere verfahrensrelevante Informationen zu erwarten sind, die über diejenigen hinausgehen, welche durch die Einführung der visualisierten Informationen im Wege des Urkunden- oder Augenscheinsbeweises (Ausdruck, Fotografie, Grafik usw.) gewonnen werden können und für das Verfahren von Bedeutung sind. Und 2) ob das Tatgericht dennoch auf die Beauftragung des IT-Sachverständigen verzichten darf, hängt davon ab, ob die durch sein Gutachten zu erwartenden zusätzlichen Informationen – unter Beachtung des (beschränkten) Verbots der Beweisantizipation – auch durch andere Beweismittel oder eine glaubhafte Einlassung des Beschuldigten gewonnen werden können und somit die Einholung des Gutachtens überflüssig ist. In den allermeisten Fällen wird das Gericht jedoch verpflichtet sein, einen IT-Sachverständigen – als bestmögliches und sachnächstes Beweismittel – zu beauftragen bzw. Beweisanträgen dahingehend stattzugeben.[842]

[842] *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 474 ff., S. 569.

b) Die Einsicht in das schriftliche Gutachten und in die Arbeitsunterlagen

Wie oben erörtert, muss das sachverständige Gutachten im Rahmen der Hauptverhandlung grds.[843] mündlich erstattet werden.[844] Das Gericht geht jedoch in den meisten Fällen im Hinblick auf die Revisibilität des Urteils ein erhebliches Risiko ein, wenn es kein vorbereitendes schriftliches Gutachten anfertigen lässt und dieses nicht eine angemessene Zeit vor der mündlichen Verhandlung, in der der Sachverständige vernommen wird, den Prozessbeteiligten zugänglich macht (siehe auch bei Leitungspflicht nach § 78 StPO, B. VII.). Da eine Gutachtenerstattung erforderlich wird, weil die eigene Sachkunde des Gerichts zur Beurteilung des Sachverhalts nicht hinreicht, ist regelmäßig ein erheblicher Schwierigkeitsgrad des Gutachtens zu erwarten, dem der Angeklagte und sein Verteidiger nicht ohne weiteres gewachsen sein werden. Die Komplexität der Sachverhalte kann zudem noch durch eine schwer verständliche Terminologie für Außenstehende (selbst für Fachkollegen) während der mündlichen Präsentation verkompliziert werden. Auch weist das gerichtliche Protokoll der Hauptverhandlung i. d. R. keine so detaillierten Gedankengänge auf, dass eine spätere Kontrolle, etwa durch einen anderen Sachverständigen, möglich wäre.[845] Damit gewinnt das vorbereitende schriftliche Gutachten für die Nachweisbarkeit von Mängeln, was wiederum für eine erfolgreiche Revision relevant ist, erhebliche Bedeutung (sofern der Sachverständige in der mündlichen Präsentation nicht davon abweicht). Weiter besteht die Gefahr vor Überraschungseffekten.

Aus den eben genannten Gründen setzt eine gründliche Auseinandersetzung mit dem Gutachten regelmäßig voraus, dass es in angemessener Zeit vor der Hauptverhandlung schriftlich abgeliefert wird. Oft endet das Interesse der Prozessbeteiligten allerdings nicht bei der Einsicht in das vorbereitende schriftliche Gutachten als Ergebnis der Analyse, sondern erstreckt sich auch auf die dazugehörigen Arbeitsunterlagen und Analysewerkzeuge. Denn nur anhand dieser können die Prozessbeteiligten oder von ihnen beauftragte private Sachverständige eine detaillierte Prüfung seiner Methoden, Berechnungen, Grundlagen und Prämissen vornehmen.[846] Die Prüfung der schriftlichen Unterlagen kann auch die Grundlage für weitere Fragen an den Sachverständigen oder entsprechende Beweisanträge sein. Das gilt gerade auch für Datenverarbeitungs- und -analysevorgänge, die der Sachverständige als Werkzeug

---

843 Zu den Ausnahmen oben in diesem Teil, II. 3. a).

844 Abgeleitet aus den in § 251 StPO verankerten Grundsätzen der Mündlichkeit und Unmittelbarkeit in der Hauptverhandlung.

845 Vgl. auch *Müller*, Der Sachverständige im gerichtlichen Verfahren, Rn. 697.

846 *Mysegades*, Software als Beweiswerkzeug, S. 152.

für seine Arbeit nutzt. Hier sind insbesondere die Tools, Rohdaten, Anwendungsanweisungen, Trainingsdaten und verknüpften Systeme relevant.[847] Zu diesen Unterlagen benötigt ein weiterer (privater) Sachverständiger zur Prüfung der Methode i. d. R. Zugang.[848] V. a. aufgrund des bereits geschilderten „Übersetzungsproblems" (A. III. und IV.) und der Beschaffenheit bzw. der (zudem nicht standardisierten) Arbeitsweise der (v. a. statistischen und selbstlernenden) Datenverarbeitungs- und -analyseverfahren können der Beschuldigte und dessen Verteidiger – ohne Zugang zu den verarbeiteten Daten und ohne detaillierte Kenntnis hinsichtlich der verwendeten Verfahren – nicht nachvollziehen, wie die gegen den Beschuldigten verwendeten digitalen Spuren zustande kommen und ob und ggf. inwieweit diese verlässlich sind.[849] Das ergibt sich auch aus dem Vorabentscheidungsersuchen an den EuGH in Bezug die Verwertbarkeit von Informationen aus EnchroChat-Daten im Strafverfahren.[850] Danach können die Fragen im Zusammenhang mit der Integrität der Daten (d. h. deren Korrektheit, Vollständigkeit und Konsistenz), die im Hinblick auf die technischen Methoden, mit denen die EncroChat-Daten abgefangen, ausgeleitet, gespeichert und schließlich nach Ländern sortiert auf dem Europol-Server zum Download bereitgestellt wurden, nur durch Zugang zu ihnen geklärt werden. Für die Verteidigung kommt es in besonderem Maße nicht nur auf die Auswertung einzelner Nachrichten, sondern auf den zeitlichen und inhaltlichen Bezug von gesendeten und empfangenen Nachrichten an. Technische Fehler und Unvollständigkeiten bergen damit in besonderem Maße die Gefahr, dass Chatverläufe auch unbeabsichtigt sinnentstellt werden, ohne dass das beim Lesen der Auswerteprotokolle zu bemerken wäre.[851] Zu einer effektiven Verteidigung gehört es, die gegen den Beschuldigten vorgebrachten Beweismittel auf ihre Verlässlichkeit zu überprüfen und diese ggf. durch die Stellung entsprechender Beweisanträge anzugreifen.[852] Das wird besonders relevant bei (statistischen) Datenanalysemethoden, bei denen die Richtigkeitswahrscheinlichkeit der in den Algorithmen steckenden Annahmen/Heuristiken entscheidende Bedeutung für den Beweiswert des Ergebnisses hat und bei der Verwendung sog. Blackbox-Tools (v. a. selbstlernende Systeme), bei denen selbst den Strafverfolgungsbehörden und IT-Sachver-

847 So etwa *Lehmann*, GA 2005, S. 639 (641); vgl. ähnlich zu Spurenakten und vergleichbaren Unterlagen *Peters*, in: GS Kaufmann, S. 913 (915 f.).

848 *Mysegades*, Software als Beweiswerkzeug, S. 152 f.

849 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 25 f., S. 698 ff.

850 LG Berlin, EuGH-Vorlage v. 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22).

851 LG Berlin, EuGH-Vorlage v. 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22), Rn. 83.

852 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 25 f., S. 698 ff.

ständigen die genaue Funktionsweise der verwendeten Methode unbekannt ist.[853]

Dem grund- und menschenrechtlich verbürgten Interesse an der Einsichtnahme durch die Verteidigung als Ausfluss des Rechts auf ein faires Verfahren in seiner Ausprägung der prozessualen Waffengleichheit nach Art. 20 Abs. 3 i. V. m. Art. 2 Abs. 1 GG und Art. 6 Abs. 1, 3[854] EMRK und abgeleitet aus dem Anspruch auf rechtliches Gehör nach Art. 103 Abs. 1 GG,[855] stehen dem allgemeinen Interessen der Justiz an der Vermeidung von Gefährdungen des Untersuchungszwecks, des Rechtsmissbrauchs und der Verfahrensverzögerung entgegen sowie dem darüber hinausgehenden polizeilichen und justiziellen Interesse, als auch den Rechten Dritter, wie etwa dem Bekanntwerden der genauen Funktionsweise bis hin zum Quellcode der Datenverarbeitungs- und -analysesoftware.[856]

Es ergibt sich die Frage, ob und wie die Verteidigung im Rahmen ihres Akteneinsichtsrechts nach § 147 StPO oder auf anderem Wege Einsicht in das vorbereitende schriftliche Sachverständigengutachten und die zugrundeliegenden Arbeitsunterlagen (in die Daten, die einzelnen Verarbeitungs- und Untersuchungsschritte und die verwendeten Datenanalysemethoden) erhält.

aa) Die Einsicht in das Sachverständigengutachten nach § 147 StPO

Wenn das vorbereitende schriftliche Sachverständigengutachten, das in der gängigen Praxis von der Staatsanwaltschaft in Auftrag gegeben wird, sowie die dazugehörigen Arbeitsunterlagen, wie etwa die Beweisdaten und verwendeten Tools, Bestandteil der Verfahrensakten bzw. Beweisstücke würden, unterfallen sie dem Einsichtsrecht bzw. Besichtigungsrecht nach § 147 Abs. 1 StPO. Nach § 147 Abs. 1 StPO ist dem Verteidiger Einsicht in alle dem Gericht vorliegende oder nach der Anklage vorzulegende (§ 199 Abs. 2) Akten zu geben.[857] Nach § 147 Abs. 3 StPO unterfallen ausdrücklich Sachverständigengutachten denjenigen Aktenbestandteilen, zu denen dem Verteidiger auch

---

853 Siehe dazu vertieft *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 688, S. 698 ff.; *Mysegades*, Software als Beweiswerkzeug, S. 156 ff.; *Valerius*, ZStW 133 (2021), S. 152 (166 ff.).

854 Siehe zum Konfrontationsrecht des Beschuldigten aus Art. 6 Abs. 3 lit. d EMRK analog für Softwareanwendung, *Mysegades*, Software als Beweiswerkzeug, S. 93 f.

855 Siehe zum rechtlichen Gehör, *Mysegades*, Software als Beweiswerkzeug, S. 99.

856 Dazu auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 700; *Nink*, Justiz und Algorithmen, S. 339 f.; *Mysegades*, Software als Beweiswerkzeug, S. 155 f.

857 Vgl. *Willnow*/KK, § 147 Rn. 4 (9. Auflage 2023).

nicht nach Abs. 2 der Zugang versagt werden darf.[858] So ergibt sich bereits aus dem Gesetzestext, dass die vorbereitenden schriftlichen Sachverständigengutachten Bestandteil der Akte sind. Was ist jedoch mit den Arbeitsunterlagen?

bb) Die Einsicht in die Arbeitsunterlagen nach § 147 StPO bzw. unter Berücksichtigung des Rechts auf ein faires Verfahren

Zu den Arbeitsunterlagen gehören z. B. Untersuchungsunterlagen, Testergebnisse[859] oder Mitschriften bzw. Tonbandaufzeichnungen von Explorationen[860]. Im Bereich der forensischen Informatik wären das u. a. Beweisdaten (bzw. ihre Kopien)[861], angwendete Datenverarbeitungs- und -analysesoftware, sowie Informationen und Quellcode der verwendeten Tools.[862]

Ob die Beweisdaten, eine exakte Funktionsbeschreibung oder sogar der Quellcode der verwendeten Datenverarbeitungs- und -analysemethoden ihren Weg in die Verfahrensakten finden, hängt zunächst maßgeblich davon ab, ob die Staatsanwaltschaft die Daten und Methoden zum Bestandteil der Verfahrensakten macht, die sie gem. § 199 Abs. 2 S. 2 StPO mit der Anklage dem Gericht vorlegt. Rückert führt in diesem Zusammenhang überzeugend aus, dass diese den Gutachten zugrundeliegenden Arbeitsunterlagen grds. dem formellen und materiellen Aktenbegriff[863] unterfallen und damit als „Akten-

---

858 Nach st. Rspr. RGSt 72, 268 (275); KG JR 1965, 69; OLG Düsseldorf JZ 1986, 508; OLG Schleswig SchlHA 1952, 50; OLG Stuttgart NStZ 1986, 45 (46), und ganz h. L. KK/*Laufhütte*, § 147 Rn. 2; *Kleinknecht/Meyer-Goßner*, § 147 Rn. 3, jeweils m. w. N. hat der Beschuldigte im Strafverfahren kein Akteneinsichtsrecht. Im Falle eines Sachverständigengutachtens wird er sich aber i. d. R. ohne Aktenkenntnis nicht hinreichend verteidigen können, so dass wegen Schwierigkeiten der Sach- und Rechtslage i. S. d. § 140 Abs. 2 S. 1 StPO ein Fall notwendiger Verteidigung vorliegt.

859 BGH StV 1989, 141.

860 BGH StV 1995, 565.

861 So ähnlich auch schon *Lehmann*, GA 2005, 639 (647), der davon ausgeht, dass eine verfassungskonforme Auslegung von § 244 Abs. 2 StPO anhand des Grundsatzes des fairen Verfahrens eine Vorlagepflicht des Sachverständigen hinsichtlich der Grundlagen und Rohdaten seines Gutachtens begründet, die der Verteidigung dann wiederum vorzulegen sind. Der Beschuldigte muss hierzu noch keine Fehleranhaltspunkte geltend machen oder bestimmte Punkte rügen.

862 Zur weiterführenden Problematik der Unzugänglichkeit des Quellcodes siehe *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 691 f., S. 708 f.

863 Ausführlich zu den Aktenbegriffen *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 701 m. w. N. Von einem engeren Verständnis des formellen Aktenbegriffs geht *Mysegades*, Software als Beweiswerkzeug, S. 338 ff. aus. Vgl. zum (Akten-)Einsichtsrecht in Unterlagen bei standardisierten Verfahren *Mysegades*, Software als Beweiswerkzeug, S. 266 f.

bestandteile“[864] zu führen wären.[865] In der Praxis ist jedoch zu beobachten, dass, wenn die Datenanalyse nicht durch die Strafverfolgungsbehörden selbst (also keinen internen Sachverständigen) erfolgt, i. d. R. zwar das Gutachten, nicht jedoch die Arbeitsunterlagen Bestandteil der Akte sind.

Befinden sich die Arbeitsunterlagen des IT-Sachverständigen nicht bei den Akten und werden sie auch nicht durch das Tatgericht im Rahmen von Nachermittlungen dem Prozessstoff hinzugefügt, stellt sich die Frage wie Verteidigerin und Beschuldigte an die Arbeitsunterlagen gelangen.

Diesbezüglich stößt man in der Kommentarliteratur auf den pauschalen Hinweis „Arbeitsunterlagen eines Sachverständigen unterliegen der Akteneinsicht grundsätzlich nicht; maßgeblich ist die Aufklärungspflicht im Einzelfall“.[866] Die bisherige Rspr. des BGH billigte der Beschuldigten diesbezüglich zwar einen neben dem Akteneinsichtsrecht bestehenden Anspruch auf Einsicht der Sachverständigenunterlagen zu, allerdings wurde dieser auf die wesentlichen und tragenden Ergebnisse beschränkt,[867] ein umfassendes Einsichtsrecht wurde abgelehnt.[868] Mindestens musste die Einsichtnahme jedoch dem Maßstab der gerichtlichen Aufklärungspflicht aus § 244 Abs. 2 StPO genü-

---

[864] Zur Unterscheidung zwischen Aktenbestandteil und Beweisstück vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 703 f.: Die Unterscheidung zwischen Aktenbestandteilen i. S. v. § 147 Abs. 1 Var. 1 StPO und sog. Beweisstücken i. S. v. § 147 Abs. 1 Var. 2 StPO entscheidet darüber, ob die Beweisdaten und die Informationen über die Datenbearbeitungsmethoden dem *Einsichtsrecht* und damit einem Zurverfügungstellen der Akte zum Download oder (nur) dem *Besichtigungsrecht* in den Örtlichkeiten der Strafverfolgungsbehörden unterfallen.

[865] Im Rahmen des formellen Aktenbegriffs sind die Beweisdaten, Ergebnisse des Datenbearbeitungsvorgangs und die dazu gehörigen Informationen erfasst, weil sie zur Klärung der Zuverlässigkeit/Richtigkeitswahrscheinlichkeit der Methode bzw. Sicherung der Integrität und Authentizität der Beweisdaten als Beweismittel in der Hauptverhandlung verwendet werden sollen oder alternativ für die Bejahung des Tatverdachts für eine Ermittlungsmaßnahme herangezogen werden. Dementsprechend sind auch die hierfür notwendigen Informationen dem Gericht vorzulegen und damit Bestandteil der Akten. Eine gegenteilige Entscheidung der Staatsanwaltschaft wäre – im Rahmen des formellen Aktenbegriffs – ermessensfehlerhaft, da auch der formelle Aktenbegriff der Staatsanwaltschaft nicht das Recht einräumt, willkürlich Informationen und Beweismittel, welche für die Hauptverhandlung relevant sind, dem Gericht und der Verteidigung vorzuenthalten. A. A. *Mysegades*, Software als Beweiswerkzeug, S. 157: Der Einsichtsanspruch beruht nicht auf dem Akteneinsichtsrecht gemäß § 147 StPO, weil die Untersuchungsunterlagen des Sachverständigen keine Akten des Gerichts darstellen.

[866] Vgl. KK/*Willnow*, § 147 Rn. 8 (9. Auflage 2023); MüKo-StPO/*Kämpfer/Travers*, § 147 Rn. 22 (2. Auflage 2023); Meyer-Goßner/*Schmitt* § 147 Rn. 18b; vgl. BGH 14.7.1995 – 3 StR 355/94, StV 1995, 565; *Lehmann*, GA 2005, 639; jew. m. w. N.

[867] BGH NJW 1999, 2746 (2750 f.).

[868] Vgl. BGH BeckRS 1995, 8836.

gen.[869] Wenn der BGH auch kein Recht der Verteidigung zur Gegenkontrolle anerkennt, stimmt er doch der Auffassung zu, dass sich aus der Aufklärungspflicht eine Notwendigkeit ergeben kann, Unterlagen zugänglich zu machen, sofern dies erforderlich ist, damit die Prozessbeteiligten durch Beweisermittlungs- und Beweisanträge den Umfang der Untersuchung nach § 244 Abs. 2 StPO mitbestimmen können[870] und „die der Beantwortung der jeweiligen Beweisfrage dienenden Gedankengänge nach Möglichkeit von allen Verfahrensbeteiligten nachvollzogen werden können."[871] Zu diesem Zwecke muss rechtliches Gehör i. S. d. Art. 103 Abs. 1 GG gewährt werden, indem die Angeklagte bzw. ihre Verteidigerin Gelegenheit erhält, alle maßgeblichen Tatsachen und Beweisergebnisse kennenzulernen.[872] Maßgeblich sollen dabei die Tatsachen sein, die für die gerichtliche Urteilsfindung i. S. d. § 261 StPO von Bedeutung sind.[873]

Hält die Tatrichterin danach die Kenntnisnahme oder Einsicht in die Unterlagen (wie etwa im Fall der Bedienungsanleitung eines verwendeten standardisierten Messverfahrens)[874] für ihre Überzeugungsbildung nicht für notwendig, weil das Beweismittel für den ordnungsgemäßen Aufbau des konkreten Messgeräts der Messbeamte ist, der die angegriffene Messung vorgenommen hat und das Tatgericht seine Überzeugungsbildung alleine auf dessen Zeugenaussage stützt, muss sie die Bedienungsanleitung auch nicht beiziehen, wenn sich aus der Aussage keine begründeten Zweifel ergeben, die die Beiziehung zu Beweiszwecken notwendig erscheinen lassen. In einigen häufig vor Gericht auftretenden Fällen, z. B. die Berechnung der BAK zur Tatzeit durch Gerichtsmediziner oder von Bremswegen und Geschwindigkeiten durch einen technischen Sachverständigen, kennt eine erfahrene Richterin die zugrundeliegenden Erfahrungssätze und wird daher regelmäßig nicht von schriftlichen

---

869 BGH StV 1989, 141, 1995, 565 (566); ähnlich auch die Situation in BGHSt 30, 131; BVerfGE 63, 45; *Eisenberg*, Beweisrecht der StPO, Rn. 1582a; Löwe/Rosenberg/*Lüderssen*, § 147 Rn. 173; *Sarstedt/Hamm*, Revision, Rn. 1026; so auch *Mysegades*, Software als Beweiswerkzeug, S. 156 f.

870 BGHSt 30, 131 (140 f.).

871 BGH StV 1989, 141. Hier formulierte der BGH präzise, aber zu wenig beschränkende Voraussetzungen für einen Anspruch auf Einsicht in Unterlagen.

872 BGHSt 30, 131 (141); der *Wasserburg*, NJW 1980, 2440 (2442) folgt.

873 BGHSt 30, 131 (141); Das BVerfG bestätigt, Art. 103 Abs. 1 GG wolle nur „verhindern, dass das Gericht ihm bekannte, dem Beschuldigten aber verschlossene Sachverhalte zu dessen Nachteil verwertet", BVerfGE 63, 45 (59). So bspw. auch der BGH in seinen Entscheidungen BGH StV 1989, 141; dazu auch eingehend *Hartmann/Rubach*, StV 1990, 425.

874 Vgl. OLG Frankfurt a. M., Beschluss vom 12.4.2013 – 2 Ss-OWi 173/13, v. a. unter Beachtung der Vereinfachung des Verfahrensganges in Bußgeldsachen im Gegensatz zu einem Strafverfahren.

Ausführungen des Sachverständigen Kenntnis nehmen müssen, um zu erfahren, welche generelle Oberprämisse die Ergebnisse stützt.

Hält die Tatrichterin dagegen die Einsicht in die Arbeitsunterlagen der Sachverständigen (wie etwa die Funktionsbeschreibung einer experimentellen sachverständigen Methode) für ihre Überzeugungsbildung für notwendig und macht damit ihre Überzeugungsbildung von der Kenntnis des Inhalts dieser Unterlagen abhängig, dann muss sie diese ordnungsgemäß als Beweismittel in das Verfahren einbringen, damit sie sie in ihrer Beweiswürdigung verwenden kann. Ähnlich fällt eine Beurteilung aus, wenn die Verteidigung z. B. signifikante Anhaltspunkte für einen Berechnungsfehler darlegen kann.[875] Wenn das Gericht die Berechnungen durch einen Sachverständigen ausführen lässt, so zeigt sich daran, dass es sich selbst für nicht hinreichend zuverlässig hält, um diese Aufgabe selbst zu bewältigen. Im Regelfall wird es dann auch nicht in der Lage sein, Fehler ohne Blick in das schriftliche Gutachten zu erkennen. In diesen Fällen ist das Gericht verpflichtet auch den übrigen Prozessbeteiligten den Blick in die schriftlichen Unterlagen zu ermöglichen. Das gilt v. a. für die wissenschaftlichen Methodiken und Erfahrungssätze, die nicht standardisiert und im Wege des gesicherten Erfahrungswissens Eingang in ein Strafverfahren finden.

Die Durchsetzung des Anspruchs auf Einsichtnahme musste nach der bisherigen Systematik des BGH über einen entsprechenden Beweisantrag erfolgen, weil der BGH vorrangig das Tatgericht in der Pflicht sah, die entsprechenden Tatsachen nach dem Maßstab des § 244 Abs. 2 StPO aufzuklären.[876] Daran war misslich, dass ein solcher Antrag erst in der Hauptverhandlung gestellt werden kann, jedoch bereits im Ermittlungsverfahren ein erhebliches Interesse an der Überprüfung der Gutachten der dort beauftragten externen IT-Sachverständigen gegeben sein kann.[877]

Um die Frage von oben wieder aufzugreifen, führt Rückert zutreffend aus, dass Verteidigerin und Angeklagte jedenfalls über das zusätzliche Informationsrecht, dass das BVerfG aus dem Recht auf ein faires Verfahren und aus der prozessualen Waffengleichheit ableitet, an die Arbeitsunterlagen gelangen.[878] So hat das BVerfG kürzlich in zwei (Kammer-)Entscheidungen zu au-

---

875 So verlangt *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 351 für die Entscheidung über die Einsicht in Unterlagen die Zugrundelegung des Konzepts des relevanten Zweifels, bspw. signifikante Anhaltspunkte für die Vertauschung von Blutproben.

876 BGH BeckRS 1995, 8836.

877 Überblick zu den bisherigen Lösungsmodellen dieses Problems: *Mysegades*, Software als Beweiswerkzeug, S. 157 f. m. w. N.

878 Siehe *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 719 f.; *Mysegades*, Software als Beweiswerkzeug, S. 156 ff. m. w. N.

tomatischen Geschwindigkeitsmessungen aus dem Akteneinsichtsrecht nach §§ 147, 32f StPO und dem daneben bestehenden, aus dem Recht auf ein faires Verfahren in seiner Ausprägung der prozessualen Waffengleichheit abgeleiteten, unmittelbar verfassungsrechtlichen Informationsrecht des Beschuldigten ein umfangreiches Recht des Verteidigers und des unverteidigten Beschuldigten auf Einsichtnahme entwickelt.[879] Rückert begründet eine Übertragung der Rechtsprechung für den Bereich der forensischen Informatik insbesondere damit, dass sich angesichts der mangelnden Standardisierung der Untersuchungsmethoden in diesem Bereich (siehe dazu v. a. im 4. Teil, A. III. 4. b) cc) (2)) die gerichtliche Aufklärungspflicht regelmäßig auf die Beweisdaten und die Funktionalität bzw. oft sogar auf den Quellcode der verwendeten Datenverarbeitungs- und -analysemethoden bezieht. So wird es regelmäßig notwendig sein den Quellcode gerade von bisher dem Gericht unbekannten Datenanalyse- und -verarbeitungsprogrammen zu untersuchen, um die Verlässlichkeit des Programms prüfen und die Ergebnisse in die richtige Kategorie der Erfahrungssätze einordnen zu können (vgl. hierzu die Zuverlässigkeitsskala im Rahmen der Beweiswürdigung, Vierter Teil, A. III. 4. b) cc) (3)).[880] Überzeugend kommt Rückert zu dem Ergebnis, dass diese Arbeitsunterlagen des IT-Sachverständigen bereits zum Tatsachenstoff der Hauptverhandlung gemacht werden müssen und dass sie sowohl nach dem funktionalen und materiellen Aktenbegriff eigentlich bereits als Aktenbestandteile zu den Akten genommen werden müssen und damit dem Einsichtsrecht unterfallen; andernfalls aber zumindest als verfahrensrelevante Informationen unter den vom BVerfG formulierten unmittelbar verfassungsrechtlichen Anspruch (unter Beachtung Grenzen des Anspruchs[881]) fallen.[882]

In Bezug auf das vorbereitende IT-Sachverständigengutachten und die Arbeitsunterlagen heißt das, dass den Einsichtsberechtigten regelmäßig eine Kopie der verarbeiteten Beweisdaten zur Verfügung zu stellen ist. Bzgl. verwendeter Tools sind nicht nur detaillierte Informationen über dieses und die verwendete Version im Rahmen der Akteneinsicht zu gewähren[883], sondern

---

879 BVerfG NJW 2021, 455; sowie dem folgend BVerfG BeckRS 2021, 10578, BeckRS 2021, 10638 und BeckRS 2021, 10577.

880 Siehe hierzu auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 675 ff.

881 Zu Einschränkungen und Art und Weise der Informationsgewährung bzw. Einsichtnahme vgl. Rückert, Digitale Daten als Beweismittel im Strafverfahren, S. 722 ff.

882 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 698 ff. m. w. N.

883 Bei kommerziellen Werkzeugen etwa Hersteller, Bezeichnung, Versionsnummer, Funktionsbeschreibungen und Anleitungen – sind diese Aktenbestandteil, vgl. SK-StPO/*Weißlau/Deiters*, § 483 Rn. 9. Sollte der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz („AI Act“) umgesetzt werden, würden künftig auch die dort vor-

auch Zugang zum Programm selbst zu ermöglichen.[884] Kann eine Programmkopie zur Verfügung gestellt werden, ist dem Verteidiger eine solche zu übergeben.[885] Ist eine Überlassung aus tatsächlichen Gründen unmöglich (etwa weil technische Kopierschutzmaßnahmen bestehen oder eine Plattformlösung vorliegt), muss dem Verteidiger Zugang zum Originalprogramm in den Räumlichkeiten der Strafverfolgungsbehörden gewährt werden, um entsprechende Funktionalitätstests durchzuführen.[886] Sollten sich Verteidiger und Beschuldigter dafür entscheiden, selbst eine Version des Programms anzuschaffen, um entsprechende Tests durchzuführen, Fehlerquellen aufzudecken und entsprechende Beweisanträge vorzubereiten, zählen die Anschaffungskosten zumindest dann zu den notwendigen Auslagen i. S. v. § 464a Abs. 2 Nr. 2 StPO, wenn der Zugang zum Programm der Strafverfolgungsbehörden nicht bzw. nicht in ausreichendem zeitlichen Umfang gewährt wird oder ein solcher Zugang (z. B. aufgrund des großen Umfangs der durchzuführenden Tests) für eine effektive Verteidigung nicht ausreichend ist.

Wenn Unterlagen/Materialien nicht zugänglich bzw. nicht mehr vorhanden sind, kann es sein, dass die Gerichte den Gutachten einen geringeren Beweiswert beimessen bzw. einen weiteren Sachverständigen bestellen müssen.[887] Weigert sich der Sachverständige, die Unterlagen offenzulegen, muss das Gericht das in der Beweiswürdigung berücksichtigen. Bestehen ohne die Offenlegung keine hinreichenden Prüfungsrechte des Beschuldigten muss das Tatgericht das Gutachten sogar als nicht verwertbar betrachten.[888]

cc) Fazit

Insgesamt lässt sich festhalten, dass das Gericht in den meisten Fällen ein erhebliches Risiko eingeht in Bezug auf die Revisibilität des Urteils, wenn es kein vorbereitendes schriftliches Gutachten anfertigen lässt und dieses den Verfahrensbeteiligten in angemessener Zeit vor der mündlichen Verhandlung

---

gesehenen technischen Dokumentationen (Art. 11 i. V. m. Anhang IV), die Aufzeichnungen zur bisherigen Funktionalität der KI (Art. 12) und Gebrauchsanweisungen, inklusive Angaben über Genauigkeitswerte, Trainingsdaten und Fehlerquellen (Art. 13 Abs. 2) zu diesen Informationen zählen, welche in die Akte aufgenommen werden müssen, vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 705.

884 Vertiefend dazu *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 718 ff., S. 797.

885 Rechtlich steht dem auch das Urheberrecht nicht entgegen, da § 45 UrhG die Vervielfältigung von Computerprogrammen zu Beweiszwecken in gerichtlichen Verfahren erlaubt.

886 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 574.

887 BGH StV 1989, 141.

888 *Mysegades*, Software als Beweiswerkzeug, S. 158 m. w. N.

zugänglich macht – auch und v. a. in Bezug auf zugrundeliegende Arbeitsunterlagen.[889]

Rückert folgend sind demnach auch die den Gutachten zugrundeliegenden Arbeitsunterlagen wie Beweisdaten (bzw. ihre Kopien) und Informationen über die Datenverarbeitungs- und -analysemethoden grds. unter den formellen und materiellen Aktenbegriff zu fassen und damit als „Aktenbestandteile" zu führen. Werden sie das nicht, erstreckt sich weiterin der vom BVerfG formulierte unmittelbar verfassungsrechtliche Anspruch auf Einsicht in die Arbeitsunterlagen der IT-Sachverständigen, da es sich um verfahrensrelevante Informationen i. S. d. § 244 Abs. 2 StPO handelt. Demnach sind stets eine Kopie der verarbeiteten Beweisdaten sowie detaillierte Informationen zu den verwendeten Datenverarbeitungs- und -analyseprogrammen und den daraus gezogenen sachverständigen Schlussfolgerungen zur Verfügung zu stellen und auch einen Zugang zum Programm selbst zu ermöglichen. Nur durch Transparenz und Zugang zu den verarbeiteten Daten sowie detaillierte Kenntnis über die verwendeten Datenverarbeitungs- und -analyseverfahren kann nachvollzogen werden, wie die gegen den Beschuldigten verwendeten Beweismittel zustande kommen und ob und ggf. inwieweit diese verlässlich sind. Das gewährleistet die Basis für eine angemessene Cyber-Strafverteidigung.

c) Die Ablehnung des IT-Sachverständigen

Auch in diesem Kapitel zu verorten ist das Ablehnungsrecht, um möglichen Mängeln an der Objektivität des Sachverständigen begegnen zu können. Die Gefahr der fehlenden Objektivität liegt darin begründet, dass ein entsprechender Mangel fehlerhafte gerichtliche Abwägungen und Entscheidungen herbeiführen kann.[890] Schon bei der Auswahl nach § 73 Abs. 1 StPO hat das Gericht als Auftraggeber zweckmäßigerweise Zweifel an der Eignung des Sachverständigen ernst zu nehmen und zu prüfen, ob ggf. ein anderer zu beauftragen ist (vgl. auch B. II. 2. c)). Wurde der Sachverständige jedoch bestellt, so kann

---

[889] So auch *Mysegades*, Software als Beweiswerkzeug, S. 158, der ausführt, dass Tatgerichte sicherstellen müssen, dass eine hinreichende kritische Prüfung der sachverständigen Methodik durch eine Expertin möglich sein muss und eine entsprechende ernsthafte wissenschaftliche Untersuchung der Methodik des Sachverständigen eine vollständige Offenlegung aller Untersuchungsunterlagen voraussetzt; Vgl. auch *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 115; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 354 f. Damit ist die Lage nicht weit von der Partikulargesetzgebung im 19. Jahrhundert entfernt, von denen noch *Strippelmann* 1858 feststellt, dass Gutachten grundsätzlich schriftlich zu erstellen waren, vgl. *Strippelmann*, Die Sachverständigen im gerichtlichen und außergerichtlichen Verfahren, S. 237 f.

[890] *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 248.

sein Tätigwerden nicht mehr mit einem bloßen Hinweis auf Zweifel an der Sachkunde verhindert werden.[891] Diesbezüglich verweist das Gesetz in § 74 Abs. 1 S. 1 StPO auf die Ausschließungs- und Ablehnungsgründen für Richter[892] in §§ 22, 24 StPO (mit Ausnahme des § 22 Nr. 5 StPO, vgl. § 74 Abs. 1 S. 2 StPO).[893] So kann ein Sachverständiger aus denselben Gründen abgelehnt werden wie ein Richter, also insbesondere wegen der Besorgnis der Befangenheit (§ 24 StPO) oder dem Vorliegen eines Ablehnungsgrundes gem. § 22 StPO. Allerdings begründen die für den Richter geltenden Ausschließungsgründe für den Sachverständigen lediglich einen Ablehnungsgrund in Form einer Beweiseinrede, §§ 74 Abs. 1 S. 1, 24 Abs. 1, 2 StPO.[894] Das Fehlen von Ausschließungstatbeständen ist damit zu erklären, dass dem Richter hier ein neutrales Urteil zuzutrauen ist, im Gegensatz zu dem Fall, in dem er sich selbst bzw. eine Gerichtsperson beurteilen müsste.[895] Allerdings sieht die StPO keine Selbstanzeige, wie in § 30 StPO für Richter, vor. Wenn sich der Sachverständige in seiner Objektivität in einer Weise beeinträchtigt glaubt, dass die Voraussetzungen des § 74 StPO (i. V. m. §§ 24, 22 StPO) erfüllt wären, wird eine Mitteilungspflicht an das Gericht aus der Pflicht zur Objektivität abgeleitet, vgl. § 79 Abs. 2 StPO. Das Gericht kann den Sachverständigen

---

891 Vgl. BGH bei *Kusch*, NStZ 1994, 228.

892 Hier wird der Unterschied zum Zeugenbeweis deutlich, bei dem das Gesetz kein Ablehnungsrecht vorsieht, da es auf dessen Unparteilichkeit nicht ankommt. Die Orientierung des Gesetzes in § 74 Abs. 1 S. 1 StPO an den Ablehnungsgründen für Richter in §§ 22, 24 StPO ergibt sich daraus, dass der Sachverständige dem Richter näher steht als bspw. dem Zeugen, denn er bereitet die Überzeugungsbildung durch Nennung möglicher anwendbarer Erfahrungssätze und Schlussfolgerungen vor. Der Bezug zur Richterablehnung beruht auch auf der historischen Entwicklung des Sachverständigenbeweises in Zusammenhang mit dem richterlichen Augenschein, vgl. auch SK-StPO/*Rogall*, § 74 Rn. 1 ff.; *Stinshoff*, Operative Fallanalyse, S. 91 ff.

893 Beispiele für Ablehnungsgründe vgl. z. B. KMR/*Neubeck*, § 74 Rn. 10 ff.; KK/*Senge*, § 74 Rn. 5 f. Vertiefend zu dem Ablehnungsrecht aus § 74 Abs. 1 S. 1 StPO i. V. m. § 22 Nr. 4 Var. 1 und 2 StPO siehe auch *Stinshoff*, Operative Fallanalyse, S. 137 f.; *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 115 ff.; *Pawlak*, Ablehnung des Sachverständigen, S. 180 ff. In Bezug auf den Richter wird die Forderung der Objektivität dem Grundsatz des gesetzlichen Richters aus Art. 101 Abs. 1 S. 2 GG zugeordnet, der u. a. gewährleisten soll, dass der Rechtssuchende nicht vor einem Richter steht, der die gebotene Neutralität und Distanz vermissen lässt, vgl. BVerfGE 21, 139 (146); Meyer-Goßner/Kleinknecht, Vor § 22 Rn. 1; Löwe/Rosenberg/*Wendisch*, Vor § 22 Rn. 1.

894 Eine Ausnahme findet sich in § 87 Abs. 2 S. 3 StPO, wonach dem letztbehandelnden Arzt nicht die Leichenöffnung übertragen werden darf, vgl. Meyer-Goßner/*Schmitt*, § 87 Rn. 19; a. A. KK/*Senge*, § 87 Rn. 5; Löwe/Rosenberg/*Krause*, § 87 Rn. 22; vgl. dazu auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 249; vgl. auch *Pawlak*, Ablehnung des Sachverständigen, S. 255 ff.: Er plädiert de lege ferenda für die Abschaffung des § 74 StPO, der historisch durch die Vorstellung eines Richtergehilfen bedingt ist, welcher selbst Richteraufgaben wahrnimmt.

895 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 249.

dann gem. § 76 Abs. 1 S. 2 StPO von seiner Verpflichtung zur Gutachtenerstattung entbinden.[896]

Bedenken kommen, neben den gängigen (auch aus anderen bekannten Konstellationen mit persönlichen Beweismitteln[897]), v. a. dann auf, wenn IT-Sachverständige schon im Ermittlungsverfahren von der Staatsanwaltschaft beauftragt werden und dann in das Hauptverfahren übernommen werden.[898] Das Problem verfestigt sich, wenn zudem IT-Sachverständige bestellt werden, die bei den Strafverfolgungsbehörden angesiedelt sind.[899]

aa) Ablehnungsrecht nach § 74 Abs. 1 S. 1 StPO i. V. m. § 22 Nr. 4 Var. 1 und 2 StPO

Von den Ablehnungsgründen des § 22 StPO dürfte insbesondere § 22 Nr. 4 StPO relevant sein. Danach kann als Sachverständiger abgelehnt werden, wer „(…) als Beamter der Staatsanwaltschaft, [oder] als Polizeibeamter (…) tätig gewesen ist".

Es stellt sich die Frage, wann ein Ablehnungsrecht gegenüber Mitgliedern einer Strafverfolgungsbehörde begründet ist.

Nach der Rspr. des BGH und der h. M. kann die reine Zugehörigkeit zu einer Strafverfolgungsbehörde die Ablehnung einer Person als Sachverständiger gem. § 74 Abs. 1 S. 1 StPO i. V. m. § 22 Nr. 4 Var. 1 und 2 StPO nicht begründen. Das gilt sowohl für organisatorisch von den Strafverfolgungsbehörden getrennte Dienststellen der Polizei[900] als auch für dort angesiedelte IT-Foren-

---

896 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 361 f.

897 Es kann auch private, emotionale oder berufliche Verflechtungen geben, die eine Befangenheit begründen, z. B. wenn ein IT-Fachmann Daten sammelt und beurteilt über ein Finanzunternehmen, bei dem er kürzlich Geld bei Spekulationen verloren hat oder wenn er in einem Missbrauchsfall recherchiert und selbst oder ein Familienmitglied Opfer (auch in einem anderen Fall) war; siehe zu Einzelfällen auch MüKo-StPO/*Trück*, § 74, Rn. 12 ff.

898 Vgl. dazu auch *Wolf*, ZWH 2012, 125 (128 ff.).

899 So liegt auch der Fokus des EGMR auf der Prüfung von Sachverständigengutachten, wenn die Sachverständigen nach den Umständen des Einzelfalls möglicherweise nicht neutral erscheinen, sondern im Dienste des Staates als Prozessgegner stehen oder sogar die Ermittlungen erst ausgelöst haben, vgl. EGMR, Urteil v. 06.05.1985 – Bönisch v. Austria, 8658/79, Rn. 32; EGMR, Urteil v. 05.04.2007 – Stoimenov v. Macedonia, 17995/02, Rn. 40, Rn. 42; vgl. auch EGMR, Urteil v. 03.05.2016 – Letincic v. Croatia, 7183/11 = NJOZ 2018, 472, Rn. 51, 61; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 339 f.; *Mysegades*, Software als Beweiswerkzeug, S. 162 f.

900 RGSt 35, 319, 320; KK/*Senge*, § 74 Rn. 2; Löwe/Rosenberg/*Krause*, § 74 Rn. 8 m. w. N.; BeckOK-StPO/*Monka*, § 74 Rn. 1a; SK-StPO/*Rogall*, § 74 Rn. 21 mit Fn. 81,

siker.[901] Das ergibt sich auch aus § 76 Abs. 2 StPO.[902] Auch für Sachverständige, die der Staatsanwaltschaft zugeordnet sind, besteht kein zwingender Ausschließungsgrund aufgrund der bloßen Zugehörigkeit.[903]

Die Beurteilung der Tätigkeit i. S. d. § 22 Nr. 4 StPO richtet sich vielmehr nach der Funktion, in der die Beweisperson im Ermittlungsverfahren herangezogen wurde.[904] Denn für eine Ablehnung bedarf es vielmehr der eigenen Teilnahme an den konkreten Ermittlungen[905] in Form von strafverfolgender „Parteitätigkeit".[906] Diese ist nach der Rspr. gegeben, wenn der Sachverständige „(…) bei der Ermittlung nicht bloß beratend tätig gewesen ist, sondern vor allem sicherheitspolizeiliche Aufgaben wahrgenommen hat (…)"[907]. Abgelehnt kann der Sachverständige somit dann werden, wenn er gemäß § 161 Abs. 1 StPO entweder im Auftrag oder auf Ersuchen der Staatsanwaltschaft Ermittlungen vorgenommen hat und dabei Art, Umfang und/oder Richtung der Ermittlungen bestimmt hat,[908] gem. § 163 Abs. 1 StPO Straftaten erforscht oder Maßnahmen getroffen hat, die keinen Aufschub gestatten, um die Verdunkelung der Sache zu verhüten oder als Ermittlungsperson der Staatsanwaltschaft i. S. d. § 152 Abs. 1 GVG tätig geworden ist und den Anordnungen der Staatsanwaltschaft Folge geleistet hat.[909] Wenn die Gutachten dagegen unabhängig und weisungsfrei erstellt wurden, ist kein Ausschlussgrund gegeben.[910]

23, 25; *Schlüchter*, Rn. 528; *Ahlf*, MDR 1978, 981, 982; *Gössel*, DRiZ 1980, 371; *Kube/Leineweber*, S. 101 f.; *Wiegmann*, StV 1996, 570, 573.

901 „Dortige EDV-Sachverständige", vgl. *Etter*, CR 1986, 166 (173); *Paul*, CR 1986, 173 (174 f.); MüKo-StPO/*Trück*, § 74 Rn. 6.

902 LG Stuttgart 10.6.1997 – 10 Qs 36/97, NStZ-RR 1998, 54 (55); MüKo-StPO/*Trück*, § 74 Rn. 6.

903 MüKo-StPO/*Trück*, § 74 Rn. 6; BGH 12.7.1955 – 5 StR 109/55, JurionRS 1955, 11761.

904 SK-StPO/*Rogall*, § 74 Rn. 19; MüKo-StPO/*Trück*, § 74 Rn. 6.

905 KK/*Scheuten*, § 22 Rn. 12.

906 SK-StPO/*Rogall*, § 74 Rn. 18; MüKo-StPO/*Trück*, § 74 Rn. 6; BGH 11.1.1963 – 3 StR 52/62, BGHSt 18, 214; RG 30.4.1888 – Rep. 777/88, RGSt 17, 415 (424); 8.7.1902 – Rep. 811/02, 319 (320); Foth/Karcher NStZ 1989, 166 (168); *Wiegmann*, StV 1996, 570 (572) mit Aufzählung von Beispielen.

907 BGHSt 18, 214, 217; vgl. auch BGH NStZ 2008, 50.

908 *Wiegmann*, StV 1996, 570, 572 f.; *Lemme*, wistra 2002, 281, 286.

909 *Wiegmann*, StV 1996, 570, 572; *Eb. Schmidt*, II, § 74 Rn. 9; SK-StPO/*Rogall*, § 74 Rn. 20; Löwe/Rosenberg/*Krause*, § 74 Rn. 7; KK/*Senge*, § 74 Rn. 2; Meyer-Goßner/*Schmitt*, § 74 Rn. 3; *Nix*, Kriminalistik 1994, 83, 85; vgl. auch *Kube/Leineweber*, Polizeibeamte als Zeugen und Sachverständige, S. 109.

910 LG Zweibrücken JW 1979, 1995; Gössel, DRiZ 1980, 363, 371; Löwe/Rosenberg/*Krause*, § 74 Rn. 7, 14; SK-StPO/*Rogall*, § 74 Rn. 23; Meyer-Goßner/*Schmitt*, § 22 Rn. 14; *Rüping*, Das Strafverfahren, Rn. 191; *Lemme*, wistra 2002, 281 (284 ff.); a. A. *Dose*, NJW 1978, 349, 354.

Die bloße Tätigkeit für die Staatsanwaltschaft soll aber jedenfalls nicht ausreichen.[911]

Ob ein Ablehnungsgrund besteht, ist demnach im Einzelfall zu entscheiden, ob sie selbst an Ermittlungshandlungen mitwirken[912] oder aufgrund der organisatorischen Gegebenheiten und der Art ihrer Heranziehung in der Lage sind, ihr Gutachten eigenverantwortlich, frei von Beeinflussung und losgelöst von der eigentlichen Ermittlungstätigkeit zu erstatten.[913] Soweit jedenfalls die „rechtliche Bewertung der festgestellten Tatsachen (…) allein der Staatsanwaltschaft" obliegt und „die Tatsachenaufbereitung (…) die Staatsanwaltschaft in die Lage" versetzt zu entscheiden, „ob das Verfahren fortgeführt werden soll und inwiefern weitere Ermittlungsmaßnahmen notwendig seien", kommen keine Zweifel an der Objektivität auf. Es dürfen keine ermittlungsrelevanten Entscheidungen vorweggenommen worden sein durch den Sachverständigen. Die Hoheit über den Fortgang der Ermittlungen muss in den Händen der hierfür von der Strafprozessordnung bestimmten Strafverfolgungsbehörden liegen.[914] Wer aber zunächst als Ermittlungsgehilfe aktiv an den Ermittlungen teilgenommen hat und dabei nicht bloß beratend tätig geworden ist, sondern an der Aufklärung von Straftaten und der Überführung der Verdächtigen beteiligt war[915] bzw. besorgen lässt, am Ausgang des Strafverfahrens ein Interesse zu haben,[916] kann in diesem Verfahren kein Sachverständiger mehr sein.[917]

---

911 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 254, 337 ff.

912 *Bittmann*, wistra 2011, 47 (51 ff.); *Dose*, NJW 1978, 349 (354); *Wiegmann*, StV 1996, 570 (574).

913 KMR/*Neubeck*, § 74, Rn. 8; SK-StPO/*Rogall*, § 74, Rn. 24; *Lemme*, wistra 2002, 281 (284 ff.); *Wolf*, ZWH 2012, 125 (127 f.); vgl. auch BGH 10.4.1979 – 4 StR 127/79, BGHSt 28, 381 (384) zur Verjährungsunterbrechung und OLG Koblenz 4.12.1997 – 1 Ws 719/97, NStZ-RR 1998, 127 (128) zu § 464a.

914 Vgl. BVerfG, Beschl. v. 31.8.2007 – 2 BvR 1681/07.

915 Nur etwa BGH v. 11.1.1963 – 3 StR 52/62, NJW 1963, 821.

916 LG Kiel v. 14.8.2006 – 37 Qs 54/06, CR 2007, 116 = NJW 2006, 3224.

917 Zwar hat die Rechtsprechung in BGH v. 2.7.1986 – 3 StR 87/86, MDR 1986, 976 = StV 1986, 465 entschieden, dass selbst wer in die sonstige Ermittlungstätigkeit des gegen den Angeklagten laufenden Verfahrens eingebunden war, ein Gutachten erstatten kann, wenn er nur eigenverantwortlich und frei von jeder Beeinflussung, losgelöst von seiner bisherigen (und zukünftigen) eigentlichen Ermittlungstätigkeit beauftragt worden ist. In dieser Entscheidung ging es jedoch nur um die Frage der Verjährungsunterbrechung, ob also eine Beauftragung als Sachverständiger vorlag oder nicht, und nicht um dessen Befangenheit, vgl. *Lemme*, wistra 2002, 281 (Fn.105); zur Vorsicht ratend auch *Bittmann*, wistra 2011, 47.

bb) Ablehnungsrecht nach § 74 Abs. 1 S. 1 StPO i. V. m. § 24 StPO

Daneben ist im Zusammenhang mit der Vernehmung von polizeilichen Cyberkriminalisten oder bei der Staatsanwaltschaft angesiedelten IT-Forensikern als IT-Sachverständige, die zudem bereits im Ermittlungsverfahren von der Staatsanwaltschaft hinzugezogen werden, auch der Ablehnungsgrund wegen Besorgnis der Befangenheit nach § 74 Abs. 1 S. 1 StPO i. V. m. § 24 StPO denkbar. Die Besorgnis der Befangenheit liegt vor, wenn vom subjektiven Standpunkt des Ablehnenden aus verständlichen Gesichtspunkten Misstrauen in die Unparteilichkeit des Sachverständigen gerechtfertigt erscheint.[918]

So stellt sich die Frage der Ablehnungsmöglichkeit aufgrund der Nähe zu den Ermittlungen. Auf Seiten des Angeklagten kann der Eindruck entstehen, dass ein gewisses Verfolgungsinteresse des Sachverständigen besteht.[919] Soweit allerdings eine Ablehnung wegen § 74 Abs. 1 S. 1 StPO i. V. m. § 22 Nr. 4 Var. 1 und 2 StPO nach den oben gemachten Ausführungen nicht in Betracht kommt, kann ohne das Hinzutreten weiterer Umstände eine Ablehnung nicht begründet werden.[920] Grundsätzlich kann von einem Überführungseifer jedenfalls dann nicht – ohne weitere Anhaltspunkte[921] – ausgegangen werden, wenn der Mitarbeiter organisatorisch getrennt von der ermittelnden Dienststelle untergebracht ist.[922] Die dienstrechtliche und räumliche Eingliederung in die Strafverfolgungsbehörde stellt für sich allein betrachtet nach h. M. aber auch noch keinen Ablehnungsgrund dar, wenn die Person ihr Gutachten eigenverantwortlich und weisungsfrei erstattet hat.[923]

Die Teilnahme an Ermittlungshandlungen (siehe dazu B. III. 2. b)) bewirkt nicht schon per se die Befangenheit des Sachverständigen, was sich in syste-

---

[918] BGH JZ 1996, 315, 316; *Lemme*, wistra 2002, 281, 283; Meyer-Goßner/*Schmitt*, § 24 Rn. 8; KK/*Scheuten*, § 24 Rn. 3a; SK-StPO/*Rogall*, § 74 Rn. 30; *Arzt*, JZ 1969, 438 (440); *Ahlf*, MDR 1978, 981, 982; kritisch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 251 m. w. N.

[919] *Ahlf*, MDR 1978, 981, 982; *Kube/Leineweber*, Polizeibeamte als Zeugen und Sachverständige, S. 104 f.

[920] So auch *Stinshoff*, Operative Fallanalyse, S. 138.

[921] Aus dem Verhalten kann im Einzelfall aber schon auch mal „Jagdfieber" abgelesen werden, der sehr wohl zu einer Ablehnung wegen Befangenheit führen kann, vgl. *Kube/Leineweber*, Polizeibeamte als Zeugen und Sachverständige, S. 111; Löwe/Rosenberg/*Krause*, § 74 Rn. 12.

[922] BGHSt 18, 214, 215 f.; *Ahlf*, MDR 1978, 981, 982; *Kube/Leineweber*, S. 105.

[923] BGH v. 11.1.1963 – 3 StR 53/63, NJW 1963, 821; BGH v. 10.4.1979 – 4 StR 127/79, NJW 1979, 2414; OLG Zweibrücken v. 9.10.1978 – WS 397/78, NJW 1979, 1995; OLG Koblenz v. 16.7.2010 – 1 Ws 189/10, NStZ-RR 2010, 359; KG v. 23.12.2008 – 1 Ws 1/07, NStZ-RR 2009, 190; Meyer-Goßner/*Schmitt*, § 74 Rn. 5 ff.; *Foth/Karcher*, NStZ 1989, 166; hierzu auch *Pause*, NJW 1985, 2576.

matischer Hinsicht bereits aus § 80 StPO ergibt.[924] Vielmehr hat das Gericht das nach seinem Ermessen nach Art und Umfang der Ermittlungen zu beurteilen.[925] Das gilt auch für die Hinzuziehung des Sachverständigen zu einer Durchsuchung bzw. Durchsicht[926], sofern sich die Aufgabenstellung auf eine beratende Tätigkeit beschränkt, z. B. um aus Gründen der Verhältnismäßigkeit die Auswahl sicherzustellender Unterlagen, Datenbestände und EDV-Anlagen einzugrenzen (siehe dazu auch bei B. II. 2. b)).[927] Etwas anderes gilt dann, wenn der hinzugezogene Experte für die Staatsanwaltschaft oder Polizei die Ermittlungshandlungen selbst vornimmt, wie den Ablauf der Durchsuchungsmaßnahme bestimmt.[928] Gleiches soll gelten, wenn ein sachverständiger Übersetzer seine Übertragungen mit Anmerkungen versieht, die eine eigene und einseitige Interpretation erkennen lassen, und er durch seine Vorauswahl die Richtung der Ermittlungen bestimmt.[929]

Es wird deutlich, dass sich die Überlegungen zu den Ablehnungsrechten wegen der Nähe zur Ermittlungstätigkeit mit den Ausführungen zur Abgrenzung zwischen IT-Sachverständigen und Ermittlungspersonen (bzw. sachverständigen Zeugen) überschneiden und deshalb an dieser Stelle nach oben zu B. II. 2. b) und B. III. 2. verwiesen wird.

Die Auftragserteilung durch die Staatsanwaltschaft oder die Polizei führt naturgemäß nicht zur Befangenheit des Sachverständigen, wegen deren Verpflichtung zu neutraler Ermittlung,[930] selbst wenn das eine Beteiligung schon im Ermittlungsverfahren zur Folge hat,[931] sofern die eben beschriebenen Grenzen eingehalten werden. Entsprechend bietet der auf geschäftsmäßige

---

924 *Bittmann*, wistra 2011, 47 (51); *Foth/Karcher*, NStZ 1989, 166 (169) zu §§ 74, 22 Nr. 4.

925 RG 15.5.1931 – 2 D 450/31, JW 1931, 2504 m. Anm. Alsberg.

926 Vertiefend dazu MüKo-StPO/*Hauschild*, § 105 Rn. 35; Vgl. BVerfG 31.8.2007 – 2 BvR 1681/07, BeckRS 2007, 26565; *Wolf*, ZWH 2012, 125 (130 f.).

927 *Etter*, CR 1986, 168 f. für EDV-Sachverständigen; *Lemme*, wistra 2002, 281 (286) für Wirtschaftsreferent; vgl. auch LG Stuttgart 10.6.1997 – 10 Qs 36/97, NStZ-RR 1998, 54 (55) für Steuerfahnder als Sachverständiger für Buchhaltungsfragen bei Nicht-Steuerdelikten.

928 LG Kiel 14.8.2006 – 37 Qs 54/06, NJW 2006, 3224 m. Anm. Wehnert; *Wiegmann*, StV 1996, 570 (573); a. A. für Buchprüfer, der nach § 88 Abs. 2 AO zur Neutralität verspflichtet ist, OLG Bremen 23.10.1998 – VAs 1/98, wistra 1999, 74 (75).

929 *Momsen/Rackow/Schwarze*, NStZ 2018, 625 (626, 629).

930 BGH 11.1.1963 – 3 StR 52/62, BGHSt 18, 214 (215); 23.11.1995 – 1 StR 296/95, NJW 1996, 1355 (1357); OLG Hamm 4.12.1957 – 3 Ss 1494/56, DAR 1957, 131; BayObLG 25.4.1951 – RevReg. Nr. II 81/51, BayObLGSt 1949 – 51, 390 (391); *Artkämper/Artkämper*, Kriminalistik 2018, 384 (387); *Kohlhaas*, NJW 1962, 1329 (1331).

931 BGH 12.7.1955 – 5 StR 109/55, JurionRS 1955, 11761.

Dinge beschränkte Kontakt zur Staatsanwaltschaft keinen Anlass für Zweifel an der Unparteilichkeit der Beweisperson.[932]

Im Falle eines Misstrauens in die Unparteilichkeit kann das Gericht den Sachverständigen auch gem. § 76 Abs. 1 S. 2 StPO entpflichten. Denn fehlendes Vertrauen in die Unparteilichkeit und Unbefangenheit ist von den in der Norm genannten „anderen Gründen" erfasst.[933]

cc) Der abgelehnte Sachverständige

Wird der Sachverständige erfolgreich abgelehnt, ist die Prozesshandlung des Gerichts nicht von Anfang an unwirksam, sondern seine Beauftragung kann lediglich ex nunc entfallen.[934] Er darf dann jedoch nicht mehr als Sachverständiger vernommen werden und ein schon eingereichtes Gutachten nicht mehr verlesen und verwertet werden.[935]

Nach seiner Ablehnung wird regelmäßig ein neuer Sachverständiger bestellt werden müssen (§ 83 Abs. 2 StPO),[936] denn mit der Bestellung eines Sachverständigen bringt der Auftraggeber zum Ausdruck, dass er selbst nicht über die erforderliche Sachkunde verfügt; das gilt dann nicht, wenn das Gericht über die entsprechende Sachkunde verfügt. Das Gericht darf allerdings nicht aus dem Gutachten des abgelehnten Sachverständigen eigene Sachkunde ableiten (Beweisverwertungsverbot).[937] Wird z. B. ein von der Verteidigung benannter Sachverständiger auf Antrag der Staatsanwaltschaft abgelehnt, so kann der Gutachter auch nicht mehr im Weg der Beweismittelpräsentation zum Sachverständigen bestellt werden, vgl. § 245 Abs. 2 StPO.[938]

Allgemein anerkannt ist aber, dass der erfolgreich abgelehnte Sachverständige in demselben Verfahren zu seinen Wahrnehmungen als Zeuge gehört werden kann, soweit er nur über *Zusatztatsachen* aussagt.[939] Grds. ist die Er-

---

932 BGH 20.11.1996 – 2 StR 323/96, wistra 1997, 147 (148).

933 Meyer-Goßner/*Schmitt*, § 76 Rn. 3; KMR/*Neubeck*, § 76 Rn. 4; SK-StPO/*Rogall*, Vor § 72 Rn. 72.

934 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S: 275.

935 Ganz h. M. z. B. BGH NJW 2005, 445, 447; BGH StV 1999, 576; SK-StPO/*Rogall*, Vor § 72 Rn. 77, § 74 Rn. 65; Meyer-Goßner/*Schmitt*, § 74 Rn. 19; Löwe/Rosenberg/*Krause*, § 74 Rn. 34; KK/*Senge*, § 74 Rn. 14; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 250, 276; *Mayer*, in: FS-Mezger, S. 455, 466; *Henkel*, Strafverfahrensrecht, S. 219; *Rüping*, Das Strafverfahren, Rn. 193; *Fezer*, Revision, Rn. 12/28.

936 Meyer-Goßner/*Schmitt*, § 84 Rn. 3.

937 SK-StPO/*Rogall*, § 74 Rn. 65; KK/*Senge*, § 74 Rn. 14. m. w. N.

938 BGH StV 1999, 576.

939 Vgl. nur Meyer-Goßner/*Schmitt*, § 74 Rn. 20; *Fezer*, JR 1990, 397 (400); *Geppert*, DAR 1980, 315, 321; vgl. insb. BGHSt 20, 222 (224): „Das Gesetz beläßt die

stattung des Gutachtens in Bezug auf die *erste* und *zweite Aussagekategorie* im Wege der Vernehmung des Sachverständigen als sachverständigem Zeugen unzulässig.[940] Die Ablehnungsmöglichkeit beruht nämlich darauf, dass das Gericht dem Sachverständigen bzgl. des Zurverfügungstellens von Werkzeugen, mit denen die erforderlichen Schlüsse gezogen werden können, also des Vermittelns von Schlussregeln, und bezüglich der Schlussfolgerung selbst, nicht mehr vertrauen darf.[941]

Umstritten ist jedoch, ob der abgelehnte Sachverständige als sachverständiger Zeuge zu *Befundtatsachen* (i. S. der dritten Aussagekategorie) befragt werden darf.[942] Für diese Überlegung gibt es einen guten Grund – nämlich wenn

---

Beurteilung solcher Befangenheit im Bereich der freien Beweiswürdigung. Deshalb kann auch die Besorgnis der Befangenheit, die Anlaß zur Ablehnung eines Sachverständigen gegeben hat, nicht dazu führen, diesen als Zeugen oder als sachverständigen Zeugen insoweit auszuschließen, als es sich um die Wiedergabe der ihm bei Durchführung des Auftrages bekanntgewordenen Tatsachen handelt. Sie können und dürfen mit zum Inhalt der Zeugenvernehmung gemacht werden, weil sie Gegenstand seiner sinnlichen Wahrnehmung gewesen sind. Daß die Wahrnehmung erst durch die Berufung zum Sachverständigen ermöglicht wurde, rechtfertigt keine andere Beurteilung; denn die Zulässigkeit der Vernehmung einer Person als Zeuge ist nicht davon abhängig, wie sie ihre Kenntnis erlangt hat. Die erfolgreiche Ablehnung eines Sachverständigen hindert daher nicht, ihn als Zeugen oder als sachverständigen Zeugen über die von ihm im Rahmen seines Auftrags ermittelten Tatsachen zu vernehmen; sie verbietet nur, daß er weiterhin als Sachverständiger im Verfahren mitwirkt. Er darf also sein Gutachten nicht als Zeuge erstatten und darf deshalb als solcher nicht zu den Schlußfolgerungen gehört werden, die er aus jenen Tatsachen auf Grund seiner Sachkunde gezogen hat und auf die das Gericht für die Urteilsfindung angewiesen ist, weil ihm insoweit die eigene Sachkunde fehlt. Wohl aber darf der neue Sachverständige die Zeugenaussage des abgelehnten Sachverständigen für die eigenen Schlußfolgerungen verwerten und zur Grundlage seines Gutachtens machen."

940 BGHSt 20, 222, 224; *Hanack*, JR 1966, 425; Meyer-Goßner/*Schmitt*, § 74 Rn. 19; SK-StPO/*Rogall*, Vor § 72 Rn. 77, § 74 Rn. 65; KK/*Senge*, § 74 Rn. 14.

941 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 250.

942 Zustimmend RG JW 1931, 2027, 2028 m. Anm. Mannheim; BGHSt 20, 222, 223 mit abl. Anm. Hanack; BGH NStZ 2002, 44; BGH NJW 2005, 445, 447; BGH NStZ-RR 2010, 210; SK-StPO/*Rogall*, § 74 Rn. 65; KK/*Senge*, § 74 Rn. 15; Löwe/Rosenberg/*Krause*, § 74 Rn. 34; Meyer-Goßner/*Schmitt*, § 74 Rn. 19; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 333; *Ulrich*, Der gerichtliche Sachverständige, Rn. 184; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 274 ff.; *Fezer*, JR 1990, 397 m. w. N., 400; *Gössel*, Strafverfahrensrecht, S. 230; *ders*., DRiZ, 1980, 363, 372; *Roxin/Schünemann*, § 27 Rn. 15; *Henkel*, Strafverfahrensrecht, S. 219; *Schlüchter*, Das Strafverfahren, Rn. 529; *Stein*, Das private Wissen des Richters, S. 76 f.; *Rüping*, Das Strafverfahren, Rn. 193; *Mezger*, AcP 117 (1918), Beilageheft, 1, 20; *Hegler*, AcP 104 (1909), 151, 219 Fn. 159, 268 f.; ablehnend *Eisenberg*, Beweisrecht der StPO, Rn. 1561; *Peters*, Strafprozess, S. 370; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 89 f.; *Geppert*, DAR 1980, 315, 321; *Hanack*, JR 1966, 425; *Schmidhäuser*, ZZP 72 (1959), S. 365, S. 373 f.; tendenziell auch Löwe/Rosenberg/*Krause*, § 74 Rn. 36.

die Beobachtungen des erfolgreich Abgelehnten unwiederholbar sind[943] – wie im Falle flüchtiger Spuren (was bei Daten oft der Fall sein kann, siehe dazu unten im 3. Teil, B. II. 3. a)). Ohne eine Verwertung der Aussage würde die Sachverhaltsfeststellung im Urteil eventuell auf einer unsicheren Grundlage ruhen.[944] Wenn z. B. bestimmte Spuren an einer Leiche wegen fortschreitender Verwesung nicht durch einen neuen Sachverständigen festgestellt werden können, so ist es möglich, den erfolgreich abgelehnten Sachverständigen darüber zu befragen, welche chemischen Tests er mit welchen Gewebeproben durchgeführt hat, welche Schnitte er an der Leiche vorgenommen hat und über welche Seh-, Hör-, Tast- oder Geruchswahrnehmungen er dabei berichten kann. Er darf aber gerade nicht darüber vernommen werden, weshalb er bestimmte Testverfahren anwandte und weshalb er bestimmte Schnitte ausführte, da das eine Aufforderung bedeutete, die nach Ansicht des abgelehnten Sachverständigen einschlägigen Erfahrungssätze zu nennen. Weiter ist es nicht gestattet (entgegen der Auffassung von Sarstedt[945]), den früheren Sachverständigen Schlussfolgerungen berichten zu lassen, die er aus bestimmten Wahrnehmungen gezogen hat, sofern dazu eine Anwendung von Erfahrungssätzen notwendig wäre, bezüglich welcher dem Gericht die erforderliche Sachkunde fehlt.[946]

Die Mindermeinung[947] lehnt das u. a. mit dem Argument ab, dass die h. M. im Widerspruch zum Auftrag als Abgrenzungskriterium stehe. Denn ginge man von dem Auftrag als Abgrenzungskriterium aus, sei er als Grund für die Tatsachenwahrnehmung für die Einordnung der Beweisperson von entscheidender Bedeutung.[948] Ohne die Beauftragung hätte die Beweisperson die Tatsachen nicht wahrnehmen können.[949] Dem entgegnet die h. M.[950] jedoch,

---

943 Bei Wiederholbarkeit von Untersuchungsergebnissen erscheint es taktisch jedenfalls klüger für das Gericht die Abgrenzungsfrage zu umgehen und einen neuen bestellten Sachverständigen mit den Wahrnehmungen zu beauftragen (soweit prozessökonomisch vertretbar).

944 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 279.

945 Löwe/Rosenberg/*Sarstedt*, 22. Aufl. § 85 Rn. 4.

946 So auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 278 mit einem Beispiel zu Spuren an einer Leiche, die wegen fortschreitender Verwesung nicht durch einen neuen Sachverständigen festgestellt werden können.

947 *Eisenberg*, Beweisrecht der StPO, Rn. 1561; *Peters*, Strafprozess, S. 370; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 89 f.; *Geppert*, DAR 1980, 315, 321; *Hanack*, JR 1966, 425; *Schmidhäuser*, ZZP 72 (1959), 365, 373 f.; tendenziell auch Löwe/Rosenberg/*Krause*, § 74 Rn. 36.

948 Zum Auftrag als Abgrenzungskriterium, siehe bei Abgrenzung der Prozessrollen in diesem Teil, B. III. 3.

949 *Schmidhäuser*, ZZP 72 (1959), 365, 373 f.; *Geppert*, DAR 1980, 315, 321; *Vyhnálek*, Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, S. 89 f.

950 Zustimmend RG JW 1931, 2027, 2028 mit Anm. Mannheim; BGHSt 20, 222, 223 mit abl. Anm. Hanack; BGH NStZ 2002, 44; BGH NJW 2005, 445, 447; BGH

dass sich aus dem Umstand, dass sich Zeugen- und Sachverständigenaussagen in der dritten Kategorie inhaltlich überschneiden, schon die Antwort für die Verwertbarkeit der Befundtatsachen eines abgelehnten Sachverständigen im Rahmen des Zeugenbeweises ergibt. So führt Toepel zutreffend aus, dass der Auftrag keine ausschließliche Abgrenzung liefert (siehe dazu auch bei B. III. 3.), sondern eine „(…) Begründung dafür, warum die Wahrnehmungen nicht nur als solche eines sachverständigen Zeugen, sondern darüber hinaus als Sachverständigentätigkeit betrachtet werden".[951] Würde sich die Ablehnungsmöglichkeit nicht nur auf die erste und zweite Kategorie beschränken, wäre die fehlende Ablehnungsmöglichkeit gegen den sachverständigen Zeugen in § 85 StPO nicht nachvollziehbar.[952] Eine nachträgliche Aufteilung in Sachverständigen- und Zeugenaussage, wie sie nach Auffassung Lents[953] vorgenommen werden muss, sei gerade nicht notwendig, da die Zeugenposition von der Sachverständigenposition bereits vor der Ablehnung lediglich überlagert war.[954] Weil es beim Zeugenbeweis eben nicht auf eine Befangenheit ankommt, gibt es hier auch kein Ablehnungsrecht, sondern das wird im Rahmen der tatrichterlichen Beweiswürdigung nach § 261 StPO berücksichtigt.[955]

Soweit befürchtet wird, dass die Sachkunde über die Mitteilung der sachkundigen Bewertung der Wahrnehmung in das Urteil einfließt,[956] verkennt diese Auffassung, dass Tatsachenwahrnehmungen stets eine gewisse Beurteilung zugrunde liegen.[957] Wie oben beschrieben, ist der Unterschied zwischen der zweiten und dritten Aussagekategorie kein logischer, sondern ein erkennt-

---

NStZ-RR 2010, 210; SK-StPO/*Rogall*, § 74 Rn. 65; KK/*Senge*, § 74 Rn. 15; Löwe/Rosenberg/*Dahs*, 24. A. § 74 Rn. 34; Meyer-Goßner/*Schmitt*, § 74 Rn. 19; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, Rn. 333; *Ulrich*, Der gerichtliche Sachverständige, Rn. 184; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 274 ff.; *Fezer*, JR 1990, S. 397 m. w. N., 400; *Gössel*, Strafverfahrensrecht, S. 230; *ders*., DRiZ, 1980, 363, 372; *Roxin/Schünemann*, § 27 Rn. 15; *Henkel*, Strafverfahrensrecht, S. 219; *Schlüchter*, Das Strafverfahren, Rn. 529; *Stein*, Das private Wissen des Richters, S. 76 f.; *Rüping*, Das Strafverfahren, Rn. 193; *Mezger*, AcP 117 (1918), Beilageheft, 1, 20; *Hegler*, AcP 104 (1909), 151, 219 Fn. 159, 268 f.

951 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 276.

952 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 251.

953 *Lent*, ZZP 60 (1936/1937), 9, 28 ff. 30 ff. für den Zivilprozess; daran anschließend auch *Schmidhäuser*, ZZP 72 (1959), 365, 374.

954 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 276 f.; *Hegler*, AcP 104 (1909), 151, 219 Fn. 159; *Mezger*, AcP 117 (1918), Beilageheft, 1, 20; *Fezer*, JZ 1990, 397, 398; SK-StPO/*Rogall*, Vor § 72 Rn. 77.

955 BGHSt 20, 222, 224.

956 Löwe/Rosenberg/*Sarstedt*, 22. A., § 85 Rn. 4.

957 Vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 277.

nistheoretischer.[958] Die Aussage des abgelehnten Sachverständigen als sachverständiger Zeuge geht somit dann nicht über die Beweisaufgabe des Zeugen hinaus, wenn sich denkende Verarbeitung im Rahmen des Selbstverständlichen bewegt.[959] Dabei wird die Grenzziehung zu Schlussfolgerungen i. S. d. zweiten Aussagekategorie nicht immer leicht sein,[960] dass der Gesetzgeber aber von der Möglichkeit einer Trennung ausgeht, ist aus § 85 StPO abzulesen (siehe dazu auch bei B. III. 3.)

Nochmal hervorzuheben ist, dass das erkennende Gericht die Befangenheit des abgelehnten Sachverständigen allerdings entsprechend zu würdigen hat. Insbesondere muss der Gefahr eines „verkappten Gutachtens“[961] durch die Zeugenaussage entgegengewirkt werden, indem dafür Sorge getragen wird, dass der Zeuge tatsächlich nur über Tatsachenwahrnehmungen aussagt[962] und die Grenze zwischen den Schlussfolgerungen der zweiten und der dritten Aussagekategorie (soweit eben möglich) eingehalten werden.[963]

Lässt der sachverständige Zeuge dennoch Erfahrungssätze oder Schlussfolgerungen einfließen, die beweisbedürftig wären, schafft er die Gefahr, dass die ganze Aussage unverwertbar wird, v. a. wenn die Teile, die der dritten Aussagekategorie angehören sich nicht deutlich von den unzulässigen Teilen trennen lassen. Verwertet das Gericht solche unzulässig über den Umweg des sachverständigen Zeugen eingeführte Gutachtenteile, so besteht ein Revisionsgrund nach § 337 StPO wegen Missachtung des Beweisverwertungsverbots[964], falls nicht ausnahmsweise das Urteil erkennen lässt, dass das Gericht ohne Berücksichtigung des Gutachtens zu demselben Ergebnis gekommen wäre[965] und das Urteil somit nicht auf der Verletzung der Verbotsnorm beruht.[966]

Um dieses Risiko zu verringern, kann das Gericht anstelle des abgelehnten den bestellten Sachverständigen bitten, der Vernehmung des sachverständigen Zeugen beizuwohnen und das Gericht auf die Verwendung von Fachtermini

---

958 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 116; *Hegler*, AcP 104 (1909), 151, 193 f.

959 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 116; *Hegler*, AcP 104 (1909), 151, 193 f.

960 Löwe/Rosenberg/*Krause*, § 74 Rn. 34; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 277 f. mit Beispielen; SK-StPO/*Rogall*, Vor § 72 Rn. 77.

961 Löwe/Rosenberg/*Krause*, § 74 Rn. 34.

962 *Dahs*, Handbuch des Strafverteidigers, Rn. 231; Löwe/Rosenberg/*Krause*, § 74 Rn. 36.

963 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 251; Löwe/Rosenberg/*Dahs*, 24. A. § 74 Rn. 34.

964 Vgl. OLG Düsseldorf MDR 1984, 71 (72).

965 Löwe/Rosenberg/*Krause*, § 74 Rn. 41.

966 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 278.

und damit verbundene Erfahrungssätze und ggf. Schlussfolgerungen hinzuweisen[967].

Soweit das Gutachten unverwertbar ist, verliert der Sachverständige auch seinen Anspruch aus § 8 JVEG.[968]

d) Fazit

Im Ergebnis zeichnet sich das Bild, dass die Ausgangspositionen für Staatsanwaltschaft und Verteidigung (immer noch) zu ungleich sind, um von Rechtsgleichheit und -sicherheit und Waffengleichheit sprechen zu können. So sind die Unterschiede wohl hauptsächlich in der tatsächlichen Rechtspraxis (und weniger in der prozessualen Regelung) zu sehen. Eine besonders kritische Beweiswürdigung, auch unter Berücksichtigung der Einwände der Prozessbeteiligten, sollte im gerichtlichen Alltag als Mindestvoraussetzung gesehen werden. Dabei müssen die Tatgerichte, v. a. wegen der mangelnden Konfrontation, die Zuverlässigkeit des nicht konfrontierbaren Beweismittels besonders vorsichtig prüfen.[969]

Den logistischen Vorteil der Staatsanwaltschaft wird die Verteidigung durch bessere Vorbereitung und damit einhergehend auch mit Zugang zu den Aktenbestandteilen (sowohl vorbereitendes schriftliches Gutachten und zugrundeliegende Arbeitsunterlagen, wie verarbeitete Beweisdaten und verwendete Datenverarbeitungs- und -analyseprogramme) und weniger Vertrauen in die Leistungsfähigkeit des Richters auszugleichen haben, indem sie ihrerseits den Sachverständigen dazu bringt, Widersprüche zu erklären oder zu beseitigen und die Voraussetzungen des Gutachtens, soweit sie nicht klar werden, darzulegen oder von anderen Anknüpfungstatsachen auszugehen.[970]

VI. Die Grenzen der Sachverständigentätigkeit

Wohl eine Kunst in der forensischen Praxis ist es, das eine zu tun, ohne das andere zu lassen – alle verfügbaren Erkenntnisquellen auszuschöpfen, ohne

---

967 Denn das Gericht ist gefährdet, die Bedeutung der Zeugenrolle mangels Sachkunde insb. dann nicht zu erkennen, wenn in der Wissenschaft der Alltagssprache entnommene Begriffe verwendet werden, die aber innerhalb eines bestimmten Wissenschaftszweigs eine präzisierte und vielleicht ganz andere Bedeutung besitzen.

968 Vgl. auch § 8a JVEG; *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, Rdnr. 166; Meyer-Goßner/*Schmitt*, § 74 Rn. 1. Bzgl. der Folgen der Sachverständigenablehnung für die Verwertung seiner Wahrnehmungen, vgl. auch *Fezer*, JR 1990, 397 ff.

969 *Mysegades*, Software als Beweiswerkzeug, S. 97 f. m. w. N.

970 So schon *Walter*, Sachverständigenbeweis, S. 156 f.

die eigene Überzeugung zu unterdrücken.[971] Das gilt besonders für die forensische Informatik und für die durch die Universalität der Technologie bedingten massenhaften Daten, die alle Lebensbereiche berühren (bis in den unantastbaren Kern der Intimsphäre, dem Beschuldigten gar ins „virtuelle" Gehirn kriechen und aufzuzeichnen zu können, was sich dort abspielt)[972].

Wie vermessen sich dabei die Grenzen für den IT-Sachverständigen im Rahmen seiner Tätigkeit? Dürfen diese, was sie können oder sind dem Grenzen gesetzt und wenn ja, wie verlaufen diese?[973]

Die Grenzen der IT-Sachverständigentätigkeit sind dabei zunächst technisch bedingt[974] oder können sich durch das Fehlen der erforderlichen besonderen Sachkunde ergeben.[975] Weiter hat sich der IT-Sachverständige im Rahmen seines Auftrags zu bewegen und sich an der zu beantwortenden Beweisfrage und den zur Verfügung gestellten Anknüpfungstatsachen[976] zu orientieren. Was aber, wenn der IT-Sachverständige im Rahmen der Beschaffung der Befundtatsachen (Dritte Aussagekategorie) in den Grenzen seines Auftrags Eingriffe in Rechtspositionen anderer Personen vornehmen muss (wie die Verletzung der Privatsphäre bei der Auswertung von Kommunikationsinhalten)[977] und dabei auf sensible Daten stößt, die vllt. auch gar nicht mit der Beweisfrage im Zusammenhang stehen, wie z. B. abgespeicherte Tagebucheinträge, die dem unantastbaren Kernbereich der Intimsphäre zugeordnet werden müssen? Gelten für den IT-Sachverständigen die Grenzen der StPO, deren Einhaltung den Strafverfolgungsbehörden aufgetragen wird?

Das soll im Folgenden erörtert werden.

---

971 Vgl. *Walter*, Sachverständigenbeweis, S. 162.

972 Vgl. in diesem Zusammenhang auch die immer lauter werdende Forderung, dass bei einer IT-Durchsuchung strengere Regulierungen zugunsten der Beschuldigten gelten sollten, https://www.handelsblatt.com/finanzen/steuern-recht/buergerrechte-it-durchsuchung-strengere-regulierung-gefordert/100094639.html?trk=feed-detail_comments-list_comment-text [19.12.2024].

973 Gedanken aus *Hassemer*, ZStW 121 (2009), S. 830.

974 Bspw. wenn ihm aufgrund verschlüsselter Daten ein Zugriff auf die Information verwehrt ist.

975 Z. B. besondere analytische Fähigkeiten, um die Daten gerichtsverwertbar aufzubereiten oder Wissen aus einer anderen ihm nicht bekannten Unterkategorie der forensischen Informatik relevant werden.

976 Unter Beachtung der Möglichkeit der Erweiterung nach § 80 StPO auf Anregung des Sachverständigen, dazu sogleich.

977 Vgl. zu den Datenschutzgrundrechten *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 32 ff.

1. Grenzen durch den Rahmen des Auftrags

Zunächst hat sich der IT-Sachverständige im Rahmen des Auftrags zu bewegen. Die Beweisfragen und die mitgeteilten Anknüpfungstatsachen sollen als Grundlage, aber auch als Grenzen der Gutachtenerstattung dienen.[978]

Hält sich ein Sachverständiger nicht an den ihm vom Auftraggeber vorgegebenen Beweisbeschluss bzw. Auftrag, ohne zuvor auf eine Klarstellung oder Ergänzung der Beweisfragen hingewirkt zu haben (vgl. § 80 StPO), kann dieses Verhalten Grund für eine Ablehnung wegen Besorgnis der Befangenheit sein (siehe dazu die Ausführungen in V. 2. c)).[979] Der Sachverständige hat etwaige Bedenken dem Auftraggeber zu unterbreiten und kann den Inhalt seines Auftrags nicht eigenmächtig verändern.[980]

2. Keine eigenen Ermittlungen

Fehlen dem IT-Sachverständigen Anknüpfungstatsachen zur Beantwortung der Beweisfrage, darf er diese nicht eigenständig ermitteln.

§ 80 StPO weist auf die Möglichkeit hin, den Sachverständigen bei der Informationsgewinnung im Rahmen der Vorbereitung seines Gutachtens zu unterstützen.[981] Zur Vorbereitung des Gutachtens kann dem Sachverständigen gem. § 80 StPO gestattet werden, an der Vernehmung von Zeugen und des Beschuldigten teilzunehmen und die Akten einzusehen. Aus § 80 StPO lassen sich allerdings keine eigenen Rechte des Sachverständigen z. B. auf Durchführung einer Zeugenvernehmung herleiten. Vielmehr besteht insoweit lediglich eine Obliegenheit des Auftraggebers: Hat der Sachverständige auf die aus seiner Sicht erforderliche weitere Beweiserhebung i. S. d. § 80 Abs. 1 StPO hingewiesen (wie auch über den Wortlaut des § 80 Abs. 1 StPO[982] hinausgehende Beschlagnahmen, Augenscheinseinnahmen und Urkundsbeweise[983]) oder Akteneinsicht bzw. Anwesenheit bei Vernehmungen i. S. d. § 80 Abs. 2 StPO begehrt, so kann ihm kein Mangel des Gutachtens vorgeworfen werden, der darauf beruht, dass das Gericht seinem Begehren nicht stattgegeben hat.

---

978 *Krauß*, ZStW 85 (1973), 320, 322.

979 OLG Celle v. 18.1.2002 – 14 W 45/01, NJW-RR 2003, 135; OLG Köln v. 30.12.1986 – 20 W 65/86, NJW-RR 1987, 1198; OLG Nürnberg v. 12.6.2006 – 5 W 980/06, MDR 2007, 295; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 367.

980 *Wolf*, ZWH 2012, 125 (129).

981 Bei psychiatrischen Gutachtern z. B. durch das Einholen von Gesundheitsunterlagen aus vergangenen Krankheitsepisoden (Arztbriefe).

982 Die Vorschrift nennt eine Selbstverständlichkeit, nämlich dass der Sachverständige das Gericht im Rahmen seiner Gutachtenerstattungspflicht auf fehlende Anknüpfungstatsachen hinzuweisen hat.

983 Vgl. KK/*Senge*, § 80 Rn. 2.

Es lässt sich jedoch nichts dagegen einwenden, falls der Sachverständige von Rechten Gebrauch macht, die ihm, wie jedermann, zur Verfügung stehen, sofern das nicht mit seiner Pflicht zu unparteiischer Gutachtenerstattung kollidiert,[984] wie z. B. das Beiziehen von Urkunden und behördlichen Akten, etwa den im Unternehmensregister publizierten Jahresabschlüssen etc.[985] Gleichwohl empfiehlt es sich, derartige Erhebungen in Absprache und Mitwirkung des Auftraggebers durchzuführen, insb. wenn die Unterlagen nicht öffentlich zugänglich sind, um nicht den Eindruck zu erwecken, der Sachverständige erhebe die Urkunden im Rahmen eines „staatsanwaltschaftlichen Auskunftsersuchens".[986]

Über die Grenzen des Auftrages und des § 80 StPO hinaus, darf der IT-Sachverständige keine eigenen Ermittlungen – v. a. bei der Beschaffung der Befundtatsachen (dritte Aussagekategorie) – vornehmen. Wird der Sachverständige anstelle von richterlichen Augenscheinseinnahmen tätig, so muss er Durchsuchungen und Beschlagnahmungen den Strafverfolgungsbehörden überlassen.[987] Aus dem Gebot der Verhältnismäßigkeit kann sich aber auch ergeben, dass einzelne technische Verrichtungen, die nicht ohne sachkundige Hilfe durchführbar sind[988], unter Aufsicht der zuständigen Beamten dem Sachverständigen selbst überlassen werden.[989] Ein eigenmächtiges Vorgehen des Sachverständigen, welches von den eigentlich für die Durchsuchung zuständigen Beamten nur geduldet wird, wäre von der StPO nicht gedeckt.[990]

---

984 Insoweit zutreffend *Fincke*, ZStW 86 (1974), 656 (664). Eine unparteiische Gutachtenerstattung läge dann nicht mehr vor, wenn der Sachverständige vor der Vernehmung Zeugen aufsucht und mit diesen über den Fall spricht, ohne dies dem Gericht mitzuteilen. Aber eine Ortsbesichtigung kann er z. B. wie jedermann vornehmen, ohne Beschuldigte oder Verteidiger benachrichtigen zu müssen (vgl. BGH VRS 35, 428).

985 OLG Stuttgart v. 29.5.1995 – 2 W 3/95; OLG Naumburg v. 17.2.2010 – 10 W 13/10; Meyer-Goßner/*Schmitt*, § 80 Rn. 4; SK-StPO/*Rogall*, § 80 Rn. 20; Löwe/Rosenberg/*Krause*, § 80 Rn. 10.

986 Vgl. auch *Wolf*, ZWH 2012, 125 (126).

987 Gesetzliche Sonderfälle der Augenscheinseinnahme: So wird die Leichenöffnung bspw. gem. § 87 Abs. 2 StPO zwei Ärzten selbstverantwortlich übertragen (abweichend von der sonstigen Durchsuchung von Sachen, gem. §§ 102 ff. StPO). Auch die Untersuchung von Personen kann der Sachverständige nach Anordnung des Richters bzw. der Staatsanwaltschaft und ihrer Hilfsbeamten selbstverantwortlich übernehmen (§§ 81, 81a, 81c, 81e StPO), vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 368.

988 Ergibt sich aus dem Gebot der Beschränkung von Beweiserhebungen auf das unerlässliche Maß durch sachkundige Hilfe, vgl. OLG Karlsruhe NStZ 1991, 50 (51).

989 So bereits *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 368.

990 Vgl. auch hier OLG Karlsruhe NStZ 1991, 50 (51): Hier wurde nicht gebilligt, dass innerstaatliche Behörden die Vornahme eigener Durchsuchungen durch amerikanische Beamte dulden.

Es gilt dabei stets, die Grenze zwischen der Tätigkeit als Sachverständiger oder als Ermittlungsperson zu wahren (siehe dazu B. III 2. b)).[991] Alle über den Auftrag hinausgehenden Ermittlungsmaßnahmen im Rahmen der Suche nach Beweisen und deren Beweissicherung obliegen strafprozessual gem. §§ 160 StPO, 152 GVG, 404 AO ausschließlich der Staatsanwaltschaft und ihren gesetzlichen Ermittlungspersonen.[992] Vor diesem Hintergrund ist eine Privatisierung der strafrechtlichen Ermittlungsmaßnahmen ausgeschlossen.[993]

Es ergibt sich nun die Frage, welche Grenzen für den IT-Sachverständigen bei seiner Tätigkeit gelten, die innerhalb des Auftrags liegen. In Gesprächen mit IT-Sachverständigen aus der Praxis bildet sich das deutliche Stimmungsbild ab, dass große Unsicherheit in Bezug auf solche Grenzen, genauer gesagt auf das Erfordernis und die genaue Ausgestaltung der Wahrung der Privatsphäre besteht – trotz eines Strebens nach einer umfangreichen „Wahrheitsermittlung" in Bezug auf die zu beantwortende Beweisfrage.[994] So empfinden die IT-Sachverständigen – nicht zuletzt wegen ihrer technischen Versiertheit – die Vertraulichkeit der Daten unbestritten als sehr wichtig und möchten das respektieren. Inwieweit dem aber bei der forensischen Auswertung Rechnung getragen werden muss, ist unsicher. Das erfordert eine deutliche Stellungnahme und Pflichtenzuweisung, nicht zuletzt durch die Auftraggeber in der Praxis.

3. Die rechtsstaatliche Bindung bei der Durchführung des Gutachtenauftrags[995]

Die StPO enthält eine Reihe von Vorschriften, die das Strafverfahren regeln und die Interessen der Beteiligten schützen sollen (sog. Prozessgrundrechte).[996] Durch die Beauftragung eines IT-Sachverständigen entsteht eine komplexere Situation aus Sicht der Betroffenen, die sich in einem Strafverfahren nun nicht mehr nur der Staatsanwaltschaft und den Tatrichterinnen gegenüber sehen, sondern auch dem IT-Sachverständigen.[997] Aus dem Gebot der Rechtsstaatlichkeit stammt die Maxime fairer Behandlung. Die rechtsstaatliche Funktion sichert dem Beschuldigten seine Subjektstellung zu (aus Art. 1 Abs. 1 GG

991 Weiter dazu Löwe/Rosenberg/*Krause*, § 80 Rn. 6; Meyer-Goßner/*Schmitt*, § 80 Rz. 2; *Krekeler*, wistra 1989, S. 52; SK-StPO/*Rogall*, § 80 Rn. 18.

992 *Wenzel*, NZWiSt 2016, 85 f.

993 *Wenzel*, NZWiSt 2016, 85 (86).

994 Bspw. *Sunde*, Non-technical Sources of Errors.

995 Vgl. *Walter*, Sachverständigenbeweis, S. 129 ff.

996 Vgl. auch *Mysegades*, Software als Beweiswerkzeug, S. 82 ff. zur Garantie eines fairen Verfahrens und dem Anspruch auf rechtliches Gehör.

997 *Plewig*, Funktion und Rolle des Sachverständigen, S. 70.

folgt, dass der Mensch niemals zum Objekt eines staatlichen Verfahrens herabgewürdigt werden darf[998]) und damit den Anspruch auf die gesetzlich festgelegte Art und Weise des Verfahrensablaufs sowie die Darlegung einer zweifelsfreien Entscheidung. Dieses Recht ergibt sich u. a. aus der Unschuldsvermutung und der Definition des Beschuldigten als Prozesssubjekt sowie dem Schutz sonstiger Prozessbeteiligter (wie Zeugen). Für den Sachverständigen gibt es weder bei der Auswertung des IT-Asservats noch bei der Durchsicht der mitübergebenen Akten ein dem Grundsatz in dubio pro reo entsprechendes Prinzip. Das wird v. a. dann gefährlich, wenn (wie häufig von der Justiz erwartet wird) ein Gewissheitsurteil abgegeben werden soll.[999]

Anhand des Beispiels der forensischen Durchsicht von IT-Asservaten sollen die nachfolgenden Argumente für ein Für oder ein Wider in Bezug auf die Geltung der verfahrensrechtlichen Grenzen für den IT-Sachverständigen erfolgen. Das gilt aber auch für alle anderen Ermittlungshandlungen, die IT-Sachverständige im Rahmen ihres Auftrags durchführen. Die §§ 110 ff. StPO richten sich dabei zunächst an die Strafverfolgungsbehörden, ermöglichen jedoch die Hinzuziehung von externen Sachverständigen.[1000] M. E. richtet sich die aus dem Gesetz ergebende Verpflichtung aber auch für den hinzugezogenen IT-Sachverständigen.[1001]

Man könnte zwar zunächst die Geltung der Ermittlungsgrenzen für den IT-Sachverständigen wie folgt ablehnen: So handelt es sich bei der Durchsicht nach § 110 StPO um eine „Ermittlungshandlung“ und nicht um eine sachverständige forensische „Durchsicht“. Auch ist der IT-Sachverständige kein Organ der Strafverfolgung. Anstatt sich um verfahrensrechtliche Grenzen der Strafverfolgungsbehörden zu kümmern, soll er sich „nur“ auf die Beantwortung spezifischer Fragen konzentrieren und dabei unparteiisch und nach bestem Gewissen verfahren. Man könnte auch an das Argument denken, dass es sich bei der sachverständigen forensischen Durchsicht mit dem Ziel der Gutachtenerstattung vor Gericht lediglich um eine „mittelbare“ Durchsuchung nach §§ 102 ff. StPO handle. Selbstständiges Beweismittel ist der IT-Sachverständige danach im Rahmen seiner berufsspezifischen Kenntnisse, im Übrigen Beweismittel als verlängerter Arm des Auftraggebers. Prozessrechtlich sollen die dabei erlangten Informationen dem Auftraggeber zuzurechnen sein. Da-

998 Vgl. *Maunz/Dürig/Herzog*, Art 1, Rn. 28, 34 ff.

999 Vgl. auch *Walter*, Sachverständigenbeweis, S. 130.

1000 LG Kiel v. 14.8.2006 – 37 Qs 54/06, CR 2007, 116 = NJW 2006, 3224.

1001 Siehe dazu vertiefend den Streit in Bezug auf Bindungspflicht des § 136a StPO und einer sich daraus ergebenden Belehrungspflicht für den Gutachter; *Plewig*, Funktion und Rolle des Sachverständigen, S. 70 f. m. w. N.; anders BGH JR 1969, 231 f.; JZ 1969, 437.

nach wäre es Aufgabe des Auftraggebers, die verfahrensrechtlichen Grenzen zu wahren bzw. herzustellen.[1002]

Die Frage ist aber doch, wie der Rechtsschutz der Betroffenen sonst gewahrt wird, wenn die Durchsicht, auf die sich die §§ 110 ff. StPO beziehen, im Kern nur die IT-Sachverständigen vornehmen und eben nicht die Strafverfolgungsbehörden (siehe notwendige besondere Sachkunde dafür bei B. II. 2. c) bb)). In diesem Zusammenhang wird auch von der tatsächlichen prozessualen Betroffenheit gesprochen.[1003] So spricht v. a. für eine Geltung der Ermittlungsgrenzen auch für den IT-Sachverständigen, dass der Gesetzgeber gesehen hat, dass zur forensischen Durchsicht von IT-Asservaten, § 110 Abs. 1 StPO, regelmäßig IT-Forensiker zum Einsatz kommen müssen. Zwar spricht er zunächst hauptsächlich von Spezialisten der gesetzlichen Ermittlungspersonen i. S. d. § 110 Abs. 1 StPO, sieht jedoch auch, dass es Fälle gibt, in denen dritte IT-Sachverständige beauftragt werden müssen; zumal Polizei und die Steuerfahndung in der Praxis überlastet sind[1004] und immer häufiger private Sachverständigenbüros mit der Auswertung von IT-Asservaten i. S. d. § 110 StPO befasst sind (siehe dazu bereits oben in der Einführung). Der Gesetzgeber wollte mit der Einführung der §§ 110 ff. StPO eine umfassende Schutzkonzeption in Bezug auf die Vertraulichkeit und Datenschutz gegenüber dem Beschuldigten, seinen Angehörigen und unbeteiligten Dritten schaffen.[1005] Eine Durchbrechung der aufgestellten Prinzipien wäre systemwidrig. Solange die Praxis also so aussieht, dass externe IT-Sachverständige weiterhin mit einer (vollständigen) Durchsicht von IT-Asservaten beauftragt werden, müssen die Prinzipien der StPO auch für diese gelten. Daneben geht auch die höchstrichterliche Rspr.[1006] davon aus, dass den Sachverständigen als „Richtergehilfen" die gleiche Pflicht wie den Richter treffe.[1007] Was jenem verwehrt sei,[1008] gelte auch für die herangezogenen Sachverständigen. Zwar ist der Sachverständige kein Organ der Strafrechtspflege, er verwischt aber die klare Abgren-

1002 Vgl. MüKo-StPO/*Hauschild*, § 110 Rn. 11; KK/*Bruns* § 110, Rn. 4.

1003 Vgl. *Plewig*, Funktion und Rolle des Sachverständigen, S. 72 m. w. N.

1004 Das ergibt sich v. a. aus Gesprächen mit Praktikerinnen und kann zum Teil auch aus den überlangen Verfahrensdauern abgeleitet werden, siehe https://www.drb.de/newsroom/presse-mediencenter/nachrichten-auf-einen-blick/nachricht/news/strafjustiz-am-limit-1 [26.6.2023].

1005 Vgl. MüKo-StPO/*Hauschild*, § 110 Rn. 11; KK/*Bruns* § 110, Rn. 4.

1006 Vgl. nur BGH St 11, 212.

1007 Im Gesetz spiegelt sich dieser Gedanke in den Mechanismen zur Gewährleistung der Objektivität – wie bei Richtern – wider, vgl. oben in diesem Teil, B. II. 2. c) dd).

1008 Damals in Bezug auf die in § 136a Abs. 1 S. 1 StPO genannten Methoden, vgl. BGH St 11, 212.

zung durch die Annahme mittelbarer Überführungstätigkeit.[1009] Auch aus den Argumenten oben wird deutlich, dass davon ausgegangen wird, dass der IT-Sachverständige „als verlängerter Arm" des Auftraggebers tätig wird. Dann sollen für ihn doch auch die gleichen Pflichten gelten (soweit das Gesetz nichts anderes formuliert). V. a. im Hinblick auf die aktuelle Bestellungspraxis der IT-Sachverständigen durch die Staatsanwaltschaften im Ermittlungsverfahren stimmt diese Argumentation auch mit den Ausführungen bei der Pflicht zur Objektivität der Sachverständigen überein (B. II. 2. c) dd)). So ergeben sich die Grenzen der einzubeziehenden Personen und die Grenzen der ihnen übertragbaren Aufgaben aus Pflicht und Stellung, die den Ermittlungsbehörden im gesetzlich geordneten Strafverfahren zukommt. Aus dieser vom Legalitätsprinzip geprägten besonderen Stellung folgt, dass an die Anklagebehörde und die Personen, deren Hilfe sie sich bedienen (und damit sind hier nicht nur ihre Ermittlungspersonen, sondern auch die IT-Sachverständigen gemeint), nicht nur hohe Anforderungen an ihre Unparteilichkeit zu stellen sind, sondern es sind auch auf die zu wahrenden Grundrechte der Betroffenen zu achten. In der Literatur verlangt man bspw. im Rahmen einer sachverständigen Befragung durch psychiatrische Gutachter und der Frage einer vorherigen „Belehrung", dass sich der Sachverständige vorher vergewissern muss, dass der Beschuldigte freiwillig zu einer Stellungnahme bereit ist.[1010] Übertragen auf die Durchsicht hieße das, dass sich der Beschuldigte auch zu einer sachverständigen forensischen Durchsicht bereit erklären müsste. Das entspräche auch § 110 Abs. 2 StPO i. V. m. § 110 Abs. 1 S. 1 Hs. 2 StPO, wonach neben der Staatsanwaltschaft und deren Ermittlungspersonen auch weitere Beamte während der Durchsuchungsmaßnahme sowie im Nachgang i. S. d. §§ 102, 103 StPO grundsätzlich zu einer Auswertung befugt sind, dafür aber die Genehmigung des Inhabers der Daten oder Datenträger vorausgesetzt wird, ohne die eine Durchsicht unzulässig ist und zu einem Beweisverwertungsverbot führt. Daraus kann abgeleitet werden, dass, wenn ohne Einverständnis des Betroffenen gehandelt wird, was (meistens) der Fall ist, wenn IT-Sachverständige eine forensische Durchsicht von IT-Asservaten im Strafverfahren ausführen, zumindest aber die prozessualen Grenzen der Vertraulichkeit und des Datenschutzes gewahrt bleiben müssen. Dem wird wohl entgegnet werden, dass die derart hinzugezogenen Sachverständigen nur einen sehr eingeschränkten Handlungsrahmen haben und nur in Bezug auf die technischen Fragestellungen zu abgegrenzten Teilfragen hinzugezogen werden, während die Kernaufgaben der Durchsicht i. S. d. § 110 StPO bei der Staatsanwaltschaft und deren Ermittlungspersonen bleiben würden.[1011] Dass die Praxis jedoch

1009 Vgl. auch *Plewig*, Funktion und Rolle des Sachverständigen, S. 72.

1010 Vgl. *Jessnitzer*, Der gerichtliche Sachverständige, S. 210.

1011 *Wenzel*, NZWiSt 2016, 85 (86 f.).

anders aussieht, wurde oben bereits dargestellt. Solange das so ist, müssen die Auftraggeber auch die zu beachtenden strafprozessualen Grenzen auf die IT-Sachverständigen übertragen. Letztlich soll der Vertraulichkeits- und Datenschutz nicht umgangen werden können, indem man die Durchsicht (auch wenn nur zu Teilen) auf Externe „outsourced", denn vielfach übernehmen die Auftragnehmer diese Ergebnisse einfach als Basis für die weitere Sachverhaltsaufklärung bzw. Urteilsfindung.[1012]

Letztlich schwanken die Strafverfolgungsbehörden zwischen der Pflicht, die Wahrheit umfassend zu ermitteln, und der Pflicht, dabei die Schutzrechte der Betroffenen zu wahren. Dabei stehen die Sachverständigen wohl eher auf der Seite der Strafverfolgungsbehörden (nicht zuletzt aufgrund des Auftragsverhältnisses und der damit zusammenhängenden Kommunikation). Soweit das Gesetz nichts anderes vorschreibt, sind mit der Übertragung der Wahrheitserforschung in Bezug auf bestimmte Fragen und zugrundeliegende Daten auch die Pflichten und Grenzen mit zu übertragen, die sich für die Strafverfolgungsbehörden ergeben hätten, würden sie die Fragen selbst beantworten.

Um also die Frage von oben wieder aufzugreifen: Nicht alles, was Experten in einem Strafverfahren könnten, dürfen sie auch. Das ist fundamentales Prinzip des Strafprozessrechts. Nach seiner Regulierung der Grenzen des Wissens ist der Maßstab des Wissendürfens nichts Geringeres als der Schlussstein der Architektur.[1013]

Insofern ist m. E. vorzuschlagen, dass die Auftraggeber aus der Strafverfolgung im Rahmen der Formulierung des Beweisthemas bei der Auftragserteilung entsprechend ihrer Leitungspflicht aus § 78 StPO auf die jeweiligen und im konkreten Fall einzuhaltenden prozessualen Grenzen hinzuweisen haben und den IT-Sachverständigen damit ein Gefühl für die prozessualen Grenzen zu vermitteln.[1014] Dass das ein z. T. aufwendiges Vorhaben sein kann und der eh schon strapazierten Prozessökonomie widerspricht, ist der Verfasserin bewusst. Hilfreich könnte sein, vorgefertigte Textbausteine mit Fallbeispielen in Bezug auf spezifische Bereiche der forensischen Informatik und Deliktsbereiche (wie Datenträgeranalyse in Bezug auf den Vorwurf der §§ 184b ff. StGB) zu entwickelt (bspw. im Rahmen einer gemeinsamen Fortbildung oder Workshops mit Technikerinnen und Juristinnen). Diese könnten dann bei der konkreten Auftragserteilung entsprechend als Anhang beigefügt werden. Wenn

---

1012 Siehe auch *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, S. 165 f. für das Zivilrecht; *Wellmann*, Der Sachverständige in der Praxis, S. 90.

1013 Gedanken aus *Hassemer*, ZStW 121 (2009), S. 832.

1014 Bisher ergibt sich bspw. aus dem Austausch mit IT-Sachverständigen, dass E-Mails von Anwälten tabu seien. Das ist ein wichtiger Schritt in die richtige Richtung.

dennoch konkrete Fragen in Bezug auf Eingriffsgrenzen aufkommen, ist Rücksprache mit dem jeweiligen Auftraggeber zu halten.

In Bezug auf die verfahrensrechtlichen Grenzen der jeweiligen Ermittlungshandlungen und v. a. dem Vertraulichkeits- und Datenschutz wird auf Rückert[1015] und die jeweilige Kommentarliteratur der strafprozessualen Eingriffsbefugnisse hingewiesen.[1016]

4. Konsequenzen und weitere Sanktionen gegen den IT-Sachverständigen

Verstößt der IT-Sachverständige gegen die oben beschriebenen Grenzen, kann das eine Ablehnung wegen Befangenheit, den Verlust der Vergütung, eine Haftung nach § 839a BGB oder Beweisverwertungsverbote nach sich ziehen. Weitere Sanktionen gegen den Sachverständigen wären bspw. ein Ordnungsgeld wegen Versäumnis der Frist zur Abgabe bzw. Weigerung einer Absprache für eine Frist[1017] oder bei weitergehenden Eingriffen, die diese Grenze missachten, kann sich der Sachverständige ggf. sogar strafbar machen, bspw. des Betrugs[1018], der Manipulation von Beweismitteln[1019], der Verletzung von Geheimhaltungspflichten[1020] oder des Datenschutzes[1021] oder wegen sonstiger illegaler Aktivitäten (wie Hacking).

1015 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 39 ff., S. 518 ff.; Siehe zum Datenschutz bspw. auch https://svv.ihk.de/blueprint/servlet/resource/blob/4931738/c4a1f6abd219c6be92ef7a82ebfe4677/informationspflicht-gerichtssachverstaendige-data.pdf [26.3.2023]; *Werner*, NJOZ 2019, 1041 – 1046.

1016 Vertiefend dazu auch *Safferling/Rückert*, NJW 2021, 287.

1017 Weitere Ordnungsmittel ergeben sich auch bei Nichterscheinen/Nichterstattung des Gutachtens/Nichtherausgabe von Unterlagen oder bspw. wegen Ungebühr in der Sitzung.

1018 Wenn ein IT-Sachverständiger ein falsches Gutachten erstellt oder absichtlich falsche Informationen gibt, um sich oder einen Dritten zu bereichern, kann er sich des Betrugs i. S. v. § 263 StGB schuldig machen.

1019 Wenn ein IT-Sachverständiger Beweismittel wie Computerdaten oder -programme manipuliert oder verändert, um einen vermeintlich unschuldigen Angeklagten zu entlasten, kann er sich strafbar machen, vgl. §§ 303a ff. StGB.

1020 Wenn ein IT-Sachverständiger vertrauliche oder geheime Informationen an unbefugte Dritte weitergibt oder anderweitig gegen Vereinbarungen zur Geheimhaltung verstößt, kann er sich strafbar machen; vgl. auch *Farthofer*, HRRS (7/2021), S. 313 ff. zum Geheimnisverrat durch einen Sachverständigen im Zuge eines Wirtschafts- oder Cyberkriminalitätsstrafverfahrens.

1021 Wenn ein IT-Sachverständiger personenbezogene Daten ohne Erlaubnis oder Genehmigung zugänglich macht oder anders gegen die Datenschutzgesetze verstößt, kann er sich ebenfalls strafbar machen. Einen guten Überblick über das Datenschutzstrafrecht bieten z. B. https://www.dr-datenschutz.de/ein-ueberblick-ueber-das-datenschutzstrafrecht/ [7.2.2024] sowie div. Beitrage von *Basar*, vgl. etwa https://www.

Wenn der Befund unbestimmt oder das Gutachten widersprüchlich oder sonst mangelhaft ist oder die Angaben zweier Sachverständiger über die von ihnen wahrgenommenen Tatsachen oder die hieraus gezogenen Schlüsse erheblich voneinander abweichen und sich die Bedenken nicht durch Befragung beseitigen lassen, so ist ein weiterer Sachverständiger beizuziehen.

VII. Die Leitung des Sachverständigen, § 78 StPO

Aus dem eben Geschilderten verdeutlicht sich, wie wichtig die Leitung des Sachverständigen durch den Auftraggeber gem. § 78 StPO ist. Sie ist eng mit der Bestellung des Sachverständigen verbunden. § 78 StPO ist eine der wichtigsten Vorschriften und Aufgaben in Bezug auf den Sachverständigenbeweis.[1022] Nichtsdestotrotz wird sie in der Praxis allzu oft vernachlässigt.[1023] Eben diese Nichtbeachtung der Vorschrift führt in der Praxis zu dem oft beschriebenen Kontroll- und Kompetenzverlust der Richter.

Nach § 78 StPO hat der Richter die Sachverständigentätigkeit zu leiten, soweit ihm das erforderlich erscheint. Wie das geschehen soll, lässt die StPO jedoch offen.[1024] Eine Konkretisierung findet sich aber in Nr. 72 Abs. 2 RiStBV.[1025] § 78 StPO formuliert dabei eine sehr anspruchsvolle Aufgabe, die keine Demonstration von verfahrensrechtlicher Rangordnung sein soll, sondern im Dienste der Wahrheitserforschung und Überzeugungsbildung des Richters steht.[1026] Eine Leitung des Sachverständigen im Ermittlungsverfahren ist dem Richter unmöglich, wenn er ihn nicht selbst ausgewählt und bestellt hat und häufig von der Tätigkeit nicht einmal Kenntnis hat. So verliert die Vorschrift des § 78 StPO einen wesentlichen Teil ihres Sinns, wenn im Ermittlungsverfahren Staatsanwaltschaft und ihre Ermittlungspersonen den Sachverständigen auswählen und bestellen, ihm Anknüpfungstatsachen zugänglich machen und ihn als Beauftragten leiten. Die Leitungspflicht soll deshalb auch für die Staatsanwaltschaft und die Polizei gelten, gem. §§ 161a

---

bvdnet.de/wp-content/uploads/2023/07/32_BvD-399_News_2023-2_web.pdf, S. 28 ff. [7.2.2024] und die Ausführungen von *Rückert* zur DSGVO, vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 518 ff.

1022 BGHSt 45, 168, 182; BGH NStZ 1995, 282; Löwe/Rosenberg/*Krause*, § 78 Rn. 1 f.

1023 So schon bei *Sarstedt*, NJW 1968, 177, 180, der in diesem Zusammenhang unter Bezugnahme auf den Wortlaut des § 78 StPO ausführt: „Ihm sollte dies [die Tätigkeit des Sachverständigen zu leiten] öfter erforderlich erscheinen, als es bisweilen geschieht".

1024 Vgl. dagegen § 404a ZPO.

1025 Siehe auch SK-StPO/*Rogall*, § 78 Rn. 3; Meyer-Goßner/*Schmitt*, § 78 Rn. 2; Löwe/Rosenberg/*Krause*, § 78 Rn. 3; KK/*Senge*, § 78 Rn. 1.

1026 *Walter*, Sachverständigenbeweis, S. 121.

Abs. 1 S. 2, 78 StPO. Das Gericht hat in diesen Fällen jedenfalls bei der späteren Hinzuziehung des Sachverständigen in der Hauptverhandlung darauf zu achten, dass die Leitung durch die Staatsanwaltschaft entsprechend eingehalten wurde, und zu prüfen, ob das Gutachten unparteiisch und unabhängig erstellt worden ist.

Nach § 78 StPO unter Berücksichtigung der Nr. 72 Abs. 2 RiStBV erfordert die Leitung des Sachverständigen eine klare und eindeutige Auftragserteilung, die von möglichst bestimmt formulierten Beweisfragen umschrieben und begrenzt werden soll.[1027] Dadurch wird den anderen Verfahrensbeteiligten auch (nötigenfalls konkludent) mitgeteilt, dass ein Sachverständiger beauftragt wurde (s. o. bei II. 2. und 3. c)).[1028] Um diesen Anforderungen entsprechen zu können, muss sich der auftraggebende Richter mit dem Beweisthema und dem Beweisziel auseinandersetzen. Um eine unbefangene und unparteiische Gutachtenerstattung durch den Sachverständigen zu ermöglichen,[1029] hat das Gericht ferner darauf zu achten, den Auftrag objektiv und unter Vermeidung von Tendenzen zu erteilen (vgl. hierzu B. II. 2. c) dd) und ee)).

Zur Leitung gehören ebenso die Überwachung der Einhaltung der Grenzen der Sachverständigentätigkeit sowie die Erörterung bei bestehenden Unstimmigkeiten.[1030] Außerdem gehört dazu auch die Terminüberwachung des Sachverständigen. Der Auftraggeber soll mit dem Sachverständigen eine Absprache treffen, innerhalb welcher Frist das Gutachten zu erstatten ist (§ 73 Abs. 1 S. 2 StPO; vgl. auch Nr. 72 Abs. 1 RiStBV). Daraus ergibt sich eine rechtzeitige Hinweisverpflichtung des Sachverständigen, wenn voraussichtlich (Mehr-)Kosten entstehen, weil es in diesem Fall dem Auftraggeber freigestellt sein muss, die Tätigkeit des Sachverständigen einzuschränken oder zu beenden.[1031]

Will der Auftraggeber seiner Pflicht zur Leitung des Sachverständigen ordnungsgemäß nachkommen, braucht er Grundkenntnisse über die Wissenschaftsrichtung, aus deren Gebiet er den Sachverständigen heranzuziehen beabsichtigt. Daraus ergibt sich notwendig die Pflicht zur Aneignung der elementaren Grundlagen aus dem Gebiet, um die Beurteilungskriterien und

---

1027 SK-StPO/*Rogall*, Vor § 72 Rn. 61; Meyer-Goßner/*Schmitt*, § 78 Rn. 3; Löwe/Rosenberg/*Krause*, § 78 Rn. 4; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 110 ff.; *Krauß*, ZStW 85 (1973), 320, 322; *Eb. Schmidt*, Nachtrag I, § 78 Rn. 8.

1028 Siehe dazu auch *Stinshoff*, Operative Fallanalyse, S. 143.

1029 So sind die beauftragten Sachverständigen nicht immer frei von dem Ziel, das ihr Auftraggeber verfolgt; vgl. zu dieser Problematik *Eisenberg*, NStZ 2006, 368, 369; *Detter*, NStZ 1998, 52, 59.

1030 BGH v. 13.3.1985 – 3 StR 8/85, MDR 1985, 629 = NStZ 1985, 421.

1031 BayObLG v. 10.3.2004 – 3Z BR 237/03, FamRZ 2005, 225.

Schlussfolgerungen aus den Ergebnissen richtig ziehen zu können. Diese Grundkenntnis soll den Auftraggeber insb. Richter nicht überlegener machen, sondern ihm gewährleisten, sich durch Sachverständigengutachten immer abgesichert zu wähnen.

Auch hat er dafür Sorge zu tragen, dass der Sachverständige den Sachverhalt nicht rechtlich bewertet – so ist die rechtliche Wertung allein Sache des juristischen Auftraggebers.[1032]

1. Die Informationsbasis für die Sachverständigentätigkeit

Durch die Vorschrift wird das rechtliche Verhältnis zwischen dem Richter als Auftraggeber und dem Sachverständigen als Beauftragten deutlich, wonach der Richter die Arbeit des Sachverständigen „zu überwachen" hat.[1033] Der Sachverständige wiederum hat das Recht, von seinem Arbeitgeber so genau über seinen Gutachtenauftrag und seine Rechte und Pflichten bei der Gutachtenerstattung informiert zu werden, dass er ein der Beweisfrage entsprechendes und verwertbares Gutachten vorbereiten und erstatten kann.[1034] Daraus ergibt sich, dass das Gericht dem Sachverständigen die benötigten Anknüpfungstatsachen möglichst bei der Auftragserteilung von sich aus und selbstständig[1035] vollständig mitzuteilen hat.[1036] Dabei kann die Auswahl der Anknüpfungstatsachen aufgrund der Schwierigkeit bestimmter Fachgebiete und Themen für den Richter u. U. sehr herausfordernd werden.[1037] Dass dabei jedenfalls nicht der komplette Akteninhalt übergeben werden sollte, wird nun erläutert. Es kommt vielmehr auf eine fallspezifische Auswahl an. Nicht zuletzt wird so auch die Gefahr von bias minimiert (siehe dazu B. II. 2. c) ee)).

Um sich Klarheit über seinen Auftrag (und damit eine gemeinsame Kommunikationsbasis zwischen Auftraggeber und Sachverständigen) zu verschaffen, besitzt der Auftraggeber zwei Möglichkeiten: 1) Er kann den Sachverhalt, den der Sachverständige seinem Gutachten zugrunde legen soll, im Beweisbe-

---

1032 Löwe/Rosenberg/*Krause*, § 78 Rn. 6.

1033 Löwe/Rosenberg/*Krause*, § 78 Rn. 1.

1034 SK-StPO/*Rogall*, Vor § 72 Rn. 59, 61.

1035 *Krauß*, ZStW 85 (1973), 320, 322; *Kühne*, Strafprozessrecht, Rn. 866; BGHSt 18,107, 108; BGHStV 1995, S. 113; Löwe/Rosenberg/*Krause*, § 78 Rn. 2; KK/*Senge*, § 78 Rn. 2; Meyer-Goßner/*Schmitt*, § 78 Rn. 4; SK-StPO/*Rogall*, Vor § 72 Rn. 61, § 78 Rn. 10; *Barton*, Der psychowissenschaftliche Sachverständige, S. 28.

1036 BGHSt 18,107, 108; BGHStV 1995, 113; Löwe/Rosenberg/*Krause*, § 78 Rn. 2; KK/*Senge*, § 78 Rn. 2; Meyer-Goßner/*Schmitt*, § 78 Rn. 4; SK-StPO/*Rogall*, Vor § 72 Rn. 61, § 78 Rn. 10; *Barton*, Der psychowissenschaftliche Sachverständige, S. 28.

1037 Vgl. *Erb*, ZStW 121 (2009), 883, 884; *Krauß*, ZStW 85 (1973), 320, 325 f.

schluss verbindlich festlegen. Der Sachverhalt bildet die vom Sachverständigen hinzunehmenden „Anknüpfungstatsachen".[1038] Ein Beispiel ist, wenn das Gericht dem psychiatrischen Sachverständigen die Ergebnisse eines (anderen) vorbereitenden schriftlichen Sachverständigengutachtens als erwiesen vorgibt und er diese unter eines der bekannten Krankheitsbilder subsumieren muss.[1039] Wenn der IT-Sachverständige über den konkreten Sachverhalt nur wenig weiß, ergibt sich der Vorteil, leichter einen objektiven Bericht verfassen zu können.[1040] Oft stellt sich die Festlegung von Anknüpfungstatsachen jedoch als schwierig dar, v. a. wenn das Gericht aufgrund seiner fehlenden Sachkunde noch nicht überblicken kann, ob bestimmte scheinbar bewiesene Umstände sich durch eine Untersuchung durch den Sachverständigen möglicherweise in einem ganz anderen Licht präsentieren würden oder weil der Auftraggeber Schwierigkeiten hat, das Beweisthema konkret zu formulieren. Verbindliche Vorgaben würden dann den Wert des Sachverständigengutachtens nur mindern.[1041] In einem solchen Fall bleibt dann die andere Möglichkeit, 2) die Übersendung der Akten (ob auszugsweise oder komplett).[1042] Die Vor- und Nachteile der Aktenüberlassung sind deutlich: Einerseits kann der Sachverständige aus dem vollen Akteninhalt schöpfen und dabei Tatsachen verwerten, die für den Nichtfachmann bedeutungslos erscheinen[1043], andererseits besteht die Gefahr, Inhalte zu verwerten, die letztlich nicht auch Ergebnis der Hauptverhandlung werden. Die Hilfe durch den Akteninhalt ist außerdem trügerisch[1044]: So könnten sich Thesen erhärten, die sich zwar aus den Akten, nicht aber aus der Untersuchung an sich ergeben würden bzw. auf einzelne Punkte lenkt, denen gegenüber Wichtiges plötzlich vernachlässigbar erscheinen mag.[1045]

Zutreffend wird vertreten, dass die Überlassung des gesamten Akteninhalts nicht durch § 80 Abs. 2 StPO gedeckt ist,[1046] da es Ziel der Norm ist, eine unnötige Belastung und Tendenz des Sachverständigen mit und aus Informa-

---

1038 Siehe vertiefend zum Umfang auch *Walter*, Sachverständigenbeweis, S. 133.

1039 Beispiel nach *Mezger*, AcP 117 (1918), Beilageheft, S. 1 (13 f.).

1040 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 344.

1041 Vgl. dazu *Müller*, Der Sachverständige im gerichtlichen Verfahren, Rdnr. 525, 550.

1042 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 103.

1043 *Sarstedt*, NJW 68, 177 (180).

1044 *Rudolph*, Die Justiz, S. 30.

1045 *Walter*, Sachverständigenbeweis, S. 133; *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 103; *Eisenberg*, Beweisrecht, Rdnr. 1591; *Sarstedt*, NJW 1968, 177 (180).

1046 Im Einzelfall kann das aber auch geboten sein, vgl. *Lürken*, NJW 1968, 1161, 1164 f.

tionen der Ermittlung zu vermeiden.[1047] Dem ist zuzustimmen, da in den Ermittlungsakten häufig belastende Indizien enthalten sind, was die Objektivität der Sachverständigen trüben kann.[1048] So wird der Pflicht zur ordnungsgemäßen Leitung und entsprechender Aufklärung über den Sachverhalt (bzw. die Mitteilung der Anknüpfungstatsachen) ausschließlich nachgekommen, wenn dem Sachverständigen nur der Teil der Akten übergeben wird, der für das Gutachten zwingend notwendig ist.[1049] In der Praxis wird die Aufklärung des Sachverständigen allerdings oft anders gehandhabt.[1050] V. a. für die oben beschriebenen schwierigen Fälle, in denen eine selektive Aktenübermittlung nicht möglich erscheint, könnte es in jedem Fall sinnvoll sein, wenn der Sachverständige in seinem Gutachten explizit darstellt, welche Teile der Akte er berücksichtigt hat.

Dieser Grundsatz (dass dem Sachverständigen nur die Informationen übermittelt werden, die er zwingend für das Gutachten braucht) muss umso strenger überprüft werden, wenn der von der Staatsanwaltschaft bzw. seiner Ermittlungspersonen beauftragte Sachverständige Mitarbeiter der Strafverfolgungsbehörde ist. Denn ist der Sachverständige bei der ihn beauftragenden Strafverfolgungsbehörde örtlich und sachlich eingegliedert, besteht die Gefahr einer „faktischen Teilnahme" an den Ermittlungen durch Informationen im Rahmen von Flurgesprächen (vgl. auch B. V. c)). Dadurch wird die Objektivität des Gutachtens gefährdet und gegebenenfalls ein Ablehnungsgrund begründet.[1051] Derartige informelle Informationsübermittlungen sind von außen kaum nachvollziehbar und nachzuweisen.[1052] So sind zwar Vorab- und Zwi-

---

[1047] *Kühne*, Strafprozessrecht, Rn. 866; *Tondorf/Tondorf*, Psychologische und psychiatrische Sachverständige im Strafverfahren, Rn. 242; *Eisenberg*, Beweisrecht der StPO, Rn. 1591; *Peters*, S. 342; *Dippel*, in: FS-E. Müller, S. 125, 138 f.; SK-StPO/*Rogall*, Vor § 72 Rn. 64 Fn. 256, § 78 Rn. 10; *Lürken*, NJW 1968, 1161, 1164 f.; *Sarstedt*, NJW1968, 177, 180; zu dieser Praxis siehe auch *Barton*, Der psychowissenschaftliche Sachverständige, S. 28; *Zwiehoff*, Das Recht auf einen Sachverständigen, S. 308 f.; *Wellmann*, Der Sachverständige in der Praxis, Rn. 214; a. A. *Ligges*, Die Stellung des Sachverständigen, S. 144; *Kube/Leineweber*, Polizeibeamte als Zeugen und Sachverständige, S. 69; *Rauch*, NJW 1968, 1173 (1775); RG JW 1895, 517 (519 f.).

[1048] Vgl. auch *Kühne*, Rn. 866; *Tondorf/Tondorf*, Psychologische und psychiatrische Sachverständige im Strafverfahren, Rn. 242 in Bezug auf die Staatsanwaltschaft. Siehe dazu auch in diesem Teil, B. II. 2. c) ee).

[1049] *Krauß*, ZStW 85 (1973), 320, 322; Meyer-Goßner/*Schmitt*, § 78 Rn. 4, § 80 Rn. 3 geht dagegen von einer regelmäßigen Überlassung des gesamten Akteninhalts aus, wobei aber auch er eine routinemäßige Überlassung des gesamten Akteninhalts ablehnt.

[1050] *Dippel*, in: FS-E. Müller, 125 (138) m. w. N.; *Rauch*, NJW 1968, 1173 (1175).

[1051] Siehe *Stinshoff*, Operative Fallanalyse, S. 137 ff., S. 146.

[1052] Das belegt auch der Eindruck, der im Rahmen der Akteneinsicht von der Verfasserin gewonnen wurde: Hier konnte eine Diskrepanz zwischen Beweisfrage und Untersuchungsumfang festgestellt werden. Da eine Änderung bzw. Ausweitung der

schenberatungen mit dem Auftraggeber bei der Vorbereitung des Gutachtens zulässig, vgl. Nr. 72 Abs. 2 RiStBV, und durchaus auch wünschenswert (siehe auch schon bei B. II. 3. c) aa)).[1053] Das kann aber auch dazu führen, dass die anderen Verfahrensbeteiligten die Gutachtenerstattung und ggf. vorgenommenen Einschränkungen, Schwerpunktsetzungen oder Änderungen der Beweisfragen nicht mehr nachvollziehen können, wenn diese „Flurgespräche" nicht verschriftlich werden. Hier bedarf es einer nachvollziehbaren Dokumentation der Kommunikation zwischen Auftraggeber und Sachverständigem – nicht zuletzt, um einem Vorwurf der Befangenheit zu begegnen.

In Fällen, in denen das Gericht nicht durch fehlende Sachkunde gehindert ist, alle notwendigen Anknüpfungstatsachen mitzuliefern, kann das Gericht dem Sachverständigen zunächst aufgeben, bestimmte Tatsachen, die der Sachverständige als Grundlage seines Gutachtens benötigt (gegebenenfalls alternativ) zu unterstellen. Nachdem sich das Gericht dann die erforderliche Sachkunde verschafft hat, kann es die Beweisaufnahme bzgl. der Anknüpfungstatsachen anschließend nachholen.

Nach § 80 StPO kann der Sachverständige auch von sich aus die notwendigen Informationen zum Verständnis des Beweisthemas „anstoßen" (siehe oben bei B. VI. 2.).

2. Achtung der Weisungsfreiheit des Sachverständigen

Die Leitung des Sachverständigen aus § 78 StPO betrifft jedoch nicht die fachliche Durchführung des Auftrags, denn diesbezüglich ist der Sachverständige grds. keiner Leitung und Weisung ausgesetzt. Bei der Entscheidung über die Art der Informationsbeschaffung und die Methodenwahl[1054] auf dem Weg zum Gutachten ist der Sachverständige weitgehend (Einhaltung der Wissenschaftlichkeit und der Standards der forensischen Informatik nach dem aktuellen Stand der Technik, dazu sogleich) frei.[1055]

Beweisfrage oder etwaige Gespräche nicht dokumentiert waren, konnten die Änderungen nur durch ein Gespräch mit dem jew. IT-Sachverständigen nachvollzogen werden. Aus dem Gutachten und dem Untersuchungsauftrag allein war das nicht möglich.

[1053] Z. B. darüber, ob der Umfang der Unterlagen eine Beantwortung der beabsichtigten Beweisfragen dem Grunde nach zulässt oder welche weiteren Unterlagen der Sachverständige hierzu benötigt.

[1054] BGHSt 44, 26 (33) = BGH BeckRS 1998, 30007833; BGH NStZ 1997, 610; BGH NStZ 1999, 630 (632).

[1055] BGH v. 8.8.2002 – 3 StR 239/02, NStZ 2003, 101; BGH StV 1992, 27 Nr. 3 [K]; BGH StV 1997, 610; SK-StPO/*Rogall*, § 78 Rn. 1; *Boetticher/Nedopil/Bosinski/Saß*, NStZ 2005, 57; Meyer-Goßner/*Schmitt*, § 78 Rn. 6; KMR/*Neubeck*, § 78 Rn. 4.

Wie die richterliche Überprüfung der angewendeten Methoden, Schlussfolgerungen und Erfahrungssätze im Rahmen der Beweiswürdigung nach § 261 StPO auszusehen hat, wird an späterer Stelle im 4. Teil erörtert.

Im Rahmen seiner Leitungspflicht hat das Gericht also darauf zu achten, dass es den Sachverständigen bei seiner Ausführung lediglich unterstützt, z. B. indem es für das Erscheinen der zu untersuchenden Person sorgt oder einen Beschluss zur Einholung von weiteren Informationen bzw. Anknüpfungstatsachen erwirkt.[1056]

3. Vorrang der Methodik mit bekannter Funktionalität

An dieser Stelle muss ein Vorgriff in Bezug auf die Beweiswürdigung der IT-Sachverständigenaussagen im Hinblick auf die unterschiedlichen Grade der Richtigkeitswahrscheinlichkeiten der angewendeten Methodiken und damit der unterschiedlichen Beweiskraft der dadurch ermittelten Tatsachen vorgenommen werden.

Aus der Weisungsfreiheit und der dadurch bedingten freien Methodenwahl des IT-Sachverständigen ergibt sich ein Spannungsverhältnis zu der Pflicht, dass das Gericht bei mehreren zur Verfügung stehenden IT-forensischen Untersuchungsmethoden die jeweils zuverlässigere, also diejenige mit einer höheren Richtigkeitswahrscheinlichkeit wählen muss. Diese Pflicht leitet Rückert[1057] aus den Grundsätzen der erschöpfenden und lückenlosen Beweiswürdigung und § 244 Abs. 2 StPO ab. Dieses Spannungsverhältnis wird insbesondere dann deutlich, wenn der IT-Sachverständige eine nicht oder weniger geeignete Untersuchungsmethode wählt (wie „Blackbox-Tools“) und insbesondere gegen wissenschaftliche Standards verstößt.

Deshalb hat der BGH die Freiheit des Sachverständigen eingeschränkt und das Weisungsrecht nach § 78 StPO zumindest darauf erstreckt, dass der Sachverständige angewiesen werden kann, wissenschaftliche Mindeststandards einzuhalten und auch überlegene, wissenschaftlich anerkannte Untersuchungsmethoden zu verwenden.[1058]

Letzteres lässt sich auch aus der Wertung des § 244 Abs. 4 S. 2 StPO entnehmen.[1059] Dementsprechend kann – und muss – der Auftraggeber den beauftragten Sachverständigen anweisen, die forensischen Mindeststandards (siehe später im 3. Teil, B. III. 5.) einzuhalten und eine Untersuchungsme-

---

1056 Löwe/Rosenberg/*Krause*, § 78 Rn. 2.

1057 Digitale Daten als Beweismittel im Strafverfahren, S. 690 f.

1058 BGH NJW 1999, 2746 (2751); MüKo-StPO/*Trück* § 78 Rn. 4; SK-StPO/*Rogall*, § 78 Rn. 5.

1059 Vgl. MüKoStPO/*Trück*, § 78 Rn. 4.

thode mit höherer wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit zu verwenden, wenn für die konkret durchgeführte forensische Untersuchung eine solche zur Verfügung steht (siehe dazu später im 4. Teil, A. III. 4. b) cc)). Diese Richtigkeitswahrscheinlichkeit kann nur dann wissenschaftlich fundiert angegeben werden, wenn die genaue Funktionalität (also bspw. die bei einem statistischen Datenverarbeitungsverfahren verwendeten Annahmen[1060]) bekannt ist. So umfasst die Leitungsbefugnis nach § 78 StPO auch die Angabe, eine Untersuchungsmethode bzw. Datenanalysemethode zu verwenden, bei der die Funktionalität bekannt ist, wenn diese mindestens gleich geeignet ist wie andere Methoden, bei denen die Funktionalität nicht bekannt ist. Das wird v. a. im Anwendungsfall von sog. Blackbox-Tools relevant (siehe dazu im 4. Teil, A. III. 4. b) cc) (2) (f)).

4. Checklisten

Sinnvolle Anhaltspunkte für die Staatsanwaltschaft für die Leitung und speziell die Auftragserteilung finden sich bspw. in der „Rostocker Checkliste für den Auftraggeber zum Gutachtenauftrag und zu Fehlerquellen in schriftlichen Gutachten".[1061] Danach soll die Staatsanwaltschaft den Gutachter in einem Auftragsschreiben u. a. darauf hinweisen, in dem Gutachten darzustellen, auf welche Tat oder Taten sich die Begutachtung beziehen soll und aufgrund welcher Anknüpfungstatsachen das Gutachten erstellt werden soll. Außerdem wird der Gutachter aufgefordert, vor der Auftragsannahme zu prüfen, ob er zur Beantwortung der Beweisfrage ausreichend sachkundig ist. Weiter sollte er darauf hingewiesen werden, dass er sich einer juristischen Wertung zu enthalten hat.[1062] Die Idee einer o. g. Forschungsgruppe aus Technikerinnen und Juristinnen, die sich der Formulierung der Grenzen der Sachverständigentätigkeit im Untersuchungsauftrag annimmt, könnte sich auch einer Erarbeitung solcher „Checklisten" speziell für den Bereich der forensischen Informatik annehmen.

1060 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 691.

1061 *Schläfke/Häßler/Schnoor/König/Rebernig/Auer/Feger*. Diese Checkliste wurde mit Förderung des Sozialministeriums und in Abstimmung mit dem Justizministerium Mecklenburg-Vorpommern zum Auftragsschreiben der Staatsanwaltschaft anlässlich eines wissenschaftlichen Symposiums in Rostock-Warnemünde entwickelt und bezieht sich in erster Linie auf Schuldfähigkeitsgutachten. Vgl. auch *Stinshoff*, Operative Fallanalyse, S. 147 Fn. 1153.

1062 Eine vollständige Darstellung findet sich auch in *Tondorf/Tondorf*, Psychologische und psychiatrische Sachverständige im Strafverfahren, Rn. 246.

VIII. Zusammenfassung „Die deutsche StPO und der Sachverständigenbeweis“

Die Ergebnisse der Darstellungen im Kapitel „Die deutsche StPO und der Sachverständigenbeweis“ lassen sich wie folgt zusammenfassen:

Die Rolle des IT-Sachverständigen als bestmögliches und sachnächstes Beweismittel, wenn es um die Einführung von digitalen Spuren in ein Strafverfahren geht, ist entscheidend von der Rolle des Zeugenbeweises abzugrenzen, insb. von Ermittlungspersonen. Das ergibt sich sowohl aus den unterschiedlichen Rechten und Pflichten, die sich an die jeweilige Stellung der Beweisperson knüpfen, als auch aus weiteren Konsequenzen wie bspw. der Begründung eines Ablehnungsrechtes. Dabei kommt es immer auf den Einzelfall an. Auch lässt sich die IT-Sachverständigentätigkeit nicht pauschal kategorisieren und im Hinblick auf eine erforderliche besondere Sachkunde beurteilen. Jedenfalls dürfte diese aber – auch aus Sicht der aktuellen Rechtsprechung und der Forensiker selbst – in den allermeisten Fällen bei der Auswertung von IT-Asservaten notwendig sein; nicht zuletzt, weil die forensische Informatik noch „in Kinderschuhen“ steckt, bisher nicht als standardisiert beurteilt werden kann und auch aufgrund der Besonderheit der Technologie universell und in einem ständigen Wandel ist. Durch die regelmäßige Zusammenarbeit mit IT-Sachverständigen können die Verfahrensbeteiligten das hier so oft betonte Grundwissen im Bereich der forensischen Informatik ausbauen und festigen, indem sie sich vertieft mit den einzelnen Punkten und Grenzen der IT-Sachverständigengutachten im Rahmen der §§ 78 und 261 StPO auseinandersetzen (müssen).

Zum aktuellen Stand der Handhabung der forensischen Informatik bzw. digitaler Spuren durch die deutsche Strafverfolgung und der damit einhergehenden Unsicherheit müssen die Strafrichter ihren eigenen Kenntnissen regelmäßig misstrauen und einen IT-Sachverständigen als bestmögliches und sachnächstes Mittel beauftragen, um die „forensische Wahrheit“ voran zu treiben.

Aufgrund der hier erarbeiteten These, dass wohl in den allermeisten Fällen die Erstellung eines IT-Sachverständigengutachtens beauftragt werden muss, um die zugrundeliegenden Informationen der digitalen Spuren optimal bewerten und würdigen zu können, wird im Anschluss auch über eine Verteilung der (oft sehr hohen) Kostenrechnungen der Sachverständigengutachten in Anbetracht des Verhältnismäßigkeitsgrundsatzes und der Waffengleichheit nachgedacht werden müssen.

Um der oft gepredigten Gefahr des Kontrollverlustes der Richter entgegnen zu können (v. a. immer dann, wenn es um neue forensische Wissenschaften in Strafgerichten geht), muss die Leitungspflicht des § 78 StPO ernstgenommen werden; das gilt auch, wenn die Sachverständigen lediglich von den Richtern

bestätigt und in die Hauptverhandlung übernommen werden und die eigentliche Zusammenarbeit und Kommunikation zwischen Staatsanwaltschaft bzw. ihren Ermittlungspersonen und IT-Sachverständigen bereits im Ermittlungsverfahren passiert. Die Richter müssen überprüfen, dass auch eine Leitung i. S. d. § 78 StPO von den Auftraggebern im Ermittlungsverfahren eingehalten wurde. Aus der Leitungspflicht nach § 78 StPO unter Berücksichtigung der Nr. 72 Abs. 2 RiStBV ergibt sich die Beauftragung eines objektiven und besonders sachkundigen Sachverständigen, eine klare und eindeutige Auftragserteilung, die von möglichst bestimmt formulierten Beweisfragen umschrieben und begrenzt werden soll. Hier gilt es, eine gemeinsame interdisziplinäre Kommunikationsbasis zu schaffen. Auch muss sichergestellt werden, dass sich der IT-Sachverständige im Rahmen seiner vorgegebenen Grenzen bewegt. Diese bestehen sowohl in den Beweisfragen als auch in den Regeln der Grundrechtseingriffe für Strafverfolgungsbehörden. Um der Pflicht aus § 78 StPO ausreichend nachkommen zu können, bedarf es nicht zuletzt einer Aneignung elementarer Grundlagen der forensischen Informatik durch die Auftraggeber.

Auch wird an die Cyberstrafverteidigung appelliert, ihr Grundwissen im Bereich der IT aufzustocken, um die Fragen zu stellen, auf die es bei der Würdigung von digitalen Spuren ankommt. Dabei soll ihnen v. a. ein umfangreiches Akteneinsichtsrecht in das vorbereitende schriftliche Gutachten und in die zugrundeliegenden Arbeitsunterlagen der IT-Sachverständigen (sowohl in die verarbeiteten Beweisdaten, die verwendeten Tools als auch die angewendeten Erfahrungssätze) helfen.

Um das gewährleisten zu können, sind die IT-Sachverständigen dazu angehalten, ihre Gutachten im Hinblick auf die syllogistische Struktur der Urteilsfindung so aufzubauen, dass sie die verschiedenen erarbeiteten Aussagekategorien, die Anknüpfungstatsachen und die zugrundeliegenden Unsicherheiten aufschlüsseln und transparent machen. Dafür und für die damit einhergehende Kommunikation mit den juristischen Auftraggebern benötigen auch die IT-Sachverständigen ein gewisses juristisches Gespür.

Auf die – (eingeschränkte) weisungsfreie – Arbeit der IT-Forensiker und die damit einhergehenden Besonderheiten für das Beweisrecht soll im nächsten Kapitel eingegangen werden.

3. Teil

Die Beschaffung des Tatsachenstoffes: Die forensische Informatik

Nach der Festlegung des Beweisthemas verlagert sich der Schwerpunkt des Prozesses auf die Tätigkeit des IT-Sachverständigen „im Labor". In Bezug auf die (allgemeine) forensische Vorgehensweise stellt auch die forensische Informatik keine Ausnahme dar: Datenträger bzw. andere Geräte werden bei einer Durchsuchung sichergestellt. Die Auswertung erfolgt dann „im Labor" durch den IT-Sachverständigen. Nur wenn es triftige Gründe für die Annahme gibt, dass die Unterstützung von Spezialisten bereits bei der Sicherstellung der Geräte erforderlich ist, werden die Ermittler schon bei der Beschlagnahme von den forensischen Informatikern beratend (unter Beachtung der Abgrenzung zur Tätigkeit von Ermittlungspersonen und eines Ablehnungsrechts, siehe Zweiter Teil, B. V. 2. c)) unterstützt. Die forensische Tätigkeit durch die IT-Sachverständigen richtet sich nach dem jeweiligen zu beantwortenden Beweisthema in Form der drei Aussagekategorien – Ermittlung von Befundtatsachen (dritte Aussagekategorie), Mitteilung, von welchen Erfahrungssätzen er dabei ausgegangen ist, (erste Aussagekategorie), und Mitteilung, durch welche Schlussfolgerungen er die Verknüpfung seiner Untersuchung mit der Beweisfrage ableitete (zweite Aussagekategorie). Und schließlich erfolgt noch die Anfertigung des vorbereitenden schriftlichen Gutachtens bzw. die mündliche Gutachtenerstattung vor Gericht. Die gefundenen digitalen Spuren werden zusammen mit dem vorbereitenden schriftlichen Gutachten (und den dazugehörenden Arbeitsunterlagen) an den Auftraggeber übergeben. Der wiederum kann die ermittelten Ergebnisse (wie Befunde) sichten und zusammen mit dem Gutachten für die (weitere) Ermittlungsarbeit bzw. Sammlung des Tatsachenstoffes für die Urteilsfindung nutzen.[1]

Während der forensischen Tätigkeit steht der Auftraggeber lediglich i. S. d. §§ 78, 80 StPO zur Ergänzung von Informationen oder Klärung bei auftretenden Unklarheiten bei der Auslegung des Beweisthemas zur Verfügung.[2]

---

[1] Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 344.

[2] *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 138.

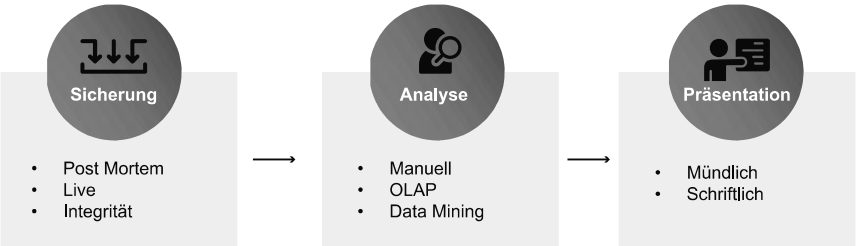


Abbildung 6: „Möglicher Ablauf einer IT-forensischen Untersuchung“[3]

Für den IT-Sachverständigen ergeben sich dabei einige Herausforderungen, die überwunden werden müssen: Aus der Abgekoppeltheit von der physischen Welt und der Universalität der Technologie folgen massenhaft Daten, die strukturlos, nicht deutlich erkennbar und oft nur temporär (auf Hardware, Software oder im Internet) aufzufinden sind. Diese müssen entdeckt, gesichert, gefiltert und gerichtsverwertbar ausgewertet werden. Dabei am Wichtigsten ist wohl die Authentizität, Integrität und Glaubwürdigkeit der Information, die aus den Daten gewonnen wird und als Beweis Eingang ins Strafverfahren finden soll. Darauf hinwirkend, muss das Ergebnis der Datenauswertung überprüfbar (transparent, wiederholbar, reproduzierbar) und verfassungskonform zustande gekommen (siehe im 2. Teil, B. VI.) sein, es muss nachvollziehbar erklärt werden können (umfassend genaue Dokumentation während des gesamten Auswertungsprozesses der Daten bzw. deren Veränderungen) und es muss präzise und korrekt sein (es darf nicht auf bloßen Annahmen beruhen). Darüber hinaus sieht sich die forensische Informatik vor weiteren finanziellen Herausforderungen: So bedarf es für die Auswertung sowohl kostenintensiver Spezial-Software als auch Hardware für die Aufbereitung großer Datenmengen sowie Kosten für das sogenannte Beweismittelnetzwerk. Wie die Entwicklung der zurückliegenden Jahre deutlich gemacht hat, steigen die Kosten insbesondere für Softwarelizenzen, zum Teil durch die Monopolstellung einiger Anbieter begründet, sukzessive erheblich an.[4] Auch permanent zunehmende Datenmengen von täterseitiger PC-Hardware, Sicherungen von Cloud-Systemen und exponentielle Zunahme von Daten auf mobilen Systemen (Smartphones, Tablets) führen zu erheblichen, kostenintensiven Speicherbedarfen sowohl bei den Ermittlungsbehörden als bei privaten IT-Sachverständigenbüros. Da digitale Daten unter die Asservatenregelung fallen, muss zum Teil von einer mehrjährigen Sicherung – mit einhergehender

[3] Vgl. *Heinson*, IT-Forensik, S. 72.

[4] https://www.bremische-buergerschaft.de/drs_abo/2023-02-08_Drs-20-1766_b85d6.pdf S. 11 [26.6.2023].

Bindung der Speicher – ausgegangen werden. Vor dem Hintergrund der kurzen technischen Innovationszyklen muss eine moderne forensische Informatik mit diesen schnellen Entwicklungsschritten gleichauf sein.

Neben diesen vielen Herausforderungen muss man allerdings auch unbedingt den großen Vorteil digitaler Spuren erkennen. Zunächst „gehen sie nicht verloren", wenn sie einmal forensisch sauber gesichert sind, und können dann beliebig oft kopiert werden. Zudem können bereits gelöschte bzw. überschriebene[5] Spuren (v. a. im Vergleich zu analog geschriebenen) trotzdem gelesen und ausgewertet werden (zumindest in der Theorie).[6] Nicht zuletzt bietet die Technologie aufgrund ihrer Universalität ein unheimliches Potential, ermittlungsrelevante Informationen zu finden.[7]

A. Die forensische Wissenschaft

Das Attribut forensisch stammt vom lateinischen Wort forum (Marktplatz) ab. Früher war der Marktplatz der Schauplatz von Gerichtsverfahren. Mit forensisch wird jeder Bezug zu Aspekten des Rechtssystems bezeichnet. Die forensische Wissenschaft (häufig abgekürzt als „Forensik") ist demnach die Anwendung wissenschaftlicher Methoden auf Fragen des Rechtssystems, etwa zur Untersuchung und Verfolgung von Straftaten.[8]

Im üblichen Sprachgebrauch verleiht das Attribut wissenschaftlich vielen Sachverhalten eine hohe Glaubwürdigkeit. Im gleichen Zug kann man einen Vorgang leicht diskreditieren, wenn man ihn als unwissenschaftlich bezeichnet. Viele Menschen, auch viele Wissenschaftlerinnen, verbinden Wissenschaft mit Wahrheit. Das hat gefährliche Auswirkungen für die tatrichterliche Überzeugung i. S. d. § 261 StPO – v. a. wenn die Tatrichter das Gutachten des IT-Sachverständigen ohne eigene Plausibilitätskontrolle als „wahr" unterstellen und ihrer Urteilsfindung zugrunde legen.

---

[5] Vgl. zur Vorgehensweise von Speichercontrollern bei SSD's in *Dewald/Freiling*, Forensische Informatik, S. 270; *Regan*, The Forensic Potential of Flash Memory; *Wie u. a.*, Reliably Erasing Data from Flashbased Solid State Drives. Der Controller sucht sich stets neue unbenutzte Speicherblöcke (Flash Translation Layer). Die Dateninhalte der alten Speicherblöcke liegen immer noch auf der SSD vor.

[6] Die Analyse kann jedoch durch anderes erschwert werden, wie bspw. proprietären Hardwarestandards bei SSD's, vgl. *Dewald/Freiling*, Forensische Informatik, S. 270; *Billard/Hauri*, Making sense of unstructured flash-memory dumps oder spezielle Dateisysteme, die forensisch oft noch wenig analysiert sind, vgl. *Dewald/Freiling*, Forensische Informatik, S. 270; *Zimmermann u. a.*, Forensic Analysis of YAFFS2.

[7] Vgl. bspw. nur *Dodge*, Feminist Theory (2018) Vol. 10 (3), S. 303 ff.

[8] *Heinson*, IT-Forensik, S. 16 m. w. N.

Die Untersuchung möchte im Anschluss an Freiling/Dewald[9] dazu beitragen, unter den Verfahrensbeteiligten ein differenziertes Verständnis für Wissenschaft zu wecken, nämlich Wissenschaft als einen nie endenden Prozess, der nur eingeschränkt etwas mit einer universellen Wahrheit zu tun hat (unabhängig davon, ob diese überhaupt existiert, vgl. dazu auch im 2. Teil, B. I. 1.).

I. Die wissenschaftliche Methode

Ausgangspunkt der Arbeit eines forensischen Wissenschaftlers[10] ist regelmäßig immer eine juristische Fragestellung, deren Beantwortung durch die wissenschaftlichen Methoden einer Disziplin unterstützt werden soll.

Mit Wissenschaft wird die Methode bezeichnet, mit der der Mensch versucht, die Welt um sich herum zu beschreiben und zu verstehen. Dabei wird versucht, allgemeine Regeln und Prinzipien aufzustellen, die die Welt erklären, wie Naturgesetze in der Physik, etwa der Zusammenhang zwischen Masse, Beschleunigung und Geschwindigkeit. Derartige Regeln können auf verschiedene Arten hergeleitet werden. Ein häufiger Ansatz besteht darin, dass wiederkehrende Muster in der Umwelt wahrgenommen und diese in Form allgemeiner Regeln, Erfahrungssätze (erste Aussagekategorie), beschrieben werden. Ein zentraler Bestandteil der wissenschaftlichen Methode sind Hypothesen. Hypothesen sind Aussagen, deren Gültigkeit untersucht werden kann, z. B. durch Experimente.[11] Das Aufstellen von Hypothesen ist ebenso wichtig wie ihre Überprüfbarkeit. Schwerpunkt dabei ist die Falsifizierbarkeit einer Hypothese.[12] Es muss also ein Experiment existieren, dessen möglicher Ausgang die Hypothese gleichwahrscheinlich widerlegen kann. In der Realität ist es unmöglich, ein Prinzip als allgemeingültig nachzuweisen. Man kann höchstens daran scheitern, es zu widerlegen. Solange ein Prinzip trotz vielfacher Anstrengung nicht widerlegt wurde, wird es akzeptiert und gilt i. d. S. innerhalb der wissenschaftlichen Gemeinschaft als richtig. Diese Art von systematischem Zweifel garantiert eine möglichst hohe Objektivität wissenschaftlicher Erkenntnisse. Insbesondere in forensischen Wissenschaften werden häufig Zusammenhänge als richtig dargestellt, wie etwa die Behauptung, dass die Kugel am Tatort von einer bestimmten Waffe abgefeuert wurde. Als (forensischer) Wissenschaftler muss man sich jedoch immer vor

---

9 *Dewald/Freiling*, Forensische Informatik, S. 19 f.

10 Vgl. zum Begriff der forensischen Wissenschaft und der Kriminalistik vgl. *Dewald/Freiling*, Forensische Informatik, S. 23 ff. In der zugrundeliegenden Untersuchung wird der Begriff der forensischen Wissenschaft verwendet.

11 Dabei können quantitative (messbare), aber auch qualitative Daten (die durch bloße Beobachtung entstehen) hervorgebracht werden.

12 *Popper*, Logik der Forschung; *Popper*, Vermutungen und Widerlegungen.

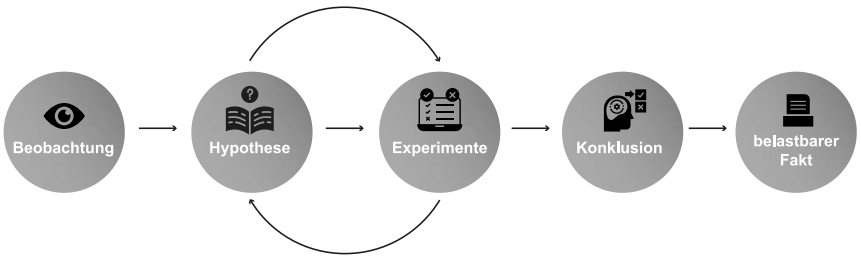


Abbildung 7: „Die wissenschaftliche Methode“

Augen halten, dass man diese Tatsache im Sinne wissenschaftlicher Arbeit nicht beweisen kann. Nur wenn man wiederholt und mit adäquaten Methoden daran scheitert, den Zusammenhang zu widerlegen, kann man schließlich zur Überzeugung gelangen, dass die Kugel tatsächlich durch die Waffe abgefeuert wurde.[13] In anderen Kontexten kann man durch bestimmte Tests die Wahrscheinlichkeit bestimmter Sachverhalte beziffern, etwa bei der DNA-Analyse. Aber selbst eine hohe Wahrscheinlichkeit bestätigt nicht die Richtigkeit einer Hypothese (siehe zur Quantifizierbarkeit unten bei B. III. 3. a)).

Ein ebenso wichtiger Bestandteil der wissenschaftlichen Methode ist, dass die Hypothesen und Experimente nachvollzogen und durch die Fachgemeinschaft begutachtet werden können. Die Präsentation von wissenschaftlichen Ergebnissen (Hypothesen und Experimente) geschieht i. d. R. auf wissenschaftlichen Konferenzen oder in Fachzeitschriften.[14] Dabei werden die Resultate vor der Veröffentlichung durch unabhängige und anerkannte Experten bewertet. Ergebnisse, die diesen Auswahlprozess überstanden haben („begutachtete Publikation“), werden in den Fundus des akzeptierten Wissens aufgenommen. Die Veröffentlichung dient dazu, die Ergebnisse der Fachgemeinschaft dauerhaft zugänglich zu machen. Veröffentlichungen, die keinem Begutachtungsprozess unterliegen (wie etwa „Whitepapers“ oder Einträge in Diskussionsforen im Internet), haben einen deutlich geringeren wissenschaftlichen Wert. Der Stand der Technik ist das Produkt einer gemeinsamen Überzeugung, die im fachlichen Austausch entsteht. Diese reflektierte Überzeugungskraft ist ein wesentlicher Faktor, warum Wissenschaftlern hohe Glaubwürdigkeit zugemessen wird. Schließlich geht es vor Gericht auch darum, die Verfahrensbeteiligten bzw. die Tatrichter von einem gewissen Sachverhalt zu überzeugen.[15]

---

13 Vgl. Beispiel aus *Dewald/Freiling*, Forensische Informatik, S. 21.

14 Vgl. zur Notwendigkeit des peer-review-Verfahrens in der forensischen Informatik in *Sunde*, Forensic Science International: Digital Investigation (2020) Vol. 35, S. 1.

15 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 20.

Zwar analysieren forensische Wissenschaftler eher als dass sie experimentieren. Dennoch ergeben sich immer wieder auch Beweisfragen, die der Sachverständige beantworten muss, die die Natur forensischer Wissenschaften an sich oder eine spezielle forensische Wissenschaft betreffen. Außerdem helfen grundsätzliche Untersuchungen in einem Fach (etwa zu mechanischen Wirkungsbeziehungen in der Physik oder zur prinzipiellen Lösbarkeit algorithmischer Probleme in der Informatik) dabei, den Einsatz der jeweiligen wissenschaftlichen Methoden für forensische Zwecke zu verbessern.[16] Auch im Rahmen der Gutachtenerstattung des IT-Sachverständigen haben die Methoden der Informatik eine wichtige Rolle: Beispiele sind die Bereiche Datenbanken, maschinelles Lernen, Softwaretechnik, Bildverarbeitung und Betriebssysteme. Das Gebiet der forensischen Informatik ist demzufolge sehr umfassend.[17]

In der Rechtsprechung wird der Wissenschaft und dem Sachverständigenbeweis ein hoher Stellenwert beigemessen. Deshalb ist es umso gefährlicher, wenn Richter Gutachten im Rahmen der §§ 261, 267 StPO einfach übernehmen, ohne auf die wissenschaftliche Methodik einzugehen – v. a. bei „neuen" (noch) nicht standardisierten Methodiken wie die der forensischen Informatik (siehe dazu Vierter Teil, A. III. 4. b) cc) (2) (b)) – und ohne zu prüfen, ob sie eingehalten wurden. In Bezug auf die forensische Informatik fällt noch erschwerend hinzu, dass eine gewisse „Technikhörigkeit" unter den Verfahrensbeteiligten besteht.[18]

Jedoch müssen die Verfahrensbeteiligten v. a. dahingehend sensibilisiert werden, dass bei der forensischen Informatik (noch) nicht standardisierte forensische Methoden angewendet werden und größtenteils nicht zum gesicherten Erfahrungswissen gezählt werden können, und deren Vorgehensweise und die dadurch produzierten Ergebnisse als richtig unterstellt werden können. Im Umgang mit dem IT-Sachverständigenbeweis ist darauf besonders Acht zu geben, denn für die forensische Wissenschaft gilt der wissenschaftliche Wandel noch stärker als für andere Wissenschaften (siehe dazu im 2. Teil, A. III.). Auch ergibt sich für digitale Beweismittel die weitere Besonderheit, dass die zugrundeliegenden Annahmen der Erfahrungssätze und der Datenverarbeitungs- und -analysemethoden bzw. deren Richtigkeit im Bereich der Befundermittlung zum Teil überhaupt nicht nachprüfbar sind (Stichwort „Blackbox-

16 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 23.

17 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 15; *Casino et al.*, Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews, 2022 Vol. 10, S. 25468: Von Networks Traffic Analysis, über Multimedia, Cloud, Social Networks, Blockchain, IoT, und File Systems.

18 So etwa *Mysegades*, Software als Beweiswerkzeug, S. 5, der einerseits vom „Eindruck der Neuartigkeit und Unverlässlichkeit" und andererseits von einem „blinden Vertrauen in die Technologie" spricht.

Tools“). Also ganz im Gegenteil zur unterstellten „Wahrheit“ der dabei produzierten digitalen Beweismittel muss zunächst des Öfteren davon ausgegangen werden, dass es sich vllt. sogar um Beweismittel von geringerem Wirklichkeits- bzw. Beweiswert handelt (vgl. zu den Auswirkungen der Digitalisierung auf den Wahrheitsbegriff auch den 2. Teil, B. I. 1.).

Dass es nicht nur im Bereich der forensischen Informatik methodische Schwächen gibt, ist allgemein bekannt. So sollten forensische Wissenschaften vor Gericht ganz allgemein wissenschaftlicher sein als sie es bisher sind.[19] Der Anspruch sollte sein, im Rahmen des Sachverständigenbeweises nur auf gesicherte wissenschaftliche Erkenntnisse zurückzugreifen.[20] Um das dem Gericht für eine eigene Plausibilitätskontrolle zugänglich zu machen, muss auf den Grundsatz der Nachvollziehbarkeit und Transparenz bei der Begutachtung geachtet werden.

II. Der Grundsatz der Nachvollziehbarkeit und Transparenz der Forensik

Wenn man es auf den Punkt bringen möchte, könnte man auch sagen, dass es bei der Beauftragung eines IT-Sachverständigen darum geht, zwar dort Kompetenzen (in Bezug auf die Sachverhaltsermittlung) abzugeben, wo die eigene Sachkunde fehlt, aber dennoch die Vorgehensweise nachvollziehen zu können, um die Autorität und Kontrolle der Entscheidungsfindung zu behalten. Gerichtspersonen müssen in ihrer Beweiswürdigung die einzelnen Schritte (verschriftlicht in der Urteilsbegründung) nachvollziehen können, auf denen der Sachverständige seine Beurteilung aufbaut. Die Pflicht zur Transparenz staatlicher Entscheidungen ergibt sich aus dem Rechtsstaats- und dem Demokratiegebot in Art. 20 Abs. 1 – 3 GG. So führt bspw. Martini überzeugend aus, dass es als Teil der Rechtssicherheit zum Selbstverständnis des demokratischen Rechtsstaates gehört, jede Form staatlicher Machtausübung vorhersehbar und rekonstruierbar auszugestalten.[21] Daraus folgend hat sich der Grundsatz der Nachvollziehbarkeit und Transparenz der Begutachtung entwickelt, die sich auch in den beweisrechtlichen Anforderungen bei der Beweiswürdigung wiederfinden.[22]

---

19 *Garrett*, Autopsy of a Crime Lab.

20 Vgl. bspw. BGH 21.2.1978 NJW 78, 1207, wozu nicht die Parapsychologie gehöre.

21 *Martini*, Blackbox Algorithmus, S. 68; vgl. auch *ders.*, NVwZ-Extra 2014, 1 (9); *Nink*, Justiz und Algorithmen, S. 331 f.; *Mysegades*, Software als Beweiswerkzeug, S. 175 ff.

22 BGHSt 45, 164 (178 ff.); auch bereits BGHSt 14, 30 (31 ff.); 36, 286 (287); 37, 231 (232); 37, 397 (399); *Eisenberg*, Beweisrecht der StPO, Rn. 1812 f.; *Göppinger*, Forensischen Psychiatrie, Bd. 2, S. 1498 ff.; *Witter*, Grundriss der gerichtlichen Psy-

Die Antworten der Experten auf die jeweilige Beweisfrage bilden nicht selten eine wichtige Entscheidungsgrundlage für die Tatrichter im Rahmen des § 261 StPO. So sind an wissenschaftlich begründete Gutachten unabdingbare Anforderungen zu stellen. Der BGH fordert dahingehend eine Begutachtung in Form von wissenschaftlichen Mindeststandards, dass der Begutachtungsprozess nachvollziehbar dargestellt und transparent ist und dass weiter zugrunde gelegte, relevante Hypothesen genannt werden. Denn Antworten auf Hypothesen stellen in jedem Falle Wahrscheinlichkeitsaussagen dar und sind mit Unsicherheiten behaftet. Den Verfahrensbeteiligten müssen diese bekannt sein. Die Einhaltung des methodischen Ablaufs muss nachgewiesen werden.[23]

Zwar wird es einem Juristen kaum möglich sein, ohne Hinzuziehung einer weiteren sachkundigen Person ein Gutachten zweckmäßig zu überprüfen, sofern ihm die Sachkunde für das einschlägige Fachgebiet fehlt. Dennoch besitzt er ein nicht zu unterschätzendes Instrument, um Begründungsmängel sichtbar zu machen: Ebenso wie die Urteilsbegründung den Tenor durch eine lückenlose logische Struktur stützen muss,[24] ist es notwendig, dass das Sachverständigengutachten eine solche Struktur aufweist. Das ergibt sich bereits daraus, dass die Argumentation des Gutachtens, sofern sie für das Gerichtsurteil relevant werden soll, sich in das syllogistische Netzwerk eingliedern lassen muss. Dem Grundsatz der Nachvollziehbarkeit und Transparenz der Begutachtung wird daher auch von der Rechtsprechung ein hoher Stellenwert zuerkannt.[25] Das Gericht muss schon deshalb am Nachvollziehen der Begutachtung interessiert sein, weil nur so der Transfer der Überzeugung des Sachverständigen auf die Überzeugung des Richters in Form eines rationalen Konsenses erfolgen kann.[26] Aber auch für den Anwalt gewinnt die Überprüfung der syllogistischen Struktur Bedeutung, indem für ihn auf diese Weise schwache Punkte in der Begründung deutlicher zutage treten können, die sich dann möglicherweise durch ergänzende Befragung einer sachverständigen Person zu einer vernichtenden Kritik an den Ergebnissen nutzen lassen.[27]

Das Erfordernis der Nachvollziehbarkeit und Transparenz kann bspw. mithilfe von Logik und Argumentation, Lehrbüchern und Anleitungen, Schemata und Standards eingehalten werden. So ergeben sich aus diesem Grundsatz die

---

chologie und Psychiatrie, S. 251 ff.; *Wolfslast*, MKrim 1979, 79; *Venzlaff*, in: Psychiatrische Begutachtung, S. 67 (77 ff.).

23 Vgl. *Köller/Nissen/Rieß/Sadorf*, Probabilistische Schlussfolgerungen, S. 57 m. w. N.

24 Dazu später bei § 267 im 4. Teil, A. III. 5.

25 Vgl. nur BGHSt 45, 164 (178 ff.).

26 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 170.

27 So wohl oft, wenn Wahrscheinlichkeiten im Gutachten angegeben werden.

Mindeststandards der forensischen Informatik, wie die Integrität und Authentizität von digitalen Spuren (vgl. dazu später bei B. III. 5.).

B. Die forensische Informatik (als Teil der klassischen Forensiken)

Auch in der forensischen Informatik geht es in der heutigen Wissenschaft immer nachdrücklicher um die Einhaltung des Grundsatzes der Nachvollziehbarkeit und Transparenz; das wird aktuell in den Medien v. a. im Hinblick auf einen Versuch der Handhabung der KI diskutiert.[28]

Wie Freiling/Dewald in ihrem Werk „Forensische Informatik"[29] zeigen, lässt sich die Informatik ohne Weiteres in die Tradition der klassischen forensischen Wissenschaften reihen. Zwar verlangt die Untersuchung digitaler Spuren manchmal neue Methoden, aber die Informatik ist keineswegs eine neue forensische Wissenschaft, für die andere Gesetze als bei den übrigen forensischen Wissenschaften gelten. Fast alle Prinzipien, die man in der klassischen Forensik für physische Spuren entwickelt hat, lassen sich auch auf digitale Spuren anwenden. Die vermeintlichen Unterschiede bei der Behandlung digitaler Spuren führen lediglich zu einer Betonung bestimmter forensischer Prinzipien, die bei der Betrachtung analoger Spuren nur am Rande vorkommt.[30]

Die forensische Informatik[31] umfasst in ihrer aktuellen Form eine Vielzahl unterschiedlichster Aufgaben. So z. B. die möglichst schnelle Bewertung eines Sicherheitsvorfalls anhand erster erhobener Daten[32] zur Planung der weiteren Untersuchung des Vorfalls; die Anfertigung einer forensischen Kopie physischer Speichermedien unter Einsatz spezieller Hard- und Software; die Umgehung von Schutzmechanismen digitaler Systeme, um eine Erhebung von Daten zu ermöglichen; die Extraktion kryptographischer Schlüssel aus Hauptspeicherabbildern zur Erhebung verschlüsselter Daten; die Rekonstruktion gelöschter Daten anhand von Dateisystem Metadaten oder durch Filecarving; die Erstellung von Timelines untersuchter Systeme, also die Erfas-

---

28 Vgl. die aktuelle Diskussion um die KI, siehe nur https://www.zeit.de/2023/27/ki-gesetz-eu-chatgpt-regulierung [26.6.2023] oder https://www.zeit.de/kultur/2023-05/kuenstliche-intelligenz-angst-zukunft-geoffrey-hinton-james-bridle [27.6.2023].

29 Insb. *Dewald/Freiling*, Forensische Informatik, S. 55 ff.

30 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 55.

31 Die forensische Informatik als forensische Wissenschaft, vgl. vertiefend dazu *Dewald/Freiling*, Forensische Informatik, S. 91 f.

32 Durch Techniken der Live-Analyse, vgl. *Carrier*, File System Forensic Analysis, S. 13 ff.

sung einer zeitlichen Abfolge vergangener Ereignisse auf dem untersuchten System.[33]

I. Definition der „forensischen Informatik“ und ihre Aufgaben

Diese forensische Wissenschaft wird mit den verschiedensten Begriffen betitelt: U. a. „forensische Informatik“[34], „IT Forensik“[35], „Computer Forensik“[36], „Iuk Forensik“[37] oder „Digitale Forensik“[38]. In dieser Arbeit soll anschließend an Freiling/Dewald[39] der Begriff der „forensischen Informatik“ verwendet werden und in Bezug auf das Strafverfahren verstanden werden.

Laut der UNODC[40] kann die forensische Informatik als der Zweig der forensischen Wissenschaft beschrieben werden, der sich mit der Ermittlung und Analyse von Spuren befasst, die in Computersystemen gefunden werden.[41]

Freiling/Dewald definieren allgemein die forensische Informatik als die Anwendung wissenschaftlicher Methoden der Informatik auf Fragen des Rechtssystems. Insbesondere stellt die forensische Informatik Methoden zur gerichtsfesten Sicherung und Verwertung digitaler Spuren bereit.[42] Die Betonung des wissenschaftlichen Aspekts verdeutlicht die Anforderung an zugrundeliegende verlässliche und objektive Methodiken. Eine besondere Rolle spielt die Unterfütterung des Gebietes mit theoretischen Grundlagen der klassischen Forensik und ein tieferes Verständnis der Art von Spuren, die in der forensischen Informatik untersucht werden.[43] Die Autoren unterscheiden dabei zwei Aspekte der forensischen Informatik und teilen die relevanten Me-

---

33 Beispiele vgl. *Dewald/Freiling*, Forensische Informatik, S. 91.

34 https://www.cybercrime.fau.de/ [28.6.2023].

35 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/IT-Forensik/it_forensik_node.html [26.6.2023].

36 *Geschonneck*, Computer Forensik.

37 https://www.polizei.bayern.de/kriminalitaet/kriminaltechnik/003760/index.html [29.6.2023].

38 https://www.cb.hs-mittweida.de/studienangebote-der-fakultaet/allgemeine-und-digitale-forensik-bachelor/ [26.6.2023]; https://www.hs-albsig.de/studienangebot/masterstudiengaenge/digitale-forensik/ [26.6.2023].

39 Forensische Informatik, S. 93.

40 United Nations Office on Drugs and Crime, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf S. 159 [26.6.2023].

41 Frei übersetzt: „the branch of forensic science concerned with the recovery and investigation of material found in digital and computer systems“.

42 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 93.

43 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 93.

thoden in zwei Gebiete: Einerseits umfasst die forensische Informatik im engeren Sinne eine sehr fokussierte Menge an Fragestellungen und Methoden, welche sich im Kern mit der Herstellung von Assoziationen, befasst. Andererseits soll es die forensische Informatik im weiteren Sinne geben, die den gesamten Prozess der Durchführung einer digitalen Ermittlung, wie z. B. die Suche nach digitalen Spuren, das Rekonstruieren gelöschter Daten, der Umgang mit großen Speichermengen etc. umfasst. Der Bereich der forensischen Informatik i. w. S. integriert viele Themenbereiche der Informatik, die bisher unabhängig voneinander agierten, wie bspw. die Massendatenanalyse (data mining, big data), das Netzwerk-Fingerprinting, Reverse Engineering, die Hauptspeicheranalyse, Seitenkanalanalyse und Datenschutztechniken.[44]

In der Praxis deutet sich eine thematische Aufteilung der eingesetzten Techniken in drei Unterbereiche an, die sich an der Flüchtigkeit der betrachteten digitalen Spuren orientiert: 1) Sicherung und Analyse persistenter Spuren, also vornehmlich Festplatten. In Anlehnung an die englischsprachige Terminologie wird dies oft als die Tot-Analyse (dead analysis) oder Post-Mortem-Analyse bezeichnet. 2) Sicherung und Analyse von flüchtigen Spuren im weiteren Sinne, also der Inhalte von Hauptspeicher, Caches etc. (zumeist im Rahmen einer Live-Analyse). Und 3) Sicherung und Analyse von flüchtigen Spuren im engeren Sinne, meist Spuren im Netz. Dieser Teilbereich wird häufig als Netzwerkforensik bezeichnet.[45]

Das UNODC (2013) wiederum unterteilt die forensische Informatik in drei Kategorien, je nach Ursprung der digitalen Spuren: 1) Die Datenträgerforensik konzentriert sich auf das Sammeln und Analysieren von Desktop-Computern und Laptops, die sich in Privathaushalten oder in Unternehmen befinden. 2) Bei der Mobilfunkforensik geht es um die Erfassung und Analyse von Mobilgeräten (mit geringem Stromverbrauch). 3) Und unter Netzwerkforensik versteht man das Sammeln und Analysieren von digitalen Spuren aus Online-Diensten und Cloud-Speichern sowie das Sammeln von Informationen über den Netzwerkverkehr.[46]

Egal wie man es kategorisiert, für die hiesige Untersuchung ist bedeutsam, dass es bei der Tätigkeit des IT-Sachverständigen auf dem Gebiet der forensischen Informatik um die Beantwortung von Fragen bzgl. der forensischen

---

[44] Einen Überblick darüber, wie viele verschiedene Bereiche es in der forensischen Informatik gibt und wo derzeit die Forschungsschwerpunkte liegen, bekommt man bspw. hier: *Casino et al.*, Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews, 2022 Vol. 10, S. 25468: Von Networks Traffic Analysis, über Multimedia, Cloud, Social Networks, Blockchain, IoT, und File Systems.

[45] Vgl. auch *Rieß*, in: Dewald/Freiling, Forensische Informatik, S. 175 ff.

[46] *Sunde*, Non-technical Sources of Errors, S. 14 f.

Auswertung und Präsentation digitaler Spuren geht. Wie eingangs bereits kurz erwähnt, stellen digitale Spuren den tatsächlichen Ausgangspunkt in der Außenwelt dar, bspw. als elektronische Dokumente, digitale Bilder, Mails, Chatprotokolle, genauso wie verschlüsselte Informationen oder Spuren von Angriffen auf Netzwerke. Sie bedürfen einer digitalforensischen, kunstgerechten Erhebung, Auswertung und Interpretation, um aus ihnen strafverfolgungsrelevante Erkenntnisse zu gewinnen. Im Folgenden soll nun auf digitale Spuren im forensischen Prozess eingegangen werden.

II. Digitale Spuren im forensischen Prozess

Eine Spur wird als ein hinterlassenes Zeichen angesehen.[47] Eine Spur ist dabei jedes Objekt, das ein Argument plausibler macht. Eine Spur ist danach ein Gegenstand, zusammen mit einer Reihe von dokumentierten Behauptungen oder Annahmen über diesen Gegenstand. Diese Behauptungen beschreiben im Wesentlichen die Herkunft der Spur, etwa den Fundort und die Zeit des Auffindens.[48] In der realen Welt kann nahezu alles zur Spur werden.[49] Etwas wird zur Spur, wenn es eine Beziehung zum untersuchten Sachverhalt aufweist.[50] Spuren sind deshalb so wichtig bei Ermittlungen, denn es ist nahezu unmöglich, Handlungen auszuführen, ohne irgendwelche Spuren zu hinterlassen.[51]

In der digitalen Welt basieren diese Spuren auf Daten, welche in Computersystemen gespeichert oder übertragen worden sind.[52] Aufgrund der Besonderheit der Universalität können diese (massenhaften) Daten ganze Persönlichkeitsprofile bis hin zu einem digitalen Zwilling darstellen, weshalb auch das Interesse der Strafverfolgungsbehörden daran so groß ist. Digitale Spuren sind zunächst immer auch physische Spuren, z. B. die Magnetisierung auf der Oberfläche einer Festplatte, elektromagnetische Wellen auf einem Datenkabel oder der Ladezustand von Speicherzellen im Hauptspeicher. Insofern können

---

47 Das Wort „Spur" kommt ursprünglich aus dem Altgermanischen und bedeutet dort Tritt oder Fußabdruck, vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 29.

48 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 29 f.

49 Im Handbuch von *Groß/Geerds*, Handbuch der Kriminalistik umfasst der Abschnitt zu Spurenkunde und deren Untersuchung mehr als 200 Seiten. Die Palette reicht von Blut, Haaren und Sekreten über Wasser, Boden, Vegetation, Luft und Gas bis hin zu Metall, Kunststoff, Holz und Textilien.

50 *Kirk*, Crime Investigation, S. 6.

51 *Kirk*, Crime Investigation, S. 1 ff.; *Dewald/Freiling*, Forensische Informatik, S. 30.

52 Vgl. *Casey*, Digital Evidence and Computer Crime (2004), S. 12. Zur Unklarheit dieser Definition vgl. *Dewald/Freiling*, Forensische Informatik, S. 55.

alle Begriffe und Prinzipien der klassischen Forensik direkt auf digitale Spuren angewendet werden.[53]

Der größte Teil von digitalen Spuren fällt nach wie vor auf Datenträgern wie klassischen Festplatten oder USB-Sticks (Flash-Speicher) an.[54] Das erklärt auch, warum die Datenträgerforensik ein gut erforschter Bereich ist und sich bereits einige Standards etabliert haben.[55] Deshalb soll sich in dieser Arbeit auf dieses Gebiet konzentriert und Beispiele aus diesem Bereich gebracht werden. Nichtsdestotrotz bestehen in vielen anderen Gebieten der forensischen Informatik noch große Lücken, die geschlossen werden müssen und deren Bedeutung – auch für juristische Verfahrensbeteiligte – immer weiter zunimmt.[56]

Beispiele für digitale Spuren, die auf Datenträgern relevant sein können sind u. a. Inhalte der Partitionstabelle, die über den weiteren Inhalt der Festplatte Aufschluss geben können. Nachdem diese Daten nicht mit bloßem Auge erkennbar sind, benötigt man Methoden (Werkzeuge z. B.), um auf sie zuzugreifen. Diese müssen in einer „forensisch sauberen" Art und Weise ausgewertet werden. Das bedeutet bspw., dass die Spuren nicht modifiziert bzw. etwaige Modifikationen dokumentiert werden.[57]

1. Information und Träger

Allgemein unterscheidet man bei Spuren zwischen (Spuren-)Information und (Spuren-)Träger. Die Information ist die Bedeutung der Spur, also das, was sie aussagt. Der Träger ist diejenige Materie, die diese Bedeutung trägt. Ein Beispiel für den Unterschied zwischen Information und Träger ist ein Brief, der am Tatort gefunden wird. Träger sind das Papier und die Tinte, aus denen der Brief besteht. Die Information ist (u. a.) die auf dem Brief codierte Bedeutung der Schriftzeichen.[58]

In der klassischen Forensik wirkt die Unterscheidung zwischen Spurenträger und Spureninformation etwas „künstlich", weil eine starke Verbindung

---

53 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 56; siehe vertiefend zu den Begriffen und Prinzipien der klassischen Forensik auch *Dewald/Freiling*, Forensische Informatik, S. 19 ff.

54 Vgl. zum Unterschied zwischen klassischen Festplatten und modernen Speichermedien auch *Dewald/Freiling*, Forensische Informatik, S. 267 ff., S. 269.

55 Vertiefend dazu *Dewald/Freiling*, Forensische Informatik, S. 278 ff.

56 Vgl. zu aktuellen Forschungsfeldern auch *Casino et al.*, Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews, 2022 Vol. 10, S. 25468.

57 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 305.

58 Beispiel aus *Dewald/Freiling*, Forensische Informatik, S. 31.

zwischen Träger und Information besteht.[59] Das kann am Beispiel des Erpresserschreibens verdeutlicht werden: Im Wesentlichen ist die Bedeutung der geschriebenen Worte (also die Spureninformation) für den Fall relevant. Mit welcher Schreibmaschine, mit welcher Tinte oder auf welchem Briefpapier der Brief geschrieben wurde erscheint vllt. zunächst nebensächlich. Der Spurenträger kann jedoch weitere Informationen enthalten, etwa die Form der (Hand-)Schrift, die benutzt wurde, um die Spur einer Person oder einer Schreibmaschine zuzuordnen. Auch kann auf der Rückseite der Briefmarke die DNA des Absenders im Speichelrückstand gefunden werden.[60]

Bei digitalen Spuren reduziert man die Spureninformation meist auf die diskrete Repräsentation der gemäß eines bestimmten Codierungsschemas (wann man eine Eins und wann man eine Null liest) auf dem Spurenträger gespeicherten Daten.[61] Das Codierungsschema ist dabei regelmäßig gleich im Spurenträger (wie Festplatte oder RAM-Chip) „mitverbaut". Durch diese Abstraktion wird die Bindung zwischen Spurenträger und Spureninformation extrem zerbrechlich: Die Spureninformation kann nämlich theoretisch auf einem beliebigen Spurenträger gespeichert werden. Das korrespondiert mit der oben beschriebenen Besonderheit der IT, der Abgekoppeltheit von der physischen Welt (vgl. im 2. Teil, A. III.), v. a. dahingehend, dass man in der digitalen Welt Daten „perfekt kopieren"[62] und an allen möglichen Orten speichern kann.

Die schwache Verbindung von Spurenträger und Spureninformation im Falle von digitalen Spuren verdeutlicht den Unterschied zwischen beiden Konzepten: Der Spurenträger ist das „Speichermedium", die Spureninformation ist die auf dem Speichermedium „gespeicherte" Information. Bei der Reduktion auf digital (also als Bits) codierte Informationen abstrahiert man von vielen weiteren Informationen, die der Spurenträger enthält.[63] Für die forensische Untersuchung ist es jedoch wichtig, den Spurenträger nicht zu vernachlässigen, da er auch Informationen mitteilen kann, die über den gespeicherten „Tatinhalt" hinausgehen können. Durch die Beschränkung auf die (digital codierte) Spureninformation verstärkt man die Gefahr, dass man mit der Abkehr vom Spurenträger unendlich viele Blickrichtungen ausschließt, die weitere Spureninformationen tragen könnten. Hätte man bspw. schon in den 1960er Jahren alle Spuren „digitalisiert" und die Spurenträger vernichtet,

---

59 Vgl. dazu auch *Heinson*, IT-Forensik, S. 21; das ergeht auch aus *Neuhaus/Artkämper*, Kriminaltechnik und Beweisführung im Strafverfahren, S. 25 ff.

60 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 31 f.

61 Weitere Beispiele auch bei *Meier*, Digitale Forensik im Unternehmen, S. 15 f., S. 22.

62 Ohne die Möglichkeit, Original und Kopie später unterscheiden zu können.

63 *Dewald/Freiling*, Forensische Informatik, S. 57.

dann wären alle DNA-Spuren verloren gegangen, weil die Bedeutung dieser Spurenart zu der Zeit noch unbekannt war. Die Betrachtung digitaler Spuren verleitet dazu, ausschließlich in digitalen Dimensionen zu denken und die Bedeutung und die Einflüsse der physischen Welt auf diese Spuren zu vernachlässigen. Die digitale Welt wird oftmals als „geschlossenes System" wahrgenommen. Die implizite Annahme lautet dabei, dass der Austausch zwischen digitaler Welt und nicht-digitaler Welt nur über wohldefinierte Schnittstellen geschieht. Es gibt aber deutlich mehr Übergänge in die digitale Welt als nur die Tastatur des Computers, v. a. im Bereich der Multimediaforensik wird deutlich, wie sich physische Phänomene direkt in digitalen Spuren niederschlagen, die mit entsprechenden Techniken ausgewertet werden können (vgl. Beispiele oben im 2. Teil, A. IV.).[64]

2. Die Entstehung digitaler Spuren

Wie entstehen diese digitalen Spuren?

Zwar gibt es in der digitalen Welt eine Zerteilbarkeit von Materie, die die Grundlage für den physischen Transfer in der realen Welt bildet, nicht im selben Maße (immerhin werden Ladungen und Magnetisierungspotentiale hin und hergeschoben) und damit auch keine Anwendung des Locard'schen Austauschprinzips.[65] Übertragung von Materie ist jedoch nur eine Art von Transfer, die im Rahmen einer Handlung erfolgen kann. Die andere Art der Übertragung ist die Übertragung von Mustern: Diese Art der Übertragung findet in der physischen Welt immer dann statt, wenn Information von einem Objekt zum anderen übertragen wird. Dieser Vorgang hat eine offensichtliche Analogie in der digitalen Welt, wo der Austausch von Informationen (Dateien, E-Mails etc.) eine so zentrale Rolle spielt. Im Prinzip ist jede Datenverarbeitung Musterübertragung.

Aber nicht nur zwischen Rechnern werden Informationen ausgetauscht, auch innerhalb eines einzelnen Rechners werden Informationen zwischen den Objekten im Speicher getauscht.[66]

---

64 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 63.

65 Zur Theorie des Transfers bei physischen Spuren siehe auch *Dewald/Freiling*, Forensische Informatik, S. 47 m. w. N.

66 Beispiele für solche Übertragungen in der digitalen Welt sind etwa folgende Operationen: Maschineninstruktion im Prozessor, zum Beispiel: mov eax, ebx Zuweisung in einer Programmiersprache, zum Beispiel: x := y Kopieroperation auf einem Computer, zum Beispiel in einem Kommandofenster (Shell): copy file1. txt file2. Txt, Kopieroperationen über das Netz, zum Beispiel in einem Kommandofenster: scp file1. txt user@host. de:/, vgl. *Dewald/Freiling*, Forensische Informatik, S. 62.

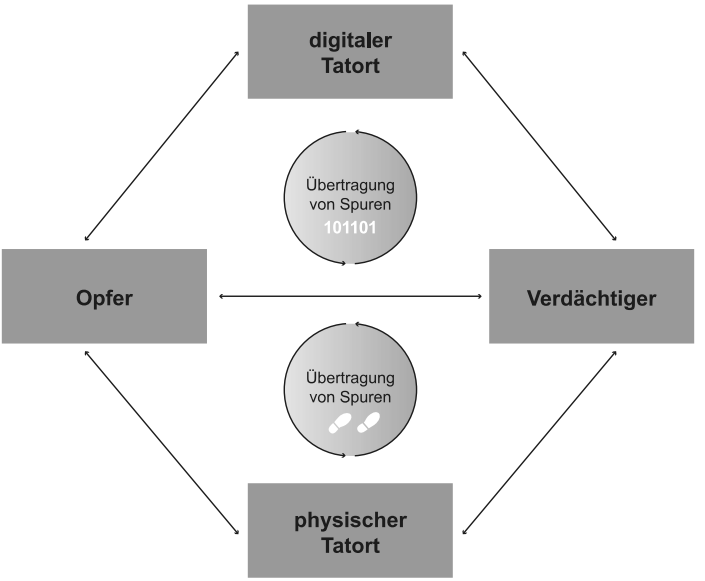


Abbildung 8: „Der digitale Tatort“

Konsequenterweise erweitert Casey[67] das ursprüngliche Austauschprinzip von Locard um einen digitalen Tatort, in dem ein Austausch von digitalen Spuren stattfinden kann.

Diese Gegenüberstellung verdeutlicht aber auch, dass ein digitaler Austausch von Spuren einhergehen kann mit einem physischen Austausch von Spuren, etwa wenn ein Schalter oder eine Taste physisch betätigt und dadurch Software gestartet wird, oder wenn (wie im Beispiel der Multimediaforensik) Umgebungseinflüsse durch entsprechende Sensorik die Spurenentstehung beeinflusst.[68] Das verdeutlicht noch einmal mehr, dass auch der Spurenträger als Ermittlungsansatz nicht vernachlässigt werden sollte. In diesem Zusammenhang muss der IT-Sachverständige jedoch die (rechtlichen) Grenzen seiner Tätigkeit im Hinblick auf die zu beantwortende Beweisfrage beachten (siehe dazu im 2. Teil, B. VI.).

67 *Casey*, Digital Evidence and Computer Crime (2011), S. 17.

68 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 64 f.; *Heinson*, IT-Forensik, S. 21.

3. Eigenschaften digitaler Spuren

Schon bei der Sicherung, während der forensischen Auswertung und auch später bei der Würdigung digitaler Beweise muss den jeweiligen Eigenschaften digitaler Spuren Rechnung getragen werden, wobei viele dieser Eigenschaften einerseits Parallelen zu Eigenschaften von Spuren der klassischen Forensik haben, andererseits aber ganz neue Herausforderungen bei der Verwendung als Beweismittel im Strafverfahren mit sich bringen. Die Eigenschaften digitaler Spuren kann man wie folgt klassifizieren: Flüchtigkeit, Technische Vermeidbarkeit, Manipulierbarkeit, Kopierbarkeit, Semantik.[69]

a) Flüchtigkeit

Wie oben beschrieben, richtet die Praxis z. T. die thematische Aufteilung der forensischen Informatik und der eingesetzten Techniken an der Flüchtigkeit der betrachteten digitalen Spuren aus (siehe bei B. I.). Die Klassifizierung nach Flüchtigkeit ist aus Sicht der forensischen Informatik nützlich, da, wie in der klassischen Forensik, Spuren je nach Flüchtigkeit unterschiedliche Vorgehensweisen und Techniken zur Sicherung und Analyse erfordern (dazu gleich bei III. 1.). Flüchtigkeit bezieht sich einerseits auf den Spurenträger (d. h. die Art und Weise, wie Daten abgespeichert werden), andererseits auch auf die Geschwindigkeit der Datenverarbeitung. Generell können dabei drei Arten der Flüchtigkeit unterschieden werden: 1) Persistente Spuren sind Spuren, die über einen vergleichsweise großen Zeitraum ohne Stromzufuhr erhalten bleiben. Sie entstehen typischerweise auf Festplatten, CD/DVDs, Solid-State-Speichern (USB-Sticks, CF-/SD-Karten etc.) und Magnetbändern. Derartige Spuren können nahezu beliebig lange nach der Tat analysiert werden, ohne Gefahr zu laufen, dass Daten mit der Zeit verloren gehen. 2) Von flüchtigen Spuren im weiteren Sinne (bzw. „semi-persistent“) ist die Rede, wenn die Spuren mit einer entsprechenden Stromzufuhr dauerhaft gespeichert werden können, bei unterbrochener Stromzufuhr aber nur kurze Zeit erhalten bleiben. Typische Vertreter sind Daten im Hauptspeicher (RAM) eines Rechners. Diese Spuren müssen entweder im laufenden Betrieb analysiert werden oder es muss zur späteren Analyse eine Kopie der Daten auf einem persistenten Datenträger erstellt werden. 3) Flüchtige Spuren im engeren Sinne sind Spuren, die im laufenden Betrieb und trotz dauerhafter Stromzufuhr nur temporär vorhanden sind. Beispiele sind Netzwerkdaten oder Inhalte von Prozessor-

---

[69] *Dewald/Freiling*, Forensische Informatik, S. 65 ff.; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 21 ff.; *Meier*, Digitale Forensik im Unternehmen, S. 24; *Mason/Seng*, Electronic Evidence, S. 23 f.; *Labudde et al.*, Forensik in der digitalen Welt, S. 9.

registern. Diese Spuren müssen entweder im laufenden Betrieb analysiert werden, oder sie werden aufgezeichnet und auf einem persistenten Datenträger gespeichert. Bspw. kann durch das Mitschneiden von Netzwerkverkehr eine Protokolldatei der transportierten Daten über einen gewissen Zeitraum angefertigt werden.[70]

Dabei ist für den Grundsatz der Nachvollziehbarkeit und Transparenz (A. II.) sowie die Integrität und Authentizität (B. III. 5.) zu berücksichtigen, dass die flüchtigen Daten mit Zeitverlauf verschwinden oder sich inhaltlich verändern können. Mit Änderung der Daten verändert sich auch der Informationsgehalt. Daten bilden als Beweismittel daher einen Informationsstand stets nur zu einem ganz bestimmten Zeitpunkt ab (deshalb sind „Zeitstempel" auch so wichtig in einem Strafverfahren, siehe dazu bei B. III. 5. f) aa)).[71]

b) Technische Vermeidbarkeit

Bei der Betrachtung von Spuren in Dateisystemen ist zu beobachteten, dass die Veränderungen bestimmter Daten dazu führen können, dass das System nicht mehr richtig funktioniert, so sind z. B. Verweise auf Datenblöcke im Dateisystem wichtig, denn ohne sie wären die Inhalte einer Datei nicht auffindbar. Diese Daten werden als (strikt/partiell)[72] essentiell bezeichnet. Andere Daten, wie etwa der eigentliche Dateiinhalt, können eine nahezu beliebige Form haben, ohne dass dies das Systemverhalten entscheidend beeinflussen würde.[73] Man kann den Begriff der essentiellen Daten sogar noch konzeptionell verallgemeinern und unterscheiden zwischen technisch vermeidbaren und technisch unvermeidbaren Spuren.[74] Technisch vermeidbare Spuren sind Spuren, die um ihrer selbst willen erzeugt werden. Sie liegen meist als Inhaltsdaten in Form von Dateien vor und gehören zu den nicht-essentiellen Daten im Dateisystem. Sie sind nicht ausschlaggebend für das Funktionieren des Systems. Die Entstehung solcher Spuren kann lokal i. d. R. durch eine Änderung

---

70 *Dewald/Freiling*, Forensische Informatik, S. 66 f.

71 Siehe auch vertiefter zur Flüchtigkeit bei *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 23.

72 Aufbauend auf *Carrier*, File System Forensic Analysis formalisierten *Freiling/Gruhn*, What is Essential in Digital Forensic Analysis? IMF (2015), S. 40 den Begriff der essentiellen Daten und entdeckten zwei Varianten in Bezug auf eine vom System bereitzustellende Funktionalität (z. B. Dateien abzuspeichern): *Strikt essentielle Daten* sind für alle betrachteten Systeme essentiell, sie sind also der Kern dessen, was die Funktionalität ausmacht (wie Blockverweise in Dateisystemen). *Partiell essentielle Daten* sind nur für manche Systeme essentiell, für andere nicht.

73 *Carrier*, File System Forensic Analysis; *Dewald/Freiling*, Forensische Informatik, S. 67 f.

74 *Dewald/Freiling*, Forensische Informatik, S. 68.

der Systemkonfiguration eingeschränkt oder gänzlich unterbunden werden. Beispiele dafür sind Log-Dateien und auch Daten, die im Rahmen einer Vorratsdatenspeicherung anfallen (auch wenn der Benutzer selbst nicht in der Lage sein wird, ihre Erzeugung zu verhindern). Technisch unvermeidbare Spuren sind solche, die unweigerlich anfallen und daher nicht durch einfache Änderungen an der Konfiguration eines Systems vermieden werden können. Eine Veränderung technisch unvermeidbarer Spuren ist grds. nicht durch die Bordmittel des Betriebssystems erreichbar. Beispiele hierfür sind gelöschte Dateien im Dateisystem, alte Stackframes im Hauptspeicher oder Inhalte des DNS-Caches.[75]

Manipulationen technisch unvermeidbarer Spuren sind mit einem deutlich höheren Aufwand verbunden als die Manipulation nicht-essentieller Daten.[76] Insofern existiert eine Analogie zwischen technisch unvermeidbaren digitalen Spuren und mikroskopischen physischen Spuren. Diese Beobachtung kann bei der Einschätzung des Beweiswertes gesicherter Spuren helfen. So sind aus Sicht der Strafverfolgungsbehörden besonders technisch unvermeidbare Spuren interessant und haben einen höheren Beweiswert als technisch vermeidbare Spuren. Letztgenannte gelten als weniger glaubwürdig, weil, wie bereits oben angesprochen, Inhaltsdaten ganz leicht geändert werden können (bspw. Kommunikationsdaten wie etwa WhatsApp-Chat-Nachrichten). Technisch unvermeidbare Spuren benötigen jedoch eine besondere Expertise bei der Sicherung und Analyse.[77] Ein Grund mehr, der für die Beauftragung eines IT-Sachverständigen spricht, wenn es um die Erlangung hochwertiger digitaler Beweismittel geht (Zweiter Teil, A. IV.).

c) Manipulierbarkeit

Unter die Argumentationen, die für einen IT-Sachverständigen als sachnächstes und bestmögliches Beweismittel sprechen, fallen auch die Ausführungen im Hinblick auf die Eigenschaft der Manipulierbarkeit von Daten.[78]

Wenn man die Betrachtung digitaler Spuren auf die Spureninformation reduziert, dann können digitale Spuren prinzipiell leicht manipuliert werden. Wie bereits aus den vorherigen Unterkapiteln zur „Flüchtigkeit“ und „techni-

---

75 *Dewald/Freiling*, Forensische Informatik, S. 68.

76 Weil die Manipulationen unter Umständen zunächst wieder rückgängig gemacht werden müssen, bevor das System benutzt werden kann. Vgl. auch *Schneider/Wolf/Freiling*, Forensic Science International: Digital Investigation (2020) Vol. 32, No. 300924.

77 *Dewald/Freiling*, Forensische Informatik, S. 68 f.

78 Siehe vertiefter zur Manipulierbarkeit bei *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 23; *Mysegades*, Software als Beweiswerkzeug, S. 57 f.

schen Vermeidbarkeit“ deutlich wurde, kann das sowohl absichtlich als auch unabsichtlich geschehen. Die Manipulation digitaler Spuren hinterlässt auf der Ebene der digitalen Spureninformation nicht notwendigerweise sichtbare Zeichen.[79] Ein praktisch relevantes Beispiel[80] ist die Manipulation von Chatverläufen in Messengerdiensten wie WhatsApp. Es ist mithilfe von Applikationen wie „FakeWhats“[81] sogar für jeden halbwegs technisch versierten Laien möglich, optisch auf dem Bildschirm eines der „beteiligten“ Smartphones nicht erkennbare Manipulationen an Chatverläufen vorzunehmen und sogar ganze Chatverläufe künstlich zu erzeugen. Andererseits wäre die technisch „perfekte“, also (auch) an den Daten im Speicher des Smartphones, nicht erkennbare Manipulation nur äußerst schwierig zu bewerkstelligen und eine forensische Untersuchung der Daten selbst kann solche Manipulationen mit hoher Wahrscheinlichkeit ausschließen bzw. aufdecken.[82]

Eine Person, die Spuren nicht nachvollziehbar manipulieren möchte, muss jedoch immer sehr viele Annahmen über die Umgebung vornehmen, egal ob in der physischen oder der digitalen Welt.[83]

---

[79] Als Beispiel für die Manipulation digitaler Spuren kann ein Rechner betrachtet werden, der mittels einer Live-CD bootet. Die Live-CD greift nicht auf die Festplatte des Rechners zu, sondern operiert ausschließlich von einer RAM-Disk. Mit einem entsprechenden Werkzeug (Hexeditor) wird anschließend ein einzelnes Bit auf der Festplatte verändert. Daraufhin wird der Rechner heruntergefahren und die Live-CD aus dem Laufwerk entfernt. Diese nicht (direkt) nachvollziehbare Manipulation von Spuren ist im Bereich der klassischen Forensik eher untypisch, denn dort geht man davon aus, dass jede Handlung eine Spur hinterlässt.

[80] Siehe auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 668.

[81] https://www.fakewhats.com/generator [29.6.2023].

[82] Zur theoretisch denkbaren „perfekten“ Manipulation an Daten *Dewald/Freiling*, Forensische Informatik, S. 39; siehe auch zur Manipulierbarkeit und der Notwendigkeit, sog. Anti-Forensik entgegenzuwirken *Heinson*, IT-Forensik, S. 54 und S. 68 ff.; zur Schwierigkeit technisch spurloser Manipulationen: *Freiling/Hösch*, Digital Investigation (2018), S. 83 ff.; *Schneider/Wolf/Freiling*, Forensic Science International: Digital Investigation (2020) Vol. 32, No. 300924.

[83] Das kann mithilfe des folgenden Beispiels verdeutlicht werden: Ein Rechner wird wiederum mit einer Live-CD gebootet. Nach dem Systemstart wird mittels einer VoIP-Software (z. B. Skype) ein verschlüsseltes Telefonat mit einer anderen Person geführt. Die Kenndaten der anderen Person werden dabei im laufenden Betrieb eingegeben. Nach dem Telefonat wird der Rechner heruntergefahren und die Live-CD entfernt. Damit die Handlung unentdeckt bleibt, müssen folgende Annahmen getroffen werden: Es wird lediglich die Festplatte des Rechners auf Spuren untersucht. Die Systembenutzung selbst hinterlässt keine zusätzlichen digitalen Spuren (etwa im BIOS). Im Netzwerk fallen keinerlei Spuren an, bzw. die dortigen Spuren werden nicht untersucht. Die Systembenutzung selbst (also die Tatsache, dass die Person den Rechner überhaupt benutzt) ist keine Spur (etwa, weil es sich um den persönlichen Rechner der Person handelt), *Dewald/Freiling*, Forensische Informatik, S. 69 f.

Die Meinung, dass es im Bereich der digitalen Spuren grundsätzlich nicht nachvollziehbare Manipulation gibt, basiert auf der Annahme, dass es sich bei dem System um ein geschlossenes System handelt (siehe auch schon im 2. Teil, A. III. und hier unter B. II. 2.). Aber Spuren entstehen auch außerhalb des eigentlich benutzten Systems. In der Praxis werden Rechner grds. nicht isoliert genutzt, sondern treten in Verbindung mit anderen Rechnern. Es entstehen also dort und auch im Netz selbst Spuren (beim Internet-Service-Provider oder im Router), die untersucht werden können. Außerdem ist das digitale System immer in die physische Welt eingebettet, in der auch Spuren entstehen, etwa in Form von Fingerabdrücken auf der Tastatur.[84] Die perfekte Manipulierbarkeit digitaler Spuren ist also ähnlich problematisch wie die perfekte Manipulierbarkeit physischer Spuren. Wenn man hingegen ausschließlich digitale Spuren betrachtet (also die reine Spureninformation), dann ist eine perfekte Manipulation denkbar. Diese beruht dann aber auf einer Selbstbeschränkung der Strafverfolgungsbehörden.

Ähnlich verhält es sich mit einer besonderen Form der Manipulation: Der Vernichtung bzw. Löschung von digitalen Spuren. Vor allem ein nicht nachweisbares selektives Löschen einzelner Dateien ist in der Praxis schwieriger als gedacht. Zum Beispiel sind Dateien, die mit den Bordmitteln des Betriebssystems gelöscht werden, i. d. R. noch lange Zeit auf der Festplatte rekonstruierbar.[85] Diese Ausführungen können v. a. bei der Formulierung der Beweisfragen im Untersuchungsauftrag hilfreich sein.

In Anbetracht des eben Geschilderten – und v. a. weil technische Laien Manipulationen digitaler Dateien nicht ohne Weiteres aufdecken können oder sie wegen der scheinbaren Objektivität der Daten sogar für unwahrscheinlich halten – ist daher in besonderer Weise die tatrichterliche Überzeugung von den Hilfstatsachen bzgl. der Integrität und Authentizität relevant, von denen das Gericht überzeugt sein muss (siehe dazu vertiefter bei B. III. 5. a)).

d) Kopierbarkeit

Digitale Rechensysteme kodieren Daten im binären Zahlensystem. Da Computer alle Informationen schlussendlich im Binärformat speichern, kennen sie nur eindeutig unterscheidbare („diskrete“) Zustände. Folglich befindet sich ein Computer zu jedem Zeitpunkt in einem klar definierten Zustand. Das steht im Gegensatz zu einer grundlegenden Erfahrung, die man in der realen Welt macht: Materie ist (nahezu) beliebig zerteilbar. Der Zustand der realen Welt ist also alles andere als „diskret“, während der Zustand eines Computers

84 *Dewald/Freiling*, Forensische Informatik, S. 70.

85 *Dewald/Freiling*, Forensische Informatik, S. 70 f. m. w. N.

zu jedem Zeitpunkt immer bis ins letzte Bit exakt definiert ist. Im Prinzip kann man alles, also auch alle Arten von Naturphänomenen, wie Bilder oder Geräusche in einer vorher festgelegten Genauigkeit als binäre Zahl kodieren (siehe auch im 2. Teil, A. III.). Das gilt umso mehr für schriftlich niedergelegte Informationen, Konzepte und Ideen. Die diskrete Form all dieser Artefakte macht es möglich, „perfekte" Kopien zu erzeugen, die von ihrem digitalen Inhalt nicht vom Original zu unterscheiden sind.[86] Aufgrund ihrer digitalen Natur kann man also auch digitale Spureninformationen im Gegensatz zu physikalischen Spuren exakt duplizieren und somit alle Untersuchungen anhand einer Kopie durchführen. Genau genommen kopiert man aber lediglich die digitale Spureninformation, der Spurenträger verändert sich nicht. Das steht im gefühlten Gegensatz zu vielen physischen Spuren wie etwa Blut oder DNA-Spuren, die für eine Untersuchung chemisch analysiert und darum teilweise zerstört werden müssen. Wenn man digitale Spuren kopiert, muss man jedoch sicherstellen, dass im Rahmen des Kopiervorgangs die Integrität gewahrt bleibt, also keine Veränderungen an den Spuren stattfinden. Die Übereinstimmung des Originals mit der Kopie lässt sich aber vergleichsweise einfach nachweisen, etwa durch einen bitweisen Vergleich mit dem Original mithilfe von kryptographischen Hashfunktionen[87], die einen kompakten Fingerabdruck eines Datenträgers erstellen können.[88]

Aufgrund der Kopierbarkeit können digitale Spuren nicht einem bestimmten „Ort" in der Realwelt zugewiesen werden. Dementsprechend ist der „Ursprungsort" von Daten oft schwer bestimmbar. Für eine Verwendung als Beweismittel verursachen diese Eigenschaften Herausforderungen: So muss bspw. gewährleistet sein, dass der Ursprungsort der Daten, die als Beweismittel dienen sollen (z. B. der Computer des Beschuldigten) nachgewiesen werden kann (Authentizität oder Ursprungsechtheit der Daten).[89]

e) Semantik

Freiling und Dewald klassifizieren digitale Spuren außerdem in Bezug auf ihre Semantik auf Anwendungsebene: Primärdaten, Sekundärdaten, Programmdaten, Konfigurationsdaten und Logdaten.[90]

---

[86] Diese Eigenschaft basiert auf der Reduktion der gespeicherten Daten auf die digitale Repräsentation.

[87] Eine Hashfunktion ist eine mathematische Funktion, die eine beliebig lange Bitfolge m auf einen Wert h mit fester Länge n abbildet („digitaler Fingerabdruck"), vertiefend zu den kryptografischen Hashfunktionen, *Dewald/Freiling*, Forensische Informatik, S. 309 f.

[88] *Dewald/Freiling*, Forensische Informatik, S. 71 f.

[89] Siehe auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 23 f.

[90] *Dewald/Freiling*, Forensische Informatik, S. 72 f.

Die Daten dieser Klassen unterscheiden sich typischerweise in ihrem Inhalt, Entstehungszeitpunkt, Speicherort und zum Teil auch in ihrer Aussagekraft im Kontext einer IT-forensischen Untersuchung. Das bedeutet, dass je nach Art der im konkreten Fall gesuchten Spuren eine oder mehrere bestimmte Klassen von Daten zu untersuchen sind.[91]

Der Begriff Primärdaten bezeichnet solche Daten, zu deren Verarbeitung eine Anwendung implementiert wurde. Primärdaten sind also in Bezug auf eine konkrete Anwendung diejenigen Daten, die von dieser Anwendung primär verarbeitet werden. Bei der Verwendung einer konkreten Bildverarbeitungssoftware werden z. B. Bilddateien verarbeitet. Bilddateien sind in diesem Fall Primärdaten. Ein weiteres Beispiel sind E-Mails als Primärdaten eines E-Mail-Clients wie Mozilla Thunderbird.[92]

Sekundärdaten werden dazu erstellt und genutzt, um die Verarbeitung von Primärdaten zu vereinfachen. Dabei kann es sich entweder um Daten handeln, die die Verarbeitung der Primärdaten durch die Anwendung unterstützen (System-Sekundärdaten) oder die dem Benutzer die Bearbeitung der Primärdaten erleichtern (Benutzer-Sekundärdaten). Übliche Beispiele für System-Sekundärdaten sind Caches, Indizes oder Journale, die die Performanz einer Anwendung bei der Verarbeitung der Primärdaten erhöhen. Systemsekundärdaten werden deshalb häufig als Nebeneffekt der Verarbeitung von Primärdaten erstellt – regelmäßig ohne Absicht oder Kenntnis der Benutzerin. Im Gegensatz dazu werden Benutzer-Sekundärdaten verwaltet, um den Benutzer bei der Arbeit mit Primärdaten durch eine Anwendung zu unterstützen. Diese Daten werden für die Gewährleistung der Kernfunktionalität der Anwendung an sich nicht benötigt. Beispiele für Benutzer-Sekundärdaten sind Lesezeichen in Webbrowsern, Adressbücher in E-Mail-Clients oder Listen zuletzt benutzter Dokumente.[93] Für Strafverfolgungsbehörden sollten v. a. System-Sekundärdaten einen hohen Beweiswert haben (technisch unvermeidbare Spuren, vgl. dazu unter 3. b)).

Programmdaten sind Daten, die eine Anwendung selbst ausmachen und werden häufig auch als Programmcode bezeichnet. Es kann sich sowohl um eine ausführbare Binärdatei oder Bibliothek als auch um einen Bytecode bzw. Quelltext (im Falle einer interpretierten Programmiersprache) handeln. Programmdaten verändern sich i. d. R. während der Ausführung der Anwendung nicht (Ausnahme wäre bspw. eine Updatefunktionalität).[94] Interessant sind diese Programmdaten insbesondere für das Akteneinsichtsrecht der Verfah-

91 *Dewald/Freiling*, Forensische Informatik, S. 72 f.
92 *Dewald/Freiling*, Forensische Informatik, S. 73.
93 *Dewald/Freiling*, Forensische Informatik, S. 73 f.
94 *Dewald/Freiling*, Forensische Informatik, S. 74.

rensbeteiligten (siehe im 2. Teil, B. V. 2. b)), wenn die Arbeitsweise der verwendeten Datenverarbeitungsmethoden und die damit produzierten Ergebnisse überprüft werden sollen.

Konfigurationsdaten wiederum bestimmen die Art und Weise, in der eine Anwendung Primärdaten verarbeitet. Eine charakteristische Eigenschaft von Konfigurationsdaten ist, dass sich diese Daten in den meisten Fällen unmittelbar nach der Installation einer Anwendung oder auf explizite Anforderung der Benutzerin verändern und ansonsten aber konstant bleiben. Es gibt („implizite") Konfigurationsdaten, auf die nicht direkt Einfluss genommen werden kann (z. B. werden bei der Installation einer Anwendung Verzeichnisstrukturen angelegt wie Ordner, in denen bearbeitete Primärdaten standardmäßig gespeichert werden). Im Gegensatz dazu existieren auch („explizite") Konfigurationsdaten, die vom Benutzer verändert werden können, um das Verhalten der Anwendung zu steuern, wie etwa Speicherort von temporären Daten oder Verzeichnisnamen).[95] Viele Anwendungen wie ausgeführte Aktionen, Fehlermeldungen oder Informationen zur Fehlerbehebung werden als Logdaten in einem Protokoll gesichert. Diese Daten ermöglichen es u. a. einem Administrator das Verhalten der Anwendung nachzuvollziehen. Wenn solche Daten vorhanden sind, bieten sie wertvolle Rückschlüsse über vergangene Aktivitäten des Systems und sind daher im Kontext einer forensischen Untersuchung von besonderer Relevanz.[96]

f) Big data

Seit 2001 werden Tools produziert, die darauf ausgerichtet sind, Daten zu sammeln und zu verarbeiten.[97] Dabei ergibt sich allerdings für den forensischen Prozess das Problem der Bewältigung großer Datenmengen, sog. big data.[98] Es ist keine Seltenheit, dass mehrere Terrabyte an Daten beschlagnahmt werden.[99] Das umfasst sowohl die reine Gewinnung, Speicherung und Verarbeitung der Daten, als auch die Aufgabe, in der beständig steigenden Datenmenge diejenigen Objekte zu identifizieren, die für die Untersuchung inhaltlich relevant sind.[100] Die Massendatenaufbereitung stellt eine der häu-

---

95 *Dewald/Freiling*, Forensische Informatik, S. 74 f.

96 *Dewald/Freiling*, Forensische Informatik, S. 75 f.

97 Vgl. auch *Galloway*, The four, S. 185 ff.

98 Siehe auch *Bäcker/Freiling/Schmitt*, DuD (2010) Vol. 34, S. 80 ff.; *Zweig*, Ein Algorithmus hat kein Tatgefühl; *Weichert*, ZD 2013, 251 f.

99 Wenn man sich diese Besonderheit vor Augen führt würde eine Auswertung von etwa 1,5 Terabyte (was heutzutage nicht mehr selten ist) dem Informationsgehalt von 750 Mil. Bedruckten DIN A4-Seiten entsprechen.

100 *Dewald/Freiling*, Forensische Informatik, S. 91.

figsten Aufgaben im Bereich der forensischen Informatik dar.[101] Die Komplexität und Mehrstufigkeit[102] der forensischen Verarbeitung sprechen jedenfalls häufig für den Bedarf einer besonderen Sachkunde im Umgang mit big data (vgl. Zweiter Teil, A. IV. sowie B. II. 2. a) und c) bb)).[103] Bereits beim ersten Schritt, der Erhebung, ist Expertise gefordert. Dabei muss festgestellt werden, welche Daten sich überhaupt auf einem Datenträger befinden; konkreter: Welche Partitionen existieren, mit welchen Dateisystemen diese formatiert wurden und um welche Arten von Daten es sich konkret handelt (komplexe oder sogar proprietäre Datenbanken, virtuelle Maschinen usw.). Weiter wird ggf. versucht, gelöschte bzw. versteckte Daten wiederherzustellen.[104]

Mittlerweile gibt es verschiedene Ansätze KI zur Lösung dieses Problems einzusetzen (unter Berücksichtigung bestimmter rechtlicher und technischer Voraussetzungen). Die zunehmende massenhafte Speicherung von Daten wirft außerdem die Probleme der Verhältnismäßigkeit des Eingriffs in die Privatsphäre (siehe dazu auch schon im 2. Teil, B. VI. 3.) und des digitalen Zufallsfundes auf.[105]

Sowohl für private IT-Sachverständigenbüros, als auch für die Strafverfolgungsbehörden sowie für die Strafverteidigung bedeutet das in erster Linie ein Ressourcenproblem.

g) Verschlüsselungstechnologien

Mit dem massenhaften „Abgreifen" von Daten gehen Verschlüsselungstechnologien einher, um eben das aus Sicht der Benutzerinnen zu verhindern – ein Gewinn für die Nutzerinnen und eine Hürde für die Strafverfolgungsorgane, denn diese Verschlüsselung gilt es bei der Sachverhaltsermittlung im konkreten Strafverfahren zu überwinden.[106] Aus Sicht der Strafverfolgungsbehörden ist es ein gravierendes Problem, dass Daten vermehrt mit kryptogra-

---

101 Siehe zu Ermittlungen bei großen Datenbeständen auch *Mysegades*, Software als Ermittlungswerkzeug, S. 42.

102 Die Vorgehensweise wird grds.in sechs Schritte unterteilt: Erhebung, Expansion, Aggregation, Reduktion, Strukturierung, Visualisierung, vgl. *Dewald/Freiling*, Forensische Informatik, S. 359.

103 Vertiefend zu dem Thema vgl. *Dewald/Freiling*, Forensische Informatik, S. 359 ff.

104 *Dewald/Freiling*, Forensische Informatik, S. 360.

105 Siehe dazu auch *Rückert/Wüst*, KriPoZ 2021, S. 66.

106 Grundsätzlich ist Verschlüsselungstechnologie sinnvoll und geboten, weswegen den Forderungen, den Einsatz von Verschlüsselungstechnologie zu beschränken oder staatliche Hintertüren einzubauen, eine Absage zu erteilen ist. Dies würde die Verschlüsselungstechnologie schwächen und Einfallstore für Angriffe Dritter bieten.

phisch sicheren Methoden verschlüsselt werden.[107] Ohne Kenntnis des Schlüssels kann der ursprüngliche Informationsgehalt nicht entnommen werden und der Beschuldigte kann nicht gezwungen werden, das Passwort zu nennen.[108] Es gibt technische und organisatorische Mittel, um Verschlüsselungstechnologien in Strafverfahren zu überwinden. Dabei können z. B. informationstechnische Systeme im laufenden, entschlüsselten Betrieb beschlagnahmt werden, (aufgefundene) Passwörter probehalber eingetippt oder gespeicherte Passwörter über spezielle Rechtsgrundlagen angefragt werden.[109] Das hat v. a. Auswirkungen auf die Grenzen der Sachverständigentätigkeit (siehe Zweiter Teil, B. VI.).

4. Fazit

Die Daten, die im Rahmen eines IT-Sachverständigengutachtens verarbeitet werden, beeinflussen durch ihre Eigenschaften die Qualität der Tatsachenbasis. Auch sollten diese Eigenschaften bei der Formulierung der Beweisfragen im Untersuchungsauftrag berücksichtigt werden. Da Daten sowohl unbewusst als auch bewusst leicht manipuliert werden können und sich im Zeitverlauf verändern können, wird die Qualität der Tatsachenbasis hinsichtlich der Zuverlässigkeit der Daten von der Ergreifung von dem Stand der Technik entsprechenden Maßnahmen zur Sicherung der Authentizität (Ursprungsechtheit) und Integrität (Unverändertheit) bestimmt (z. B. Berechnung und Abgleich von Hash-Summen, Einhaltung der Verwahrkette etc.).[110]

III. Der forensische Prozess („the journey from data to evidence“)[111]

Bei der Sicherung und Analyse digitaler Spuren muss eine allgemein akzeptierte und erprobte Vorgehensweise (sog. Vorgehensmodelle) angewandt werden.[112] Das entspricht auch den Anforderungen des Beweisrechts (Grund-

---

[107] Kryptographie ist der bekannteste Weg, Daten vor unautorisierter Nutzung zu schützen. Hierbei wird eine Eingabesequenz – zum Beispiel ein Text oder ein Bild – mit Hilfe eines Schlüssels übersetzt in einen Chiffretext. Bei guten Verschlüsselungssystemen lassen die statistischen Eigenschaften des Chiffretextes keinen Rückschluss auf den Inhalt der Eingabe zu, vgl. *Rieß*, in: Dewald/Freiling, Forensische Informatik, S. 176.

[108] Er genießt das verfassungs- und menschenrechtlich geschützte Recht, nicht an seiner eigenen Überführung mitwirken zu müssen.

[109] *Rückert/Wüst*, KriPoZ 2021, S. 66.

[110] *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 544, S. 677 f.

[111] Vgl. auch *Sunde*, Non-technical Sources of Errors, S. 21 ff.

[112] Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 227.

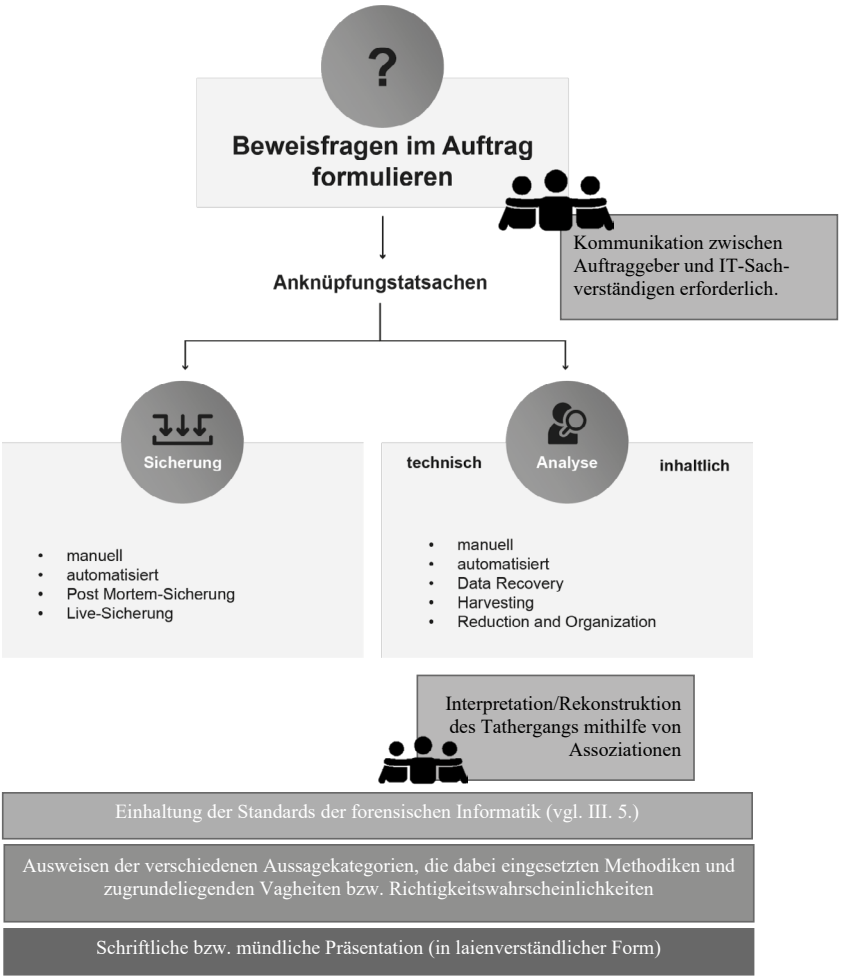


Abbildung 9: „Der forensische Prozess“

satz der Nachvollziehbarkeit und Transparenz, A. II.).[113] Diese sollen lediglich einen Handlungsrahmen bilden, an dem sich das eigene Vorgehen orientieren kann. Charakteristische Vertreter für solche Vorgehensweisen sind bspw. das „Incident-Response-Modell“[114] und der „investigative Prozess“[115] sowie das

113 *Sunde*, Non-technical Sources of Errors, S. 18.
114 Von *Mandia u. a.*, Incident Response & Computer Forensics.
115 Von *Casey*, Digital Evidence and Computer Crime (2004).

„common model“[116], das auf den beiden anderen aufbaut.[117] In dieser Arbeit soll v. a. auf das Letztgenannte Bezug genommen werden, da es sehr abstrakt, übersichtlich und ganzheitlich ist.[118] Hier wird das Modell speziell zugeschnitten für das Strafverfahrensrecht betrachtet. Die forensischen Schritte, die näher dargestellt werden sollen, sind die Sicherung, Analyse, Interpretation (i. S. d. Assoziation) und die abschließende Präsentation.

Während dieses gesamten forensischen Prozesses müssen sowohl rechtlichen als auch technischen Fragestellungen Rechnung getragen werden, z. B.: Wie greife ich auf digitale Spuren zu, ohne ihren Beweiswert zu schmälern? Was bedeuten digitale Spuren? Wie kann ich sicherstellen, dass die Spuren das bedeuten, was ich glaube?[119] Auch hier wird wieder deutlich, wie wichtig es in diesem Tätigkeitsfeld ist, sowohl für die juristischen Verfahrensbeteiligten als auch für die technischen Experten, ein gewisses Grundverständnis von der jeweils anderen Disziplin zu haben.

1. Die Sicherung digitaler Spuren

Ermittlerinnen suchen am Tatort nach Spuren, die über den Tathergang Aufschluss geben können.[120] Dabei sind v. a. Spuren für die Ermittlungen interessant, die unabsichtlich hinterlassen werden, wie etwa Fingerabdrücke, Fasern oder Sekrete. Im Bereich der forensischen Informatik sind das z. B. die oben beschriebenen technisch unvermeidbaren Spuren (siehe B. II. 2. b)). I. d. R. sind diese aber schwer zu erkennen und müssen von Spezialisten gesucht und ausgewertet werden. Dieser Vorgang wird allgemein auch Spurensicherung genannt. Bei der Sicherung einer Spur entstehen die ersten Behauptungen, die in irgendeiner Form an die Spur geheftet werden, etwa als Aufschrift auf einem Asservatenbeutel oder als Eintrag in einem Durchsuchungsbericht. Spuren können eine Theorie über einen Tathergang stützen oder widerlegen. Die Überzeugungskraft solcher Spuren hängt stark davon ab, wie „nah“ die (vor Gericht) vorgelegten Spuren an den Spuren sind, die am Tatort gefunden wurden.[121] Diese Nähe versucht man mit zwei Begriffen zu fassen: der Integrität und der Authentizität von Spuren (dazu bei B. III. 5. a)).

---

116 Von *Freiling/Schwittay*, A Common Process Model for Incident Response and Computer Forensics.

117 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 227; einen weiteren Überblick über Vorgehensmodelle vgl. *Dewald/Freiling*, Forensische Informatik, S. 259 ff.

118 Vertiefend vgl. *Dewald/Freiling*, Forensische Informatik, S. 246 ff.

119 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 267.

120 Vgl. zu der Aufteilung der Sicherung in „identification, collection and examination auch *Sunde*, Non-technical Sources of Errors, S. 21 ff.

121 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 32.

a) Isolation des Beweismittels

Bevor die digitalen Spuren an sich ausgewertet werden können, müssen zunächst die Datenträger selbst forensisch gesichert und ausgewertet werden (zumindest in der Datenträgerforensik).[122] Hierfür erforderlich sind Kenntnisse im Bereich der Festplattentechnologie und der Abstraktionsschichten auf Datenträgern (Partitionssysteme).[123]

Dabei gibt es verschiedene Arten des Zugriffs auf einen Datenträger im Rahmen der forensischen Untersuchung: So gibt es bspw. die Post-Mortem-Sicherung[124] eines technisch isolierbaren Speichermediums; eine sog. Live-Sicherung (oder Live Imaging)[125], wenn die Daten während des Betriebs des informationstechnischen Systems mithilfe von Software – u. a. mittels des ColdBoot-Verfahrens oder dem DMA[126] oder der Speicherakquise durch Ruhezustand – gesichert werden oder die Sicherung von Daten aus Speichern von Mobiltelefonen („Mobilfunkforensik")[127]. Der Zugriff auf ein „lebendiges" System kann z. B. erfolgen, wenn der Datenträger aktuell im Gebrauch durch einen oder mehrere Computer ist, wobei die Gefahr besteht, digitale Spuren zu verändern (was wiederum Auswirkungen auf die Integrität und Authentizität hat),[128] oder auf ein „totes" System – ohne die Hilfe des Betriebssystems, wenn der Datenträger (zumindest kurzzeitig) „in ausgeschaltetem Zustand" vorgefunden wird (bspw. als ausgebaute Festplatte).[129]

Bei dem Zugriff auf die Daten sollten diese nicht verändert werden. Um die Originaldaten zu schützen, muss der Zugriff mit entsprechenden Werkzeugen unterstützt werden. Dafür werden Hardware Write Blocker oder Software Write Blocker verwendet.[130]

Zur Dokumentation des Zustandes vor dem Sichern wird eine vollständige 1:1-Kopie (auch „Festplattenabbild" bzw. „disk image" genannt) vorgeschlagen.[131] Allerdings kann das aus verschiedenen Gründen unverhältnismäßig

---

122 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 267; Vertiefend zu den verschiedenen Dateisystemen vgl. *Schneider/Eichhorn/Freiling*, Forensic Science International: Digital Investigation 2022, S. 2.

123 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 268.

124 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 679 m. w. N.

125 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 679 m. w. N.

126 Direct Memory Access.

127 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 680 ff.

128 Vertiefend dazu vgl. *Dewald/Freiling*, Forensische Informatik, S. 306.

129 Vertiefend dazu vgl. *Dewald/Freiling*, Forensische Informatik, S. 306; zu dem Thema auch die Bachelorarbeit von *Müller*, Die digitale Durchsuchung Abbilderstellung im Strafprozess, S. 15 ff.

130 Siehe dazu auch *Dewald/Freiling*, Forensische Informatik, S. 306 f.

131 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 307m. w. N.

sein[132] und stößt in der Praxis mittlerweile an seine Grenzen: wachsender Zeitaufwand, zunehmende Mengen an Speicherressourcen zur Archivierung, steigende Kosten der Analyse überproportional mit der Datenmenge oder unverhältnismäßiger Eingriff in die Privatsphäre.[133]

b) Abstraktionsschichten

Wie auch bei vielen Arten von physischen Spuren, die man oft nicht mehr mit bloßem Auge erkennen kann, müssen digitale Spuren in der Regel immer zunächst extrahiert und in eine lesbare Form übersetzt werden. Diese Aufbereitung erfordert den Einsatz von Werkzeugen, die eine Abstraktion bzw. Interpretation der physischen Spuren zeigen. Charakteristisch für moderne Computersysteme ist zudem, dass es meist mehrere Abstraktionsebenen gibt, auf denen die Daten dargestellt werden können.[134]

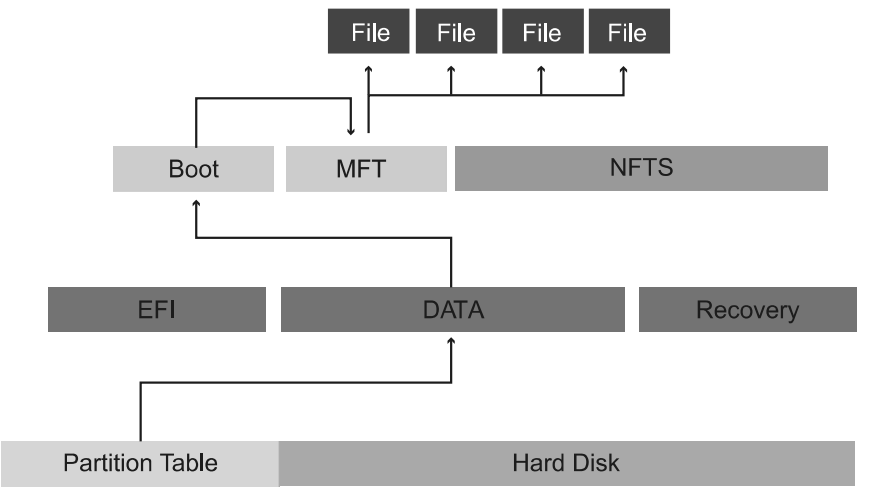


Abbildung 10: „Die Abstraktionsschichten von Datenträgern“

132 Siehe dazu auch *Dewald/Freiling*, Forensische Informatik, S. 356 ff.
133 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 307, S. 350.
134 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 65.

Das kann an einem Beispiel zu Abstraktionsschichten verdeutlicht werden, die durchlaufen werden, wenn eine E-Mail-Nachricht als digitale Spur untersucht wird:[135]

- Interpretation der Magnetisierung der Festplatte (Bits)
- Interpretation der Bits durch eine Zeichenkodierung
- Interpretation der Zeichen durch ein Dateisystem
- Interpretation der Daten im Dateisystem als zusammengehörige Datei
- Interpretation der Datei als E-Mail

Jede einzelne dieser Abstraktionsebenen kann Quelle für Interpretationsfehler sein. Daher ist es bei einer forensischen Untersuchung digitaler Spuren insbesondere erforderlich, die Plausibilität jeder einzelnen Interpretation bzw. Abstraktion zu prüfen.[136]

Die Abstraktionsschichten von Computersystemen erlauben verschiedene Ansatzpunkte für die Datensicherung: Auf Ebene des Laufwerks, der Partitionen, der Dateisysteme oder der Applikationsebene. In diesem Zusammenhang ist darauf zu achten, dass auf jeder Abstraktionsebene Daten verloren gehen, bspw. verliert man beim Zugriff auf der Partitionsebene die Informationen der Partitionstabelle, weshalb mindestens auf der Ebene zuzugreifen ist, welche die für die Analyse interessanten Daten enthält, aber unter dem Aspekt der Verhältnismäßigkeit noch „erlaubt" sein muss. Also „so tief wie nötig und so hoch wie möglich", sog. selective imaging.[137] Dieser Umstand muss im Rahmen der Verhältnismäßigkeit des Umfangs der Sicherung und Durchsuchung von IT-Asservaten schon bei der Formulierung der Beweisfragen im Untersuchungsauftrag von den Strafverfolgungsbehörden berücksichtigt werden.[138] In der Praxis ist jedenfalls zu beobachten, dass derzeit in kleineren Verfahren auf physischer Ebene gesichert und in Großverfahren (wie Durchsuchung in Rechenzentren) auf Dateiebene gesichert wird.

---

135 Beispiel 6 (Abstraktionsschichten digitaler Spuren), *Dewald/Freiling*, Forensische Informatik, S. 65.

136 *Dewald/Freiling*, Forensische Informatik, S. 65.

137 Vereinfacht gesprochen wird dabei nicht auf die gesamte Festplatte zugegriffen, sondern nur auf relevante Teilbereiche sowie alle relevanten Metadaten der darunterliegenden Schichten, vgl. dazu *Stüttgen*, Selective Imaging Revisited; dazu auch *Dewald/Freiling*, Forensische Informatik, S. 308, S. 350 ff.

138 Vgl. in diesem Zusammenhang insbesondere die Ausführungen im 2. Teil, B. VI. 3.

c) Fazit

In Bezug auf die obigen Ausführungen bzgl. der Kategorisierung der Sachverständigentätigkeit und einer entsprechenden Bewertung im Hinblick auf eine besondere Sachkunde lässt sich zunächst festhalten, dass es sich bei der forensischen Sicherung (je nach konkretem Einzelfall) um eine vorbereitende Tätigkeit bzw. eine Befundermittlung i. S. d. dritten Kategorie handeln kann. Dass dabei oft auch Bewertungen i. S. v. Schlussfolgerungen für den konkreten Sachverhalt oder Erfahrungssätze der forensischen Informatik zum Einsatz kommen (das wird an späterer Stelle noch beispielhaft erklärt), qualifiziert die Arbeit auch als eine Sachverständigentätigkeit i. S. d. ersten und zweiten Kategorie. Es wird deutlich, dass für die Durchführung von solchen Sicherungen durchaus ein umfassendes Wissen in einer Vielzahl an Teilgebieten der Informatik i. V. m. forensischen Vorgehensweisen erforderlich ist; v. a. wenn IT-Sachverständige mit Sperrcodes, spezialisierter Hardware oder gewaltigen Datenspeichern aus dem Firmenumfeld konfrontiert sehen. Aufgrund des ständigen Technikwandels und der rasenden Verbreitung neuer Technologien, müssen sich die Praktikerinnen auch ständig auf dem aktuellen Stand der Technik halten und über „best practices“[139] informieren, um Fehlern vorbeugen zu können.[140] Das eben gesagte spricht jedenfalls in den allermeisten Fällen für die Einordnung als Sachverständigentätigkeit; ob das letztlich der Fall ist, muss jedoch im Einzelfall entschieden werden.[141]

2. Die Analyse digitaler Spuren

Nach der Sicherung werden die Spuren näher untersucht. Diesen Vorgang nennt man Spurenanalyse, und er geschieht meist durch Experten, i. d. R. Wissenschaftler (Biologen, Physiker, Chemiker, Mediziner oder Informatiker), in speziellen Laboren. In der Praxis spricht man auch von „kriminaltechnischer Untersuchung“[142]. Die Analysephase[143] ist abhängig von der zu beantwortenden Beweisfrage.

Analyse[144] meint eine Rekonstruktion des Vorfalls. Sie ist „die Verarbeitung von (den bereits sichergestellten) Informationen, die sich mit der Beantwortung der Beweisfrage befassen, die Fakten über ein Ereignis, die Bedeu-

---

139 Hier eine Übersicht: https://enfsi.eu/about-enfsi/structure/working-groups/documents-page/documents/best-practice-manuals/ [26.6.2023].

140 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

141 Vgl. dazu auch die Ausführungen im 2. Teil, B. IV.

142 Siehe dazu im 2. Teil, B. II. 2.

143 Vertiefend vgl. *Dewald/Freiling*, Forensische Informatik, S. 253 ff.

144 Vetriefend vgl. *Dewald/Freiling*, Forensische Informatik, S. 256 ff.

tung der Beweise und die verantwortliche(n) Person(en) zu ermitteln".[145] In diesem Schritt werden im Hinblick auf die Beantwortung der jeweiligen Beweisfrage Hypothesen gebildet. Um eine möglichst objektive Analyse gewährleisten zu können, müssen auch hier die forensischen Prinzipien und beweisrechtlichen Anforderungen eingehalten werden. Es muss insbesondere darum gehen, unter Verwendung wissenschaftlicher Methoden unterschiedliche Hypothesen aufzustellen und zu versuchen, diese zu widerlegen, anstatt sie zu beweisen (siehe zur Bildung von Alternativhypothesen auch oben im 2. Teil, B. II. 2. c) ee)). So haben die verbleibenden Hypothesen eine höhere Wahrscheinlichkeit den Tathergang korrekt zu rekonstruieren.[146]

Im Detail kann diese Phase (Casey folgend)[147] zweigeteilt werden: 1) Der technische Analyseprozess und 2) der inhaltliche Analyseprozess (Bewertung und Interpretation von digitalen Spuren).

Unter technischer Analyse versteht man Tätigkeiten mit überprüfbaren Ergebnissen, was bedeutet, dass sie sicher außerhalb eines akkreditierten Labors durchgeführt werden können. Diese Tätigkeiten können z. B. das Anfertigen von forensischen Kopien, das Extrahieren aktiver und gelöschter Dateien, die Feststellung, ob sich illegales Material in der Beweisdatei befindet mit Hilfe von digitalen Signatursuchen, das Entschlüsseln von Daten oder das Scannen auf Viren sein.

Inhaltsanalyse bedeutet, Informationen zu identifizieren und zu dokumentieren, die potenzielle Beweismittel enthalten. Das kann bedeuten, dass festgestellt wird, ob sich unter den Daten Bilder von sexuellem Missbrauch von Kindern i. S. d. § 184b StGB befinden und dass die relevanten Informationen exportiert und in Berichten dokumentiert werden. Bei der Beweisauswertung geht es darum, die Richtigkeit, Kausalität, Verknüpfung, Beweiskraft und Bedeutung der Daten zu ermitteln. Dabei handelt es sich oft um die Beantwortung von Fragen, wie: Wer hat die illegale Datei auf den Computer heruntergeladen? Mit welcher Kamera wurde dieses digitale Bild aufgenommen? Oder wurden Beweismittel auf diesem Computer absichtlich zerstört? Der Grund dafür, diese Inhaltsanalyse als Teilphase der Analysephase zu formulieren, ist folgender: „Die Beantwortung solcher Fragen beinhaltet die Interpretation und Bewertung digitaler Beweismittel, was ein höheres Maß an Spezialisierung des Wissens, Formalisierung des Prozesses, Durchführung von Tests, Forschungsgrundlage und Qualitätskontrolle erfordert".[148] Die Bewertung von Beweisen sollte in einem akkreditierten Labor mit geeigneten Qualitätsmanagementsystemen wie Peer Review durchgeführt werden.

---

145 *Flaglien*, Digital Forensics (2017), S. 13 (42) m. w. N.

146 Vertiefend vgl. *Dewald/Freiling*, Forensische Informatik, S. 256.

147 *Casey*, Digital Evidence and Computer Crime (2016).

148 *Casey*, Digital Evidence and Computer Crime (2016), S. 2.

Der Vorteil (in dieser Zweiteilung der Analysephase) besteht zunächst darin, eine klare Unterscheidung zwischen denjenigen Tätigkeiten zu treffen, die v. a. ein Qualitätsmanagementsystem in Bezug auf die angewendeten Datenanalysemethoden und eine akkreditierte Laborumgebung erfordern – und solchen, die das nicht benötigen. Auch kann dadurch den Anforderungen an Nachvollziehbarkeit und Transparenz nachgekommen werden. Denn durch diese Unterteilung werden die einzelnen Schritte, die zugrundeliegenden Datenverarbeitungsmethoden und die dafür verwendeten Annahmen, Werkzeuge und letztlich auch die inhaltliche Bewertung der digitalen Spuren und enthaltenen Informationen einzeln dargestellt und kenntlich gemacht. Diese Unterscheidung kann weiter dazu beitragen, Probleme im Zusammenhang mit der erforderlichen Sachkunde in Bezug auf die einzelnen Schritte zu lösen – v. a. wohl in Bezug auf den Schritt der inhaltlichen Analyse: Inwieweit hat die Analyse aufgrund von erforderlicher technologischer besonderer Sachkunde von einem IT-Sachverständigen zu erfolgen bzw. kann und muss das im Wege der Inaugenscheinnahme durch das Tatgericht selbst geschehen, weil entweder keine erforderliche Sachkunde benötigt wird oder es sich um eine rechtliche Bewertung und Subsumtion unter Straftatbestände handelt?

a) Ein Beispiel für den Ablauf einer Datenträger-Analyse[149]

In der Praxis wird der Ablauf einer Analyse in Bezug auf die Existenz von kinder- bzw. jugendpornografischem Material auf einem Datenträger i. S. d. §§ 184b ff. StGB wie folgt beschrieben: Nachdem die Daten erfolgreich gesichert wurden, werden diese entsprechend aufbereitet, meist automatisiert (siehe bereits oben im 2. Teil, B. IV. 1.).

Im ersten Schritt wird die Datenextraktion im Hinblick auf Vollständigkeit[150] überprüft und untersucht, ob es Hinweise auf antiforensische Maßnahmen wie verschlüsselte Bereiche oder das Verstecken von Daten mittels Steganographie gibt. Werden solche Anomalien festgestellt, wird versucht, diese Daten sichtbar zu machen.[151]

Im Anschluss werden die Daten mittels spezialisierter Tools (teils) automatisiert aufbereitet bzw. gesichtet.[152] Da auf einem Asservat eine Vielzahl an

---

149 Zur Datenträgeranalyse vgl. auch *Baur*, Zur Beweiskraft informationstechnologischer Expertise.

150 Um sicher zu gehen, dass man keine Daten einer Festplatte übersehen hat, muss auf die Existenz einer HPA oder eines DCO geprüft werden, vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 307.

151 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

152 So werden bspw. bei Ermittlungen im Kriminalitätsfeld der §§ 184b ff. StGB verstärkt an automatisierten Werkzeugen gearbeitet; auch bereits als präventive Maß-

unterschiedlichen Anwendungen vorhanden ist, wird in der Forensik Spezialsoftware eingesetzt, die die Spuren von Anwendungen und Betriebssystemen automatisiert aufbereitet, zusammenstellt, strukturiert und (für den Auftraggeber) durchsuchbar macht. Der große Vorteil der Nutzung dieser Software liegt in der einfachen und prozessökonomischen Bedienung. Im Schnitt würden zum Anstoßen eines solchen Prozesses nicht einmal 10 Min. pro Aufbereitung benötigt.[153]

In Bezug auf die Bewertung dieses forensischen Schrittes als Sachverständigentätigkeit, die eine besondere Sachkunde voraussetzt, würde man in diesen „Plain-Vanilla-Fällen" – wie das eben beschriebene automatisierte Sichten und Aufbereiten der Daten – das Erfordernis einer besonderen Sachkunde zunächst wohl eher ablehnen und die Arbeit als eine eher „triviale" Aufgabe einschätzen (siehe dazu auch schon oben im 2. Teil, B. IV. 1.). Standardmäßig könnte das von Ermittlungspersonen auch durchaus selbst durchgeführt werden und die aufbereiteten Daten als Anknüpfungstatsachen zur weiteren Gutachtenerstellung an einen IT-Sachverständigen übergeben werden.[154] Einerseits wird allerdings angemerkt, dass ein Externalisieren dieser Aufgabe zurück an die Ermittlungsbehörden einen hohen zeitlichen und kostentechnischen Mehraufwand bedeuten würde. Aus Sicht der meisten Forensiker wäre die Ausgliederung der vorbereitenden Tätigkeit der Aufbereitung und Sichtung bestimmt wünschenswert, jedoch in der Praxis aufgrund der aktuellen enormen Auftragslage und der Wahrung des Prinzips des beschleunigten Verfahrens wohl nicht umsetzbar.[155] Weiter müssten sich die Ermittler zunächst die (meist) teure Software anschaffen, die in Sachverständigenbüros standardmäßig vorhanden ist und sich in die Anwendung und Interpretation der Ergebnisse der Tools einarbeiten (zumal es auch bei der Softwareanwendung, wie oben im 2. Teil beschrieben, häufig besonderer Sachkunde bedarf).[156] Andererseits wurde oben auch schon ausgeführt, dass es sich in den seltensten Fällen um „Plain-Vanilla-Fälle" handelt, in denen keine besondere Sachkunde aus dem Bereich der forensischen Informatik gebraucht wird und von einem durchschnittlichen Ermittler bearbeitet werden kann. Im Deliktsbereich der §§ 184b ff. StGB könnten bspw. beim Auffinden von inkriminierten Daten Folgefragen entstehen, die meistens nur durch eine tiefgründige technische Expertise beantwortet werden können. Es ist z. B. entscheidend, ob ein Bild „willentlich besessen" oder „unbewusst automatisiert erstellt" wurde. Wurde

---

nahme in der Polizeiarbeit vgl. z. B. *Sunde/Sunde*, Nordic Journal of Studies in Policing, S. 1 ff.

153 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

154 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

155 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

156 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

das Bild ohne Wissen des Besitzers auf dem Asservat erstellt, was bspw. durch die Mitgliedschaft in einer WhatsApp-Gruppe entstehen kann, oder beim Surfen auf einer Webseite, auf der sich im nicht sichtbaren Bereich ein inkriminiertes Bild befindet, das automatisch im Cache abgelegt wird, muss darauf explizit im Gutachten hingewiesen werden. Besonders der Cache-Bereich ist hierbei problematisch, da der normale Anwender bzgl. dessen Existenz meist ahnungslos ist und auch den Inhalt dort nicht explizit löschen kann (vgl. oben technisch unvermeidbare Spuren, B. II. 3. b)). Ein IT-Sachverständiger kann diesen allerdings problemlos auswerten und fallrelevante (inkriminierte) Dateien finden. Es soll deutlich werden, dass – um bspw. die Frage nach dem willentlichen Besitz beantworten zu können – weitere forensische Untersuchungen erfolgen müssen, bei denen tiefgründiges technisches Wissen erforderlich ist, das eine Ermittlungsperson (im Normalfall) nicht aufbringen kann.[157]

Aufgrund dieser Problematiken wird eine komplette Fallsachbearbeitung z. B. im Bereich der §§ 184b ff. StGB bei einem IT-Sachverständigen als gerechtfertigt angesehen.[158] Die oben beschriebene automatisierte Sichtung kann dabei als „Hilfsdienst" (siehe im 2. Teil, B. II. 2. f)) bzw. eine „vorbereitende Verrichtung" (siehe im 2. Teil, B. II. 3. d) dd)) darstellen und im Wege einer „Gesamtbetrachtung" (siehe im 2. Teil, B. IV. 3.) der Sachverständigentätigkeit zugeordnet werden.

Das Resultat der Aufbereitung muss nach Fertigstellung auf Plausibilität überprüft werden. Aufgrund des großen Funktionsumfanges sind Anwendungsfehler häufig und können erst durch eine nachträgliche manuelle Überprüfung festgestellt werden. Je nach Einzelfall (und Deliktsfeld) kann diese Plausibilitätskontrolle an die Strafverfolgungsbehörden übergeben werden.[159]

Wird die für das Verfahren notwendige Anwendung nicht durch die automatisierte Spezialsoftware unterstützt, muss die Analyse manuell durch den Sachverständigen vorgenommen und aufbereitet werden. Dieser Vorgang erfordert Expertenwissen im Bereich der Anwendungsforensik und dem Reverse Engineering.[160]

Die Befunde werden dann mit dem schriftlichen Gutachten (häufig an die Strafverfolgungsbehörde als Auftraggeberin) zurückgegeben, wo diese dann deliktspezifisch ausgewertet werden und entsprechend Eingang in den Tatsachenstoff der §§ 244 Abs. 2, 261 StPO finden (dazu mehr unter B. III. 5.).

---

157 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.
158 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.
159 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.
160 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

b) Datenanalyse-Methoden

Wie eben beschrieben, kommen bei der Analyse der Daten Tools zum Einsatz, die teils eine automatisierte Untersuchung ermöglichen, teils aber auch eine manuelle Arbeit unterstützen, bspw. Blockchain-Analyse-Tools für Ermittlungen in Kryptowährungssystemen,[161] Such- und Verknüpfungswerkzeuge zur systematischen Durchsuchung des „Darknets"[162] oder allgemeine Datenauswertungswerkzeuge zur Analyse, Verknüpfung und dem Abgleich von Daten-sätzen wie etwa das „Analysts Notebook"[163] sowie die Plattformen Maltego[164] oder Encase[165]. Diese Tools braucht es v. a. deshalb, weil die Daten in digitaler Form für den Menschen und damit das Tatgericht nicht les- und verstehbar sind und erst übersetzt werden müssen. Diese dateninterpretierenden und -übersetzenden Programme weisen unterschiedliche Komplexitäts-, Verlässlichkeits- und Nachvollziehbarkeitsstufen auf, was – Rückert[166] folgend – Auswirkungen auf den Beweiswert und die entsprechende Würdigung hat.

aa) Deterministische Methoden

Hier als deterministische Methoden bezeichnete Arten der Datenverarbeitung generieren nur solche Informationen aus den Daten, die in diesen unzweifelhaft vorhanden sind. Beispiele dafür sind alle Programme, die lediglich digitale Daten in eine menschenlesbare Form (Text, Bild, Video) übersetzen wie Textverarbeitungsprogramme und Programme zum Anzeigen von Bildern und Videos.[167] Hierzu gehören auch Programme, die komplexere Informationen übersetzen und visualisieren, wie etwa (einfache) Programm-Darstellung und Sichtbarmachung des Inhalts von (Festplatten-)Speichern oder Ermittlungstools zur Darstellung von Transaktionen in Kryptowährungssystemen. Schließlich zählen ebenso Such- und Filterprogramme zu den deterministischen Methoden, solange sie keine Interpretation der Informationen bei der Suche oder Filterung vornehmen, sondern sich auf das Anzeigen von unzwei-

161 Z. B. https://www.chainalysis.com [29.6.2023]; https://ciphertrace.com [29.6.2023]; https://github.com/citp/BlockSci [29.6.2023].

162 Z. B. der Dark Web Monitor, https://dws.pm/ [29.6.2023]; vgl. auch *Rückert/Scheler*, KriPoZ 2022, S. 227 f.

163 https://www.ibm.com/security [29.6.2023].

164 https://www.maltego.com [23.6.2023].

165 https://security.opentext.com/encase-forensic [23.6.2023].

166 Digitale Daten als Beweismittel im Strafverfahren, S. 21, S. 673 ff.

167 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 678.

felhaft in den Daten vorhandenen Informationen beschränken (z. B. Volltextsuchen).[168] Bei Mysegades sind das Beispiele der „trivialen Software".[169]

bb) Statistische Methoden

Deutlich komplexere Funktionen weisen Programme auf, die als statistische Methoden der Datenverarbeitung bezeichnet werden. Diese Programme errechnen aus Datensätzen Informationen, die sich diesen Daten nicht unzweifelhaft entnehmen lassen, sondern die nur mit einer gewissen Wahrscheinlichkeit zutreffend sind.[170] Solche Programme stützen sich auf Annahmen und Heuristiken, die ihrerseits nicht unzweifelhaft richtig, sondern nur mit einer gewissen Wahrscheinlichkeit richtig sind. Die „Richtigkeitswahrscheinlichkeit" der Ergebnisse solcher Programme hängt von der „Richtigkeitswahrscheinlichkeit" der zugrundeliegenden Heuristiken und Annahmen ab.[171] Zu diesen Methoden gehören viele der gängigen forensischen Datenanalysewerkzeuge, insb. aus dem Bereich des sog. Data Minings[172] wie Programme für „Ähnlichkeitsanalysen" (Cluster-Analysis), bei denen Datensätze nach vorher definierten Kriterien einer Gruppe von ähnlichen Datensätzen zugeordnet werden (sog. Cluster). Umgekehrt gehören hierher auch Tools für „Ausreißer-Analysen", welche nach bestimmten Kriterien „ungewöhnliche" Datensätze identifizieren. Hierzu zählen etwa Kryptowährungsanalyse-Tools, die auf der Multi-Input-Heuristik basieren.[173] Weitere Beispiele sind sog. Assoziationsanalysen, bei denen Beziehungen und Abhängigkeiten zwischen einzelnen Informationen gefunden werden sollen.[174] Anwendungsbeispiele sind Social Network Analysis-Tools, die Beziehungen zwischen einzelnen Personen innerhalb einer Gruppe oder auch verschiedenen Gruppen herstellen, z. B. innerhalb von sozialen Netzwerken oder innerhalb des Organisierten Verbrechens.[175]

---

168 *Rückert* Digitale Daten als Beweismittel im Strafverfahren, S. 679.

169 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 13 f.

170 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 680.

171 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 680 f.

172 *Zweig*, Ein Algorithmus hat kein Taktgefühl, S. 83 ff.

173 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 680.

174 *Cleve/Lämmel*, Data Mining, S. 191 ff.

175 Zu Entwicklung, Theorie und Anwendung dieser Methoden: *Burcher*, Social Network Analysis and Law Enforcement, 2020.

cc) Machine learning-Methoden

Noch komplexer sind die als selbstlernende Methoden bezeichneten Programme des maschinellen Lernens (ML), so auch die berühmte „künstliche Intelligenz" (KI)[176]. Dabei entwickeln die Programme auf Grundlage von Trainingsdaten die Annahmen und Heuristiken, die ihren Algorithmen[177] (z. B. „Wenn-dann-Bedingung") zugrunde liegen, selbst. Bei solchen Programmen kommt zu dem Problem der nur statistischen Richtigkeitswahrscheinlichkeit noch ein prinzipieller Mangel an Nachvollziehbarkeit des gefundenen Ergebnisses hinzu.[178] Praxisbeispiele in der forensischen Informatik sind Tools zur Aufdeckung von Betrügereien im Bankgeschäft und beim Wertpapierhandel,[179] Software für technische Ermittlungsmethoden i. S. d. §§ 100a ff. StPO,[180] Programme zur Spracherkennung,[181] Gesichts- und Stimmidentifizierung[182], Bilderkennungssoftware zur Identifikation von Kinderpornographie[183], Programme zur Zuordnung einer Kugel zu einer bestimmten Feuerwaffe[184] und Data Mining Tools zur Identifizierung von Menschenhandel-Hotspots[185].[186] Hierunter fallen auch die Beispiele von Mysegades der „opaken Software".[187]

---

176 Eine übersichtliche Aufarbeitung von KI als Beweismittel (auch) in einem Strafverfahren findet sich hier: *Grimm/Grossman*, J. Tech & Intell. Prop. (2021) Vol. 9, S. 19; *Biasiotti*, KI – Künstliche Intelligenz (2022) Vol. 36, S. 143 ff.; *Lorch/Scheler/Rieß*, Compliance Challenges in Forensic Image Analysis Under the Artificial Intelligence Act, https://doi.org/10.48550/arXiv.2203.00469 [26.6.2023].

177 = präzise Verarbeitungsvorschriften für ein elektronisch arbeitendes Gerät, vgl. *Nink*, Justiz und Algorithmen, S. 143.

178 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 21, S. 684.

179 *Alpaydin*, Maschinelles Lernen, S. 9 f.

180 *Mysegades*, Software als Beweiswerkzeug, S. 258 f.

181 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 260 f.

182 *Rückert*, Mit künstlicher Intelligenz auf Verbrecherjagd: Einsatz von Gesichtserkennungstechnologie zur Aufklärung der „Kapitolverbrechen", Verfassungsblog, 22.1.2021, https://verfassungsblog.de/ki-verbrecherjagd/ [26.6.2023]; vgl. auch zur intelligenten Videoüberwachung, *Mysegades*, Software als Beweiswerkzeug, S. 35 f.

183 https://news.microsoft.com/de-de/ki-im-einsatz-gegen-kinderpornografie/ [10.4.2023].

184 *Hare/Hofmann/Carriquiry*, Law, Probability and Risk (2017) Vol. 16, S. 203 ff.

185 https://polarisproject.org/ [23.4.2023]; *Ferguson*, The Rise of Big Data Policing, S. 117 f.

186 Vgl. hierzu auch https://netzpolitik.org/2024/polizei-und-ki-vom-iris-scan-bis-zum-automatischen-aufstandsmelder/ [7.11.2024].

187 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 15, S. 18 ff.: In der Regel kommen opake Softwareauswertungen vor, wenn die Software Prämissen, Datengrundlagen oder Methoden nutzt, die nach außen nicht ohne Weiteres erkennbar sind. Bei komplizierterer und umfangreicherer Software kommt auch in Betracht, dass die vorgenommene Rechnung oder das zugrundeliegende Modell so kompliziert ist, dass sie praktisch nicht im Einzelnen oder „händisch" nachvollziehbar ist.

c) Folgen für das Beweisrecht

Die Anwendung solcher Programme muss in der Praxis der Strafverfolgung aufgrund der Komplexität des Anwendungsvorgangs und der Fehleranfälligkeit i. d. R. durch spezialisierte IT-Forensiker der Strafverfolgungsbehörden oder extern beauftragte IT-Sachverständige erfolgen.[188] Sind die Daten in eine menschenlesbare Form übersetzt und die Informationen aus den Daten gewonnen, stellt sich für das Tatgericht und die sonstigen Verfahrensbeteiligten das Problem, dass sie den „Weg" der Daten bis zur menschenverstehbaren Information zu Teilen nur schwer nachvollziehen und keinen Zugang zu einer Einschätzung bzw. Quantifizierung einer Richtigkeitswahrscheinlichkeit der Datenverarbeitung vornehmen können. Das Tatgericht muss sich mit der beschränkten Richtigkeitsgewähr von Datenverarbeitungen und ggf. bestehenden Mängeln in der Nachvollziehbarkeit dieser Vorgänge vor dem Hintergrund der Amtsaufklärungspflicht und der Pflicht zur Suche nach der „materiellen Wahrheit" nach § 244 Abs. 2 StPO stellen (siehe dazu auch schon im 2. Teil, B. I. 1.). Da das deutsche Strafverfahrensrecht – anders als in anderen Rechtsräumen – grds. keine gesetzlichen Beweisregeln kennt, müssen die Tatrichter außerdem die mangelhafte Zuverlässigkeit und die fehlende Nachvollziehbarkeit im Rahmen ihrer freien richterlichen Beweiswürdigung nach § 261 StPO berücksichtigen.[189] Problematisch ist in diesem Zusammenhang, dass für die Anwendung der Grundsätze über die wissenschaftlich gesicherten Erkenntnisse eine Richtigkeitsgewähr der Ergebnisse mit „an Sicherheit grenzender Wahrscheinlichkeit" notwendig ist (siehe dazu im 4. Teil, A. III. 4. b) cc) (2) (a)). Ob ein derart hoher Grad der Richtigkeitswahrscheinlichkeit von einer angewendeten Methodik garantiert werden kann, muss anhand dieser Einteilung der Datenanalysemethoden in deterministische, statistische und selbstlernende Methoden bestimmt werden (siehe dazu im 4. Teil, A. III. 4. b) cc) (2)).[190]

3. Die Rekonstruktion des Tathergangs mit Assoziation mithilfe digitaler Spuren

Im Folgenden soll nun spezifischer an der Analyse und in diesem Zusammenhang an der Rekonstruktion des Tathergangs mithilfe von Assoziationen angeknüpft werden. Dabei geht es sowohl um die forensische Befundermittlung mithilfe von Datenverarbeitungsmethoden unter Bezugnahme ihrer zu-

---

188 So auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 22; *Mysegades*, Software als Beweiswerkzeug, S. 169.

189 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 23.

190 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 673 ff.

grundeliegenden Richtigkeitswahrscheinlichkeit, aber auch um Schlussfolgerungen im Allgemeinen.

Ziel der Strafverfolgungsbehörden ist die Rekonstruktion des wahren Tathergangs unter Einbeziehung der aufgefundenen Spuren. Praktisch werden jeweils Hypothesen über eine Menge von möglichen Tathergängen aufgestellt, die den aufgefundenen Spuren nicht widersprechen.[191]

Gemäß der Theorie des Transfers bei physischen Spuren nimmt man an, dass alle Spuren ausschließlich auf den Prinzipien der Zerteilbarkeit und des Transfers beruhen (siehe dazu bei B. II.).[192] Spuren sind dann jeweils Hinweise auf einen Kontakt zwischen zwei Objekten. Assoziation bezeichnet wiederum den Vorgang, bei dem der Kontakt zwischen zwei Objekten festgestellt wird.[193] Als Ergebnis der Assoziation steht ein Ereignis.[194]

Rekonstruktion bedeutet nun, alle ermittelten Ereignisse in einen räumlichen und zeitlichen Zusammenhang zu bringen, wobei alle diese Ereignisse individuell hergeleitet und begründet werden müssen.[195] Diese gutachterlichen Schlussfolgerungen von Sachverständigen (i. S. d. Zweiten Aussagekategorie) beinhalten neben diesen logischen Konzepten, aber auch subjektive Elemente (Ungenauigkeiten durch persönliche Einschätzungen bis hin zu menschlichen Irrtümern), die kategorische Feststellungen nicht zulassen und auch aus diesem Grund nur Wahrscheinlichkeitsaussagen sein können (siehe weiter dazu unter 3. d)).[196]

a) Die Quantifizierung der Irrtumswahrscheinlichkeit

In diesem Sinne muss ein wesentlicher Bestandteil der Assoziation die Quantifizierung der Irrtumswahrscheinlichkeit sein. Die Irrtumswahrscheinlichkeit beziffert die „Überzeugungskraft" der Assoziation im Gerichtsverfah-

---

191 *Dewald/Freiling*, Forensische Informatik, S. 48.

192 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 47 m. w. N.

193 Beispiele: Die Zuordnung eines konkreten Schuhs zu einem konkreten Schuhabdruck. Die Zuordnung einer konkreten Kugel zu einer konkreten Waffe. Die Zuordnung einer konkreten Blutspur zu einer konkreten Person. Die Zuordnung eines konkreten Fingerabdrucks zu einer konkreten Person.

194 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 48. Beispiele: Person P war am Ort X (etwa weil Fingerabdrücke von P am Ort X gefunden wurden). Ein Schuh S war am Ort Y (etwa weil S einen charakteristischen Sohlenabdruck an Ort Y hinterlassen hat). Ein Auto A war am selben Ort, an dem auch Person Q war (etwa weil man Blutspuren von Q auf der Motorhaube von A gefunden hat).

195 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 48.

196 Vgl. *Köller/Nissen/Rieß/Sadorf*, Probabilistische Schlussfolgerungen, S. 58 f., deren Ausführungen sich vordergründig auf die Anfertigung von Schriftgutachten beziehen. Sie lassen sich aber auch auf andere Disziplinen übertragen.

ren. Entweder genügen Richtwerte oder die Angabe von echten Quantifizierungen. Das wird v. a. im Rahmen der objektiven Tatsachengrundlage (§ 261 StPO) bei der Bestimmung der Beweiskraft von Indizien, genauer der Zuverlässigkeit der zugrundeliegenden Häufigkeitsverteilung, wichtig (siehe im 4. Teil, A. III. 4.).

Die Berechnung der Irrtumswahrscheinlichkeit ist, wie auch im Bereich der klassischen Forensik, immer abhängig vom Kontext. Meist müssen sehr viele Annahmen getroffen werden, um zu einer Berechnungsgrundlage zu kommen. In den klassischen forensischen Wissenschaften wird die Quantifizierung von Assoziationsaussagen unterschiedlich gehandhabt: Häufig haben sich in der Praxis Richtwerte herausgebildet, die allgemein als Nachweis einer Assoziation akzeptiert werden (ohne exakte Quantifizierung). Ein Beispiel ist der Bereich der Daktyloskopie. Hier werden Fingerabdrücke auf bestimmte Merkmale hin untersucht (z. B. das Zusammenlaufen oder Auseinandergehen von Hautrillen an bestimmten Punkten des Fingers). Fingerabdrücke werden als übereinstimmend angesehen, wenn es eine bestimmte Mindestanzahl (acht oder zwölf) übereinstimmender Merkmale und keine widersprüchlichen Merkmale gibt.[197] Eine echte Quantifizierung hingegen würde eine Aussage treffen, bei wie vielen Personen eine spezifische Kombination von Merkmalen vorkommt. Weisen sowohl die Abdrücke am Tatort als auch die Abdrücke einer verdächtigen Person diese Merkmalskombination auf, dann kann man die Irrtumswahrscheinlichkeit der Assoziation bestimmen. Weist bspw. eine Person von 10.000 Personen die Merkmalskombination auf, dann beträgt die Irrtumswahrscheinlichkeit 1:10.000. Repräsentative Studien über die Verteilung von Merkmalen in der Bevölkerung sind allerdings rar. Besonders gut untersucht sind Merkmalsverteilungen und entsprechende Wahrscheinlichkeiten im Bereich der DNA-Analyse. Hier gibt es relativ viele und umfassende Studien über die Verteilung von bestimmten Merkmalen in der menschlichen Erbsubstanz. Liegt genügend DNA-Material vor, kann man Wahrscheinlichkeiten berechnen, die eine bestimmte Person „identifizieren" können (bspw. bei einer Irrtumswahrscheinlichkeit von 1:25 Milliarden).[198] Es besteht aber auch bei der DNA-Analyse die Gefahr einer fälschlichen Assoziation, nämlich durch verunreinigte, vertauschte oder falsch beschriftete Spuren.

Bei vielen Fällen in der Praxis ist es schwierig, die Irrtumswahrscheinlichkeit der Assoziation anzugeben. Trotzdem sollte bei jeder Assoziation hinterfragt werden, auf welcher Basis der Schluss erfolgte.[199] Denn die Assoziation und das daraus resultierende Ereignis sind nur das Endergebnis einer Folge

197 *Garrett*, Autopsy of a Crime Lab, S. 41 ff.; *Neuhaus/Artkämper*, Kriminaltechnik und Beweisführung im Strafverfahren, S. 82 ff.

198 *Benecke*, Genetischer Fingerabdruck, S. 7 f.

199 *Dewald/Freiling*, Forensische Informatik, S. 49 f.

von Schritten, die nach und nach die Mengen der zueinander passenden Objekte derart einschränken, dass am Ende nur zwei Objekte übrigbleiben: Identifizierung, anschließend Klassifizierung und Individualisierung einer Spur.[200]

Der Prozess der Assoziation gilt für die forensische Informatik analog zu jenem aus der klassischen Forensik. In der digitalen Welt kann man jedoch nur den Kontakt von digitalen Objekten feststellen. Formal werden hierbei Ähnlichkeiten in den Speicherinhalten zugrunde gelegt, die den Zustandsraum des Computers ausmachen. Findet man bspw. eine inhaltsgleiche Datei an zwei Orten (im gleichen Dateisystem oder auf Festplatten unterschiedlicher Rechner), dann kann die Hypothese einer gemeinsamen Quelle aufgestellt werden. Ziel ist die Assoziation zweier Datenobjekte (Bitfolgen) auf Basis von Musterübertragung.[201]

b) Identifizierung/Klassifizierung/Individualisierung/Assoziation

Bei der Identifizierung wird die prinzipielle Tauglichkeit der Spur als Beweismittel geprüft. Es wird gefragt: Was ist es? Identifikation kann charakterisiert werden als die Einschränkung der potentiellen Spuren am Tatort „mit bloßem Auge".[202] Bspw. muss eine Blutspur zunächst gefunden und dann als Blutspur erkannt werden. In der forensischen Informatik kann die Spur selbst eine beliebige Bitfolge sein, die potentiellen Tatbezug aufweist, etwa weil sie auf einer Festplatte liegt, die am Tatort gefunden wurde. Aber nicht alle Bitfolgen müssen auch Spuren sein. Die Identifizierung unterscheidet diese beiden Fälle. Ziel der folgenden Schritte ist, das „Gegenstück" der gefundenen Spur zu finden, wie die Quelle, aus der die Bitfolge stammt, oder die Umstände/Aktionen, die beim Entstehen der Bitfolge stattgefunden haben müssen.[203]

Bei der Klassifizierung einer Spur wird die Menge der Spuren weiter eingegrenzt durch eine genauere Analyse der Form, der Größe, des Gewichts, der Temperatur oder der Oberflächenstruktur des Gegenstandes. Hier muss die Frage lauten: Zu welcher Klasse von Gegenständen gehört das Objekt? Charakteristisch für die Klassifizierung ist die Tatsache, dass man spezielle Werkzeuge wie eine Waage, ein Längenmaß, ein Mikroskop oder einen chemischen Test benötigt. Z. B. kann die Herkunft eines am Tatort gefundenen länglichen

---

200 *Dewald/Freiling*, Forensische Informatik, S. 50. M. w. N.

201 *Dewald/Freiling*, Forensische Informatik, S. 76.

202 *Dewald/Freiling*, Forensische Informatik, S. 50 f.

203 *Dewald/Freiling*, Forensische Informatik, S. 76; Das entspricht auch dem forensischen Prozess, den andere beschreiben als „authentication, identification, classification, reconstruction, and evaluation of traces", vgl. https://serval.unil.ch/resource/serval:BIB_32FB580596A3.P001/REF.pdf [2.7.2024].

Gegenstandes zunächst als biologisch klassifiziert werden. Weitere Untersuchungen erlauben dann die genauere Klassifizierung als Haar, und schließlich als menschliches Haar. Klassifizierungsmerkmale entstehen regelmäßig aus kontrollierten Herstellungsprozessen, die dann jeweils charakteristisch für die Klasse von Objekten sind.[204] Im Falle digitaler Spuren sind etwa Dateinamenssuffixe (die den Typ einer Datei andeuten) oder die Entropie einer Datei klassifizierende Merkmale.[205]

Mit Individualisierung bezeichnet man die Zuordnung der Spur zu einer eng umgrenzten Menge von Objekten, die potentiell die Spur verursacht haben könnten.[206] Idealerweise führt die Individualisierung zu einer 1:1-Zuordnung zwischen Spur und dem Referenzobjekt, das die Spur verursacht hat. Die Merkmale, die eine Individualisierung erlauben, entstammen i. d. R. zufälligen und unkontrollierten Prozessen, wie sie bspw. durch Abnutzung geschehen.[207] Individualisierende Merkmale im Bereich der digitalen Spuren sind z. B. Nutzungsspuren, die durch menschliche Benutzer verursacht worden sind, also Inhalte von Dokumenten oder Logdateien menschlicher Interaktionen. Auch Spuren von Systemaktivitäten können individualisierend sein, wie die Namen von temporären Dateien oder die Wahl zufälliger Schlüssel bei der Datenübertragung (siehe diesbezüglich auch bei II. 3. b) und e)).[208]

Unter bestimmten Voraussetzungen ist es gar nicht notwendig, die ganze Wegstrecke bis hin zu einer Individualisierung gehen zu müssen. Abhängig vom Delikt kann manchmal schon nach der Identifizierung oder der Klassifizierung aufgehört werden. Ein Beispiel wäre die Identifizierung oder Klassifizierung von bestimmten Betäubungsmitteln, deren Besitz bereits unter Strafe stehen kann (zumindest nach aktueller Rechtslage). Es ist dann für die Ermittlung meist nicht mehr relevant, von welchem Dealer oder aus welchem Drogenlabor das Objekt genau stammt. Ein anderes Beispiel ist der Besitz kinder- oder jugendpornographischer Inhalte. Für die Ermittlung der Umstände einer Straftat mag relevant sein, woher diese bezogen wurden (Individualisierung). Für die Anklage kann allerdings bereits die Klassifizierung eines Dokuments ausreichen.[209]

---

204 *Dewald/Freiling*, Forensische Informatik, S. 51.

205 *Dewald/Freiling*, Forensische Informatik, S. 77.

206 Der Begriff wird fälschlicherweise oft verengt als die Zuordnung einer Spur zu einem Individuum verstanden.

207 *Dewald/Freiling*, Forensische Informatik, S. 51.

208 *Dewald/Freiling*, Forensische Informatik, S. 77.

209 *Dewald/Freiling*, Forensische Informatik, S. 53.

c) Beispiele (USB/Browser)

Um die Art der Assoziation in der digitalen Welt besser zu veranschaulichen, soll der Prozess anhand zweier Beispiele veranschaulicht werden.[210]

Beispiel anhand von USB-Speichergeräten[211]: Zunächst soll die Assoziation zwischen einem Wechseldatenträger und einem bestimmten Computer betrachtet werden. Speichergeräte werden regelmäßig über den Universal Serial Bus (USB) an einen Computer angeschlossen. Betriebssysteme sammeln dabei Informationen über die an das System angeschlossenen Datenträger und nutzen die individuellen Charakteristika eines Speichergerätes, um z. B. den korrekten Gerätetreiber auszuwählen.[212] Diese Tatsache kann es ermöglichen, Aussagen wie „USB-Stick A war schon einmal mit Computer B verbunden" zu treffen.

Identifikation: Objekt A ist in diesem Fall ein kleines Plastikobjekt mit einem Metallende, das am Tatort gefunden wurde. Es wird davon ausgegangen, dass es sich um eine Ermittlung bzgl. Datendiebstahls i. S. d. § 202a StGB handelt. Das sollte ausreichen, um Objekt A als potentielles Beweismittel zu identifizieren.

Klassifizierung: Eine weitergehende Untersuchung auf klassifizierende Merkmale des Gerätes ergibt, dass es sich bei Objekt A tatsächlich um ein USB-Massenspeichergerät einer bestimmten Marke handelt. Die Klasse der Objekte B, zu denen Objekt A assoziiert werden könnte, umfasst zu diesem Zeitpunkt die Menge aller Computersysteme, die über eine USB-Schnittstelle verfügen.

Individualisierung: Unterstellt wird in diesem Zusammenhang das Vorhandensein einer Menge von Computern (von verschiedenen Verdächtigen), die ebenfalls sichergestellt wurden, und dass auf all diesen Geräten Microsoft Windows als Betriebssystem eingesetzt wird. Sobald ein USB-Speichergerät an ein Windows-System angeschlossen wird, erstellt das Betriebssystem eine „Geräteinstanzkennung" (device instance identifier) auf Basis unterschiedlicher auf dem Gerät hinterlegter Werte (wie die eindeutige Seriennummer). Diese Geräteinstanzkennungen werden unter Windows in der Windows Registrierung (Registry) gespeichert und können unter Einsatz entsprechender Software extrahiert werden.[213] Weitere individualisierende Merkmale könnten in einer bestimmten Menge von Dateien bestehen, die sich sowohl auf Objekt A als auch auf Objekt B befinden.

---

210 *Dewald/Freiling*, Forensische Informatik, S. 78 f.

211 *Dewald/Freiling*, Forensische Informatik, S. 78.

212 *Carvey/Altheide*, Digital Investigation (2005) Vol. 2, S. 94 f.

213 *Carvey/Altheide*, Digital Investigation (2005) Vol. 2, S. 94 f.

Assoziation: Das Auffinden der einzigartigen Gerätekennung eines USB-Speichergerätes an einer bestimmten Stelle auf einem Computersystem ist ein starkes Indiz dafür, dass dieses konkrete Gerät (Objekt A) in der Vergangenheit einmal an diesen konkreten Computer (Objekt B) angeschlossen war.[214]

Ein weiteres Beispiel ist der Browser Cache[215]: Aus Performanz-Gründen sichern Webbrowser regelmäßig lokale Kopien besuchter Webseiten in Cache-Dateien, um diese bei einem erneuten Aufruf der Webseiten nicht nochmals herunterladen zu müssen. Diese Dateien gehören zu den System-Sekundärdaten (siehe dazu bereits unter B. II. 3. b) und e)) und sind äußerst interessant für IT-Sachverständige, um zu rekonstruieren, welche Webseiten von einem Benutzer eines Computers in der Vergangenheit aufgerufen wurden. Das bedeutet, dass es Cache-Dateien ermöglichen, eine Verbindung zwischen einem bestimmten Computer (Objekt A) und einer konkreten Webseite (Objekt B) herzustellen. Der Prozess der Assoziation kann in einem solchen Fall (und wird in den meisten Fällen bereits implizit) auf folgende Art und Weise angewandt werden:

Identifikation: Auf den ersten Blick könnte der IT-Sachverständige Dateien unter einem bestimmten Pfad im Dateisystem vorfinden, von dem bekannt ist, dass er üblicherweise von einem bestimmten Webbrowser für die Sicherung von Cache-Dateien genutzt wird. Daher könnte der Sachverständige in diesem Schritt zu dem Schluss kommen, dass diese Dateien potentiell zum Browser-Cache gehören könnten und sie daher als potentielle Spuren identifizieren.

Klassifizierung: Im nächsten Schritt benötigt der IT-Sachverständige typischerweise irgendeine Art von (Software-)Werkzeug, um weitere Schlüsse ziehen zu können. Abhängig von dem Webbrowser, der die Cache-Dateien erzeugt hat, kann z. B. ein spezieller Parser für das konkrete Dateiformat eingesetzt werden, um zu verifizieren, dass die identifizierten Dateien tatsächlich zum Cache des betreffenden Browsers gehören.

Klassifizierung: Diese Spuren entstehen durch einen bekannten und kontrollierten Herstellungsprozess, da dieser Webbrowser bekanntermaßen immer (so lange nicht manuell anderweitig konfiguriert) Cache-Dateien unter diesem bestimmten Pfad und Dateinamen in diesem konkreten Format speichert. Das ist ein wichtiges Kriterium für die Unterscheidung der Klassifizierung und der Individualisierung. Das Ergebnis dieses Schrittes ist, dass diese Dateien tatsächlich Cache-Dateien dieses Webbrowsers sind.

Individualisierung: Schließlich werden die eigentlichen Inhalte der als Cache klassifizierten Dateien untersucht. Hierzu kommen meist wiederum Werkzeuge zum Einsatz, wie Bildbetrachtungssoftware zur Darstellung ge-

214 *Dewald/Freiling*, Forensische Informatik, S. 80 f.

215 *Dewald/Freiling*, Forensische Informatik, S. 82 f.

cachter Bilddateien oder ein Webbrowser, um zwischengespeicherte HTML-Dateien zu rendern. In diesem Schritt versucht der IT-Sachverständige herauszufinden, um welche konkreten Inhalte es sich handelt. In Abhängigkeit vom bereits erwähnten Format der Dateien und dem eingesetzten Betriebssystem, können auch weitere Informationen, wie Zeitstempel oder der Name des Benutzers, der das Cachen der Webseite verursacht hat, zur Verfügung stehen. Auch die Herkunft der Inhalte (die URL, von der sie durch den Browser heruntergeladen wurden) können ausgelesen werden. Diese Art von Spuren unterliegen für gewöhnlich einem unbewussten Entstehungsprozess, da die Tatsache, dass ein Benutzer mit diesem konkreten Benutzernamen das Cachen dieser konkreten Webseite mit diesen Inhalten zu genau dieser Zeit anstößt, höchst individuell ist. Daher ist es als unwahrscheinlich anzusehen, dass sich ein zweiter Computer (insbesondere im Kreis der Verdächtigen) findet, der exakt die gleichen (und nur diese) Spuren aufweist. Als Ergebnis der Individualisierung würde der IT-Sachverständige feststellen, dass auf dem untersuchten System dieser konkrete Webbrowser zur spezifizierten Zeit diese Inhalte geladen und daher gecacht hat.[216] Bei Browsern neuester Generation könnte diese Aussage zum Teil nur weniger scharf formuliert werden, da zum Teil Inhalte von Webseiten im Voraus geladen werden, wenn sie von der aktuell betrachteten Seite verlinkt werden.

Assoziation: Als Ergebnis der vorausgegangenen Schritte ist der IT-Sachverständige in der Lage, eine Assoziation zwischen einem konkreten Benutzer des untersuchten Systems und einer Webseite herzustellen. Außerdem kennt er den Zeitpunkt des Ereignisses (den Aufruf der Website) und die geladenen Inhalte.[217]

d) Verwendung von Wahrscheinlichkeiten

Nicht nur in Bezug auf die Quantifizierung von Irrtumswahrscheinlichkeiten bei der sachverständigen Tätigkeit, sondern auch und v. a. im Rahmen der (mündlichen) Gutachtenerstattung, wird der IT-Sachverständige von den Verfahrensbeteiligten regelmäßig nach der Richtigkeitswahrscheinlichkeit der Assoziationen bzw. allgemein seiner Ergebnisse gefragt – sowohl in Bezug auf die Befundermittlung, als auch in Bezug auf Schlussfolgerungen und Erfahrungssätze.

Der Grund für die Notwendigkeit von Wahrscheinlichkeitsaussagen ist darin zu sehen, dass die forensische Informatik im Rahmen einer empirischen Wissenschaft stattfindet. Dabei generierte Befunde treten nicht mit Sicherheit

---

216 *Dewald/Freiling*, Forensische Informatik, S. 82 f.

217 Häufige Ausrede ist dann: Der Computer sei für viele Leute zugänglich.

auf, sondern sie sind statistische Ereignisse.[218] Ein zusätzlicher subjektiver Grund für die Notwendigkeit von Wahrscheinlichkeitsaussagen ist die Ungenauigkeit und Unvollkommenheit des menschlichen Urteilsvermögens. Da der Sachverständige um sie weiß, sind die Irrtumsmöglichkeit und die daraus hervorgehende Fehleranfälligkeit in den Sicherheitsgrad der Schlussfolgerung einzubeziehen (siehe dazu bereits unter 3. a)).[219]

In diesem Rahmen sei kurz angemerkt, dass dem Sachverständigen oft – fälschlicherweise – vermittelt wird, dass er sein Gutachten (wie die Richterin wiederum ihr Urteil) nicht auf Wahrscheinlichkeiten, sondern auf Gewissheiten aufbauen müsste.[220]

Welchen Grad an Sicherheit die Folgerungen eines Gutachtens haben müssen, um beim Richter das für die Überzeugungsbildung notwendige Maß an Gewissheit zu erzeugen, lässt sich generalisierend nicht festlegen[221] und ist auch keine Frage des Fachs, sondern hängt von den jeweiligen Fallgegebenheiten ab. Aber auch ein Gutachten, in dem der Sachverständige nahezu nichts als gesichert bezeichnen kann und alles in der Schwebe lassen muss, kann dennoch eine „rechtliche Sicherheit" vermitteln, nämlich die des nicht aufklärbaren, möglicherweise weiteren Zweifels oder des non liquet, wie ebenso ein mit großer Sicherheit erkannter Befund auch nur die gleiche „rechtliche Sicherheit (oder Unsicherheit)" anbieten kann. So kann es keine rechtlichen Anforderungen an die Sicherheit eines sachverständigen Gutachtens geben. Die Forderung an den Sachverständigen ist eine tatsächliche: im Gutachten sein Wissen zu den vom Gericht angegebenen Themen oder Fragen kundzutun. Wenn der Sachverständige dem nachkommt, erfüllt er den an ihn ergangenen Auftrag.[222] Das mag mal sorgfältiger, mal weniger sorgfältig geschehen bzw. einmal mehr und einmal weniger präzise Ergebnisse haben und deshalb für den Auftraggeber mal mehr und mal weniger hilfreich sein.

Nach der Befunderhebung erfolgt die Beantwortung der Untersuchungsfrage im Gutachten oft durch eine in verbalen Wahrscheinlichkeitsgraden von Hypothesen formulierte Schlussfolgerung des Sachverständigen. So definiert

---

218 Die empirischen Wissenschaften bieten als methodischen Weg hypothesenbegleitete Vorgehensweisen innerhalb der Inferenzstatistik und im Besonderen nach der Bayes-Logik zur Erlangung von Wahrscheinlichkeitsaussagen an. Im Zusammenhang mit dem IT-Sachverständigenbeweis kommen grds. vier Arten der Wahrscheinlichkeiten zum Einsatz: 1) klassische Wahrscheinlichkeit, 2) statistische Wahrscheinlichkeit, 3) subjektive/personelle Wahrscheinlichkeit und 4) die logische Wahrscheinlichkeit. Vgl. auch *Köller/Nissen/Rieß/Sadorf*, Probabilistische Schlussfolgerungen, S. 6.

219 Vgl. *Köller/Nissen/Rieß/Sadorf*, Probabilistische Schlussfolgerungen, S. 2.

220 Vgl. Löwe/Rosenberg/*Krause*, § 78 Rn. 8; kritisch dazu *Walter*, Sachverständigenbeweis, S. 121 f.

221 *Walter*, Sachverständigenbeweis, S. 122.

222 *Walter*, Sachverständigenbeweis, S. 123.

Casey[223] sieben qualitative Grade von Wahrscheinlichkeit. Diese Stufen verbindet er mit sprachlichen Ausdrücken, die in Gutachten oder vor Gericht verwendet werden können:

1) Das Ereignis ist fehlerhaft/inkorrekt (C0). Die Spuren widersprechen bekannten Fakten bzw. Erfahrungssätzen oder stimmen nicht überein. Z. B. wäre die Behauptung, eine Person hätte absichtlich und manuell diese Spam-Nachrichten verschickt, fehlerhaft, wenn ein gesicherter Erfahrungssatz besteht, dass der Versand von Spam durch bekannte Formen von Schadsoftware durchgeführt wird.

2) Das Ereignis ist sehr unwahrscheinlich (C1). Die Spuren sind fragwürdig. Die Assoziation, die 80-jährige pensionierte Dame, in deren abhandengekommenen Handtasche die verfahrensgegenständliche externe Festplatte gefunden wurde, wäre die Inhaberin der dort gespeicherten diversen Kryptowallets, wäre sehr unwahrscheinlich.

3) Das Ereignis ist unwahrscheinlich (C2). Es gibt nur eine Quelle für die digitale Spur und diese Quelle war nicht geschützt vor Manipulationen. So wäre das Ergebnis, der Verdächtige könne auf dem Video der Überwachungskamera indentifiziert werden, unwahrscheinlich, wenn Spuren von Bildbearbeitungssoftware auf dem Videomaterial gefunden werden konnten.

4) Das Ereignis ist möglich (C3). Die Quelle(n) der digitalen Spur sind schwerer zu manipulieren als im Fall C2, aber es gibt entweder nicht genügend Spuren oder die Spuren sind inkonsistent. So wäre das Ergebnis der angemeldete Nutzer X des Laptops Y wäre wissentlicher Besitzer jugendpornografischer Inhalte lediglich „möglich“, wenn sich diese mglw. (unentdeckt) in einer ZIP-Datei mit anderem pornografischem Material befunden haben. Die IT-Forensiker müssen dann nach Indizien suchen, die für oder gegen die Einlassungen sprechen, z. B. willentlich gespeichert, systembedingt erzeugte (Cache) oder gelöschte Dateien.

5) Das Ereignis ist wahrscheinlich (C4). Entweder ist die digitale Spur gegen Manipulationen geschützt gewesen, oder es existieren mehrere unabhängige und übereinstimmende digitale Spuren. Beispiele sind konsistente Spuren auf der Festplatte eines mutmaßlichen Erpressers: Die Erpressungs-E-Mail als Kopie im Postausgang sowie mehrere Entwürfe derselben E-Mail und elektronische Kontoauszüge, die den Eingang des abgepressten Geldes auf dem Konto des Beschuldigten dokumentieren.

6) Das Ereignis ist sehr wahrscheinlich (C5). Es gibt mehrere unabhängige und übereinstimmende digitale Spuren, die zudem vor Manipulationen ge-

223 *Casey*, Digital Evidence and Computer Crime (2011), S. 69 f.: „levels of certainty“.

schützt waren. Allerdings existieren kleinere Inkonsistenzen, beispielsweise leichte Abweichungen der Zeitstempel. Wenn etwa die IP-Quelladresse von bösartigem Netzwerkverkehr auf einen Anschluss X aufgelöst wird und zusätzlich durch die Überwachung von Netzwerkverkehr festgestellt wird, dass derselbe Verkehr vom Anschluss X kommt, dann ist es sehr wahrscheinlich, dass die Aktivitäten in der Tat über den Anschluss X ins Netz gelangten.

7) Das Ereignis ist sicher (C6). Die digitalen Spuren waren vor Manipulationen geschützt oder haben hohe statistische Konfidenz. Beispiele sind Funde von inkriminierten Dateien auf einer Festplatte, die neben einer visuellen Inspektion auch über ihre kryptographischen Fingerabdrücke (mittels kryptographischer Hashfunktionen) als solche identifiziert werden können.[224]

Betont wird allerdings auch, dass diese Stufen weiterhin subjektiv bleiben: Verschiedene IT-Sachverständige können auf Basis derselben Spuren zu unterschiedlichen Einschätzungen kommen. Insofern sei die Skala auch nur als ein erster Ansatz zu verstehen, welcher noch weiter erforscht werden muss. Aus einer aktuellen Untersuchung von Sunde[225] ergibt sich, dass bei sachverständigen Gutachten (aus verschiedenen Disziplinen, darunter auch der forensischen Informatik), neben anderen teils erheblichen Mängeln[226], eine große Vielfalt von Gewissheitsausdrücken verwendet wurde i. V. m. dem Fehlen einer Bedeutungserklärung oder eines Verweises auf einen Standardrahmen. Das deutet darauf hin, dass Standards wie eine Gewissheitsskala oder die Gewissheitsdeskriptoren für digitale Beweise nicht ausreichend bekannt sind und/oder umgesetzt werden.[227]

Generell basiert aber bereits die Quantifizierung einer relativ einfachen Aussage wie „Der Nutzer hat Datei X über die Tauschbörse Y bezogen" auf einer Vielzahl von Annahmen. Sie alle aufzuzählen und darauf eine komplexe Berechnung aufzubauen, erscheint generell möglich, ist aber nur für sehr eingeschränkte und sehr exakt fassbare Aussagen sinnvoll.[228]

Zudem muss wie in der klassischen Forensik zwischen zwei Wahrscheinlichkeiten unterschieden werden.

---

224 *Dewald/Freiling*, Forensische Informatik, S. 87 f.

225 *Sunde*, Science & Justice (2021) Vol. 61, S. 586 (593).

226 Wichtige Informationen fehlen, sind vage oder wurden fehlerhaft dargestellt.

227 Das bestätigt auch die Akteneinsicht der Autorin.

228 *Overill et al.*, Quantification of digital hypotheses using probability theory, S. 1 ff.; *Overill/Silomon*, Uncertainty Bounds for Digital Forensic Evidence and Hypotheses, S. 590; *Overill et al.*, A Complexity Based Model for Quantifying Forensic Evidential Probabilities, S. 671 ff. vgl. Auch *Deuber et al.*, Argumentation Schemes for Blockchain Deanonymization (vorgestelltes Paper bei JURISIN 2022), https://doi.org/10.48550/arXiv.2305.16883 [26.6.2023].

1. Die Irrtumswahrscheinlichkeit bei der Interpretation einer digitalen Spur, und

2. die Wahrscheinlichkeit, mit der die digitale Spur unverfälscht vorliegt.

In der klassischen Forensik gibt es im Kontext der vermeintlich so objektiven DNA-Analyse immer wieder Pannen, die vor allem die zweite Wahrscheinlichkeit beeinflussen (etwa die Kontamination des Spurenträgers wie beim „Phantom von Heilbronn“[229]).[230] Gerade die zweite Wahrscheinlichkeit muss bei der Anfälligkeit digitaler Spuren gegenüber Manipulationen besonders beachtet werden.

Sinnvoll ist die Quantifizierung der Irrtumswahrscheinlichkeit also nur bei sehr einfachen Fragestellungen, die man präzise als Assoziationen ausdrücken kann und für die einfache Basisannahmen getroffen werden können; d. h. man sollte bereits im Untersuchungsauftrag präzise Beweisfragen formulieren. Komplexere Aussagen werden insbesondere durch die Summe möglichst vieler unabhängiger (und untereinander konsistenter) Spuren überzeugend, auch wenn für sie keine exakte Irrtumswahrscheinlichkeit anzugeben ist.[231]

e) Fazit

Anhand der bisherigen Ausführungen ergibt sich, dass auch die einzelnen forensischen Schritte (v. a. in Bezug auf die Assoziation und der Besonderheiten der digitalen Spuren), der mitgeteilten Anknüpfungstatsachen, die verschiedenen Sachverständigenkategorien[232] und die dabei eingesetzten Methodiken und zugrundeliegenden Vagheiten bzw. Richtigkeitswahrscheinlichkeiten (soweit bekannt) mitzuteilen sind. In diesem Zusammenhang müssen sich die Verfahrensbeteiligten auf ein einheitliches Verständnis der verschiedenen Grade der Wahrscheinlichkeiten einigen. Dabei sollten auch Alternativhypo-

---

229 Jahrelang suchten Ermittler in drei Bundesländern nach einer mysteriösen Unbekannten, deren Spuren die Polizei an voneinander völlig unabhängigen Tatorten gesichert hatte. Es stellte sich heraus, dass die „verantwortliche“ Frau eine Verpackerin des Herstellers der Wattestäbchen war, die die Polizei zur Spurensicherung einsetzt, siehe MAH/*Neuhaus* (2. Aufl.) § 62 Rn. 28, Fn. 127; vgl. auch https://www.zeit.de/2009/15/M-Phantom [1.7.2023].

230 Siehe zur Prolematik mit der aktuellen DNA-Identifikation mittels Software auch ausführlich *Mysegades*, Software als Beweiswerkzeug, S. 250 ff.

231 *Dewald/Freiling*, Forensische Informatik, S. 89 f. Wie wichtig, aber auch schwierig die Angabe von Fehlertoleranzen ist siehe *Dror*, Journal of Forensic Sciences (2020), S. 1 ff.

232 *Sunde*, Non-technical Sources of Errors, S. 66.: „A DFD [IT Expert] told s/he normally separated the report into two parts: An objective part, and more subjective part. The subjective part was more explanatory, where the findings were put into a context, e. g. an image was sent as a result of a threat posed on a chat conversation“.

thesen dargestellt werden. Erst durch Offenlegung der syllogistischen Struktur kann eine „optimale" Beweiswürdigung erfolgen. Die Offenlegung der einzelnen Schritte der forensischen Rekonstruktion des Tathergangs schafft Transparenz und Diskutierbarkeit. Außerdem bringt es grundlegendes Verständnis für die Schritte der forensischen Informatik mit sich und ermöglicht den Verfahrensbeteiligten damit die Beweisfragen besser zu formulieren. Auch soll diese Darstellung beim Verständnis helfen bzgl. der Erörterung der Zuverlässigkeit der zugrundeliegenden Häufigkeitsverteilungen im Rahmen der objektiven Elemente zur Bestimmung der tatrichterlichen Überzeugung i. S. d. § 261 StPO.

4. Die Präsentation

Nach der StPO werden die Gutachten i. d. R. mündlich in der Hauptverhandlung erstattet. In den allermeisten Fällen lässt das Gericht bzw. die auftraggebende Strafverfolgungsbehörde ein vorbereitendes schriftliches Gutachten anfertigen.

Im 18. und 19. Jahrhundert wurde ein Sachverständigengutachten für den Richter u. a. dann als verbindlich erklärt, wenn es gründlich war.[233] Die Forderung nach einer sauberen Gutachtenerstattung ergibt sich jedenfalls nicht aus einer Detailversessenheit. Sondern es hat sich gezeigt, dass „gute" Berichte zu einer „guten" mündlichen Präsentation und Verteidigung führen.[234] Auf diese stützen die Richter ihre Urteilsfindung. Also könnte man weiter behaupten, dass dadurch auch „gute" Gerichtsentscheidungen bedingt werden – zumindest wären sie eine „gute" Basis dafür. Auch in der Praxis hat sich gezeigt, dass der Aufbau und die Ausgestaltung des Gutachtens sehr wichtig sind.[235] Ebenso entstand bei einer von der Verfasserin durchgeführten Akteneinsicht der Eindruck, dass je ordentlicher das Gutachten erstellt wurde – auch im Hinblick auf die äußere Form, Rechtschreibung, Quellenangaben und Literaturverzeichnis[236] etc. –, desto kompetenter und überzeugender wirkte der

---

233 *Mittermaier*, AcP 2 (1819), S. 119 (135, 137, 140) m. w. N.; zur Bindungswirkung vgl. auch *Poppen*, Die Geschichte des Sachverständigenbeweises, S. 116 ff.

234 *Frank*, Quality measurements of digital forensics analysis reports, S. 48.

235 Vgl. bspw. Vorgaben zum Aufbau von schriftlichen Gutachten hier: *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige, Rn. 331 ff.

236 *Vogel/Volkmann*, GesR 2021, 753 (758 f.).: „Wer darüber hinaus häufige Fehler auf Sachverständigenseite vermeiden und ein ‚perfektes' Gutachten befördern will, mag in dem Gutachtenauftrag noch auf ein korrektes Literaturverzeichnis hinweisen. Das zwingt den Gutachter, seine Bewertung nicht lediglich auf eigene Erfahrung zu gründen, sondern nachzulesen und überhaupt ein Literaturverzeichnis beizufügen. Überdies werden Fehler vermieden dergestalt, dass die Literatur zu neu ist oder nicht neu genug."

Inhalt (jedenfalls aus einer juristischen und technisch laienhaften Perspektive). So sollte auch im 21. Jahrhundert der Forderung einer ordentlichen Gutachtenerstattung Nachdruck verliehen werden.

Bei der Art und Weise der Anfertigung sind die IT-Sachverständigen zunächst grds. frei (siehe hierzu vertieftere Ausführungen im 2. Teil, B. II. 3.). Seit 2016 regelt § 407a ZPO allerdings einige Einzelheiten zu den Pflichten gerichtlicher Sachverständiger. Die Vorschrift gilt gem. § 98 VwGO entsprechend im Verwaltungsgerichtsverfahren und analog auch im Strafverfahren.[237] Zudem existieren in anderen forensischen Bereichen unverbindliche interdisziplinäre Leitlinien[238] auf Grundlage der höchstrichterlichen Rspr.; so z. B. für psychiatrische Gutachten zur Schuldfähigkeit[239] und die Prognose zukünftigen Verhaltens.[240] Der BGH hat etwa zu psychologischen Glaubwürdigkeitsgutachten umfangreiche Anforderungen aufgestellt, deren Einhaltung Tatsachengerichte auch in den Urteilsgründen darlegen müssen.[241] Auch andere Institutionen geben Mindestanforderungen an Gutachten heraus.[242] Für den Bereich der forensischen Informatik existieren ebenso internationale verschiedene Standards, Leitlinien und bewährte Verfahren: bspw. verschiedene Manuals vom European Network of Forensic Science Institute (ENFSI)[243],

---

237 Vgl. SK-StPO/*Rogall*, Vor § 72 Rn. 67.

238 Zu Kritik und Zustimmung zu diesen siehe *Erb*, ZStW 121 (2009), 882 (902) m. w. N. Vgl. auch die formalen Vorgaben bei *Foerster/Dreßing*, in: Psychiatrische Begutachtung, S. 62 ff.

239 *Boetticher/Nedopil/Bosinski et al.*, NStZ 2005, 57 (59 ff.); vgl. auch *Foerster/Dreßing*, in: Psychiatrische Begutachtung, S. 62 (66). Ein typisiertes Beispiel eines Schuldfähigkeitsgutachtens findet sich bei *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 399 ff.; *Mysegades*, Software als Beweiswerkzeug, S. 125.

240 *Boetticher/Kröber/Müller-Isberner et al.*, NStZ 2006, 537 (541 ff.) auf Grundlage der vorherigen Vorgaben des BVerfG, Urteil v. 5.2.2004 – 2 BvR 2029/01 = BVerfGE 109, 133, Rn. 114 ff. zur Sicherungsverfahrung nach Anhörung von Sachverständigen (Rn. 61); vgl. auch *Mokros*, in: Psychiatrische Begutachtung, S. 30 (S. 47 f. m. w. N.) zu standardisierten und psychometrische Untersuchungsverfahren in der forensisch-psychiatrischen Begutachtung.

241 BGH, Urteil v. 30.07.1999 – 1 StR 618/98 = BGHSt 45, 164, zit. n. juris, Rn. 11 ff.; *Ahrens*, Der Beweis im Zivilprozess, Rn. 21 f.; *Jansen*, StV 2000, 224 (224 ff.); ausführlich hierzu *Otte*, Rechtsgrundlagen der Glaubwürdigkeitsbegutachtung von Zeugen im Strafprozess, S. 198 ff.

242 Vgl. nur die von den Industrie- und Handelskammern herausgegebenen Mindestanforderungen, siehe etwa https://www.ihk.de/koeln/hauptnavigation/recht-steuern/empfehlung-aufbau-gutachten-5289966 [18.1.2024].

243 Das Best Practice Manual für die forensische Untersuchung von digitaler Technologie (Stand: Nov. 2015), siehe http://enfsi.eu/wpcontent/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf [18.1.2024]; oder Best Practices für das digitale Imaging: Für den Gesichtsbildvergleich (Stand: Jan. 2018), siehe https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf-01.pdf [18.1.2024]; Für die Bild- und Videobearbeitung (Stand Jun. 2018), siehe https://enfsi.

Richtlinien von der International Criminal Police Organization Interpol[244], verschiedene Standards der International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), wie „guidance on assuring suitability and adequacy of incident investigative method" nach ISO/IEC 27041:2015(en)[245], „guidelines for the analysis and interpretation of digital evidence" nach ISO/IEC 27042:2015[246], „guidelines for identification, collection, acquisition and preservation of digital evidence" nach ISO/IEC 27037:2012[247], oder „general Requirements for the Competence of Testing and Calibration Laboratories" nach ISO/IEC 17025:2017[248]. Weiter gibt es das US National Institute of Standards and Technology (NIST), das immer wieder Vorschläge zur Standardisierung veröffentlicht.[249] Darüber hinaus gibt es das Template vom Forensic Science Regulator (UK) bzgl. der Methodenvalidierung in der forensischen Informatik[250], das Berkeley Protocol bzgl. OSINT-Ermittlungen[251] und verschiedene Vorschläge der Scientific Working Group on Digital Evidence (SWGDE)[252], sowie der Association of Chief Police Officers in UK (ACPO)[253]. Für Deutschland existiert außerdem der BSI-Leitfaden, der allerdings schon über 10 Jahre alt ist.[254] Praktikerinnen und Akademikerinnen der forensischen Informatik haben aber nach wie vor Be-

---

eu/wp-content/uploads/2017/06/Best-Practice-Manual-for-Forensic-Image-and-Video-Enhancement.pdf [18.1.2024]; oder für Bildauthentifizierungen (Stand: Okt. 2021), siehe https://enfsi.eu/wp-content/uploads/2022/12/1.-BPM_Image-Authentication_ENFSI-BPM-DI-03-1.pdf [18.1.2024].

244 Richtlinien für die Sicherung und Durchsicht digitaler Beweismittel (Stand: März 2021) oder die Richtlinien für die Labore der forenischen Informatik sowie die „guidelines for digital forensics first responders" unter https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics [18.1.2024].

245 https://www.iso.org/obp/ui/#iso:std:iso-iec:27041:ed-1:v1:en [18.1.2024].

246 https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en [18.1.2024].

247 https://www.iso27001security.com/html/27037.html [18.1.2024].

248 https://www.iso.org/standard/66912.html [18.1.2024].

249 https://www.nist.gov/ [18.1.2024].

250 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/921392/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf [18.1.2024].

251 https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf [18.1.2024].

252 Bspw. „Establishing confidence in digital and multimedia evidence forensic results by error mitigation analysis, Version 2.0", siehe https://fenix.tecnico.ulisboa.pt/downloadFile/845043405513436/SWGDE_Establishing_Confidence_in_Digital_Forensic_Results_by_Error_Mitigation_Analysis.pdf [18.1.2024].

253 https://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/ [18.1.2024].

254 https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/IT-Forensik/forensik_node.html [18.1.2024].

denken über den Mangel an wissenschaftlicher Validierung in der digitalen Forensik[255], während die Krise der Reproduzierbarkeit in diesem Bereich auch immer häufiger von internationalen Standardisierungs- und Regierungsgremien[256] kommentiert wird.[257] Die Diversität und die mangelnde Aktualität der eben genannten Vorschläge machen deutlich, dass universell anerkannte Mindeststandards für die Methodik und sachverständigen Schlussfolgerungen der forensischen Informatik ausgearbeitet und den juritsischen Anwenderinnen zugenänglich gemacht werden müssen (dazu sogleich unter B. III. 5.).

Für die Gutachtenerstellung bzw. die Dokumentation in den Arbeitsunterlagen im Bereich der forensischen Informatik heißt das, die sogleich erörterten Mindeststandards zugrundegelegt, im Einzelnen, dass IT-Sachverständige Befund- und Anknüpfungstatsachen, Hypothesen, Methoden und Testverfahren inkl. ihrer Leistungsfähigkeit, Erfahrungssätze inkl. ihrer Quellen offenlegen müssen. Ferner müssen sie angeben, ob sie Informationen von Dritten oder aus Datenbanken beziehen. Naheliegende oder nicht auszuschließende Fehlerquellen sind mitsamt ihrer Wahrscheinlichkeit anzugeben. Ebenfalls müssen die Grenzen der verwendeten Datenverarbeitungs- und -analysemethoden dargelegt und angegeben werden und erläutert werden inwieweit der IT-Sachverständige die Einzelheiten des Tools selbst verstehen und nachprüfen kann. In Bezug auf die Angabe von „Wahrscheinlichkeiten" bzw. „Unsicherheiten" wird auf die Ausführungen von Casey[258] in B. II. 3. d) verwiesen. Soweit möglich muss er insb. Verknüpfungen mit anderen Datenbanken, Libraries oder vernetzten Systemen ebenso angeben wie die Prämissen und Modelle, die in der Software verarbeitet sind. Soweit ihm das nicht möglich ist, muss er das offenlegen. Verwendet der Sachverständige digitale Spuren als Grundlage, muss er dem Gericht die Technik, die mit ihrer Entstehung und ihrer Bedeutung für das Verfahren zusammenhängt, bestmöglich auf Laienebene erläutern.[259] Und genau darin besteht wohl die größte Herausforderung bei der Gutachtenerstellung; die Ausrichtung für das Zielpublikum: In erster Linie sind das Nichttechniker bzw. Juristen, und erst in zweiter Linie Spezialisten, die die Ergebnisse ggf. überprüfen wollen.[260] So hat es sich in der Pra-

---

255 *Casey*, Forensic Science 2019 (Vol. 6), 649 f.; *Horsman*, Science Justice 2018, S. 433 f.; *Hughes/Karabiyik*, WIREs Forensic Science 2020 (Vol. 2), 1364 ff.; *Jones/Vidalis*, Annals of Emerging Technologies in Computing (AETiC) 2019 (Vol. 3), S. 41 ff.

256 Rat der Europäischen Union 2016; PCAST 2020.

257 Vgl. dazu auch *Stoykova*, Computer Law & Security Review 2021 Vol. 42, S. 105575.

258 *Casey*, Digital Evidence and Computer Crime (2011), S. 69 f.

259 *Mysegades*, Software als Beweiswerkzeug, S. 136 ff. m. w. N.

260 Vertiefend dazu Aufbau forensischer Berichte bei *Dewald/Freiling*, Forensische Informatik, S. 323 f. und *Frank*, Quality measurements of digital forensics analysis reports.

xis bewährt, immer zunächst eine kurze Zusammenfassung für die Laien zu formulieren und dabei die relevanten Befundermittlungen und Schlussfolgerung in Bezug zur jeweiligen Beweisfrage darzustellen. In der Praxis haben sich in Anbetracht einer besseren Les- und Verstehbarkeit für Laien auch verschiedene Darstellungsmöglichkeiten bewährt, z. B. Visualisierungen von Zeitstrahlen, das „information mapping“[261]; im Anschluss an Wigmore[262] wird in den USA teilweise eine Darstellung der syllogistischen Struktur mit Hilfe von Symbolen versucht[263]; oder Toepel[264] schlug eine grafische Aufzeichnung der Grobstruktur einzelner Argumentationen von den Anknüpfungs- und Befundtatsachen bis hin zur Stellungnahme zum Beweisthema vor, indem unmittelbar die Kernsätze genannt werden. Die syllogistische Struktur und die Verlässlichkeit der einzelnen Argumente könnte man auch mithilfe von „argumentation schemes“ und den damit zusammenhängenden „critical questions“ verdeutlichen[265]; in diesem Zusammenhang könnte auch das Konzepts der „Hierarchie der Hypothesen“ aus der DNA-Analyse[266] als Idee dienen.

Wünschenswert wäre zwar kein „Mustergutachten“[267], aber eine Art Standardisierung, zumindest des Aufbaus. So kann eine strukturelle Vorlage in Bezug auf den allgemeinen Aufbau die Lesbarkeit sowie die Vollständigkeit und damit die Qualität forensischer Untersuchungsberichte deutlich steigern. Helfen würde in diesem Zusammenhang bspw. eine explizite Nennung relevanter Kriterien bei der vollständigen Analyse, sofern diese eben nicht als Checkliste blind abgearbeitet, sondern als eine Art Erstellungshilfe herangezogen werden. Unter den Verfahrensbeteiligten kann so eine Vergleichbarkeit der verschiedenen Gutachten mglw. in Bezug auf eine ähnlich lautende Be-

---

261 Information Mapping® ist eine Methode zum Schreiben technischer Dokumente. So auch im Vortrag von Salzberger (Fast Detect) im Rahmen d. GRK’s 2022, vertiefendere Hinweise auf https://informationmapping.com/pages/information-mapping-methodology [29.6.2023].

262 *Wigmore*, Science of Proof, S. 862 ff.

263 Vgl. *Anderson/Schum/Twining*, Analysis of Evidence, S. 134 ff.

264 Grundstrukturen des Sachverständigenbeweises, S. 394.

265 *Deuber et al.*, Argumentation Schemes for Blockchain Deanonymization (vorgestelltes Paper bei JURISIN 2022), https://doi.org/10.48550/arXiv.2305.16883 [26.6.2023].

266 Vgl. auch *Vennemann/Oppelt/Grethe et al.*, NStZ 2022, 72.

267 Ein fester, statischer Untersuchungsbericht sei grundsätzlich kritisch zu betrachten, da die darin vorgeschlagenen Sätze und Prozesse leicht als Checkliste und Standardfloskeln zweckentfremdet werden können („Verklausulierung verleitet“). Dadurch wäre der Sinn einer vollständigen, einzelfallspezifischen Untersuchung untergraben und eine tatsächliche Gewährleistung der geschriebenen Tätigkeiten kaum gegeben. Vgl. dazu auch *Frank*, Quality measurements of digital forensics analysis reports.

weisfrage in einem Deliktsbereich (wie §§ 184b ff. StGB) geschaffen werden.[268]

Bei der mündlichen Präsentation der IT-Sachverständigengutachten bedarf es aus Sicht der Verfasserin jedenfalls einer Visualisierung der Ergebnisse im Gerichtssaal und damit auch einer Aufrüstung der technischen Ausstattung der deutschen Justiz.[269]

5. Die Standards der forensischen Informatik

Grundlegend muss der forensische Prozess (von der Sicherung bis hin zur Präsentation, einschließlich der zugrundeliegenden Datenverarbeitungsmethoden, soweit diese als Beweismittel im Rahmen der Würdigung des IT-Sachverständigen Eingang in das Strafverfahren finden sollen)[270] den Standards der forensischen Informatik nach dem derzeitigen Stand von Wissenschaft und Technik genügen. Das ergibt sich v. a. daraus, dass dem oben beschriebenen Grundsatz der Nachvollziehbarkeit und Transparenz der Forensik nachgekommen werden muss.[271] Wie bereits beschrieben, hat auch der Auftraggeber darauf zu achten nach § 78 StPO, dass diese eingehalten werden. Rückert leitet diese Pflicht überzeugend auch aus §§ 244 Abs. 2 und 261 StPO ab.[272] Für die Verfahrensbeteiligten ergibt sich aus dem Gesetz die Pflicht zur Einhaltung der Standards der forensischen Informatik. Im Rahmen des § 261 StPO muss die tatrichterliche Überzeugung auf einer („starken") objektiven Tatsachengrundlage basieren. Diese ist dann gegeben, wenn sie mit hoher Wahrscheinlichkeit richtig ist. Damit bemisst sich die „Stärke" der Tatsachengrundlage u. a. danach, wie zuverlässig und aussagekräftig die Ergebnisse (Befundermittlung) des Sachverständigen sind. Die Zuverlässigkeit und Aussagekraft bemessen sich wiederum danach, ob die sachverständige Tätigkeit den jeweiligen Standards genügt. Somit bestimmen die Einhaltung dieser Standards der

---

268 Vgl. dazu auch ENFSI, Strengthening the Evaluation of Forensic Results across Europe (STEOFRAE), und https://svv.ihk.de/blueprint/servlet/resource/blob/4931736/64e4f47868c28261011bfb6d4d4b29d4/literatur-zum-gutachtenaufbau-data.pdf [26.6.2023].

269 Vgl. dazu die Studie „Experiences of evidence presentation in court: an insight into the practice of crime scene examiners in England, Wales and Australia": Wunsch der forensischen Praktiker, die Ergebnisse mit besserer und moderner Technologie in Gerichtssälen zu präsentieren, vgl. *Sheppard/Fieldhouse/Casella*, Egyptian Journal of Forensic Sciences, 2020, S. 1 ff.

270 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 383 bereits auf Stufe der Verdachtsgewinnung im Ermittlungsverfahren.

271 Diese wurden auch in anderen forensischen Disziplinen entwickelt: DNA, Merkmale bei Daktyloskopie, ICD-10 in psychiatrischen Gutachten, etc, vgl. dazu eine Übersicht in *Garrett*, Autopsy of a Crime Lab.

272 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 674 ff.

forensischen Informatik auch nach der hier vertretenen Auffassung den Beweiswert des IT-Sachverständigengutachtens (und der zugrundeliegenden digitalen Daten und Datenverarbeitungsergebnisse) als Beweismittel in der Hauptverhandlung.[273]

Wie eben erläutert haben sich in anderen forensischen Disziplinen Standards herausgearbeitet, die von den Sachverständigen eingehalten werden müssen,[274] die den fachlichen Standard festschreiben und die Sorgfaltspflichten des Sachverständigen in fachlicher Hinsicht konkretisieren.[275] Diese können als Vorbild für die forensischen Informatik dienen.

Auch Tatgerichte verlangen in ihrer Rechtsprechung eine gewisse Standardisierbarkeit der sachverständigen Methodik im Bereich der forensischen Informatik. Ohne eine solche könnten die Verfahrensbeteiligten keine sinnvolle kritische Prüfung der Methode vornehmen und wären daher nicht in der Lage eine eigene Entscheidung vorzunehmen.[276] Im Umgang mit digitalen Daten äußern sich Gerichte (inzwischen) ausdrücklich zu Standards beim forensischen Vorgehen. So wurde bspw. erst kürzlich in einem Fall[277] vom Gericht beanstandet, dass die mitgeteilten verfahrensrelevanten Daten von einem deutschen Gericht oder einem Sachverständigen nicht forensisch überprüfbar sind und eine an den anerkannten Grundsätzen der IT-Forensik gemessene Dokumentation fehlt. In diesem Zusammenhang hob das Gericht auch die Wichtigkeit der Einblicke in die technische Infrastruktur und eingesetzten Algorithmen der Ermittlungswerkzeuge hervor. „Die Vorlage inkriminierenden Materials macht nicht entbehrlich, dass die Ergebnisse auch im Nach-

---

273 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 674 ff.; siehe auch *Garfinkel*, Digital Investigation (2010) Vol. 7, S. 64, der beschreibt, weshalb es einer Standardisierung bedarf.

274 Vgl. auch die Ausführungen von *Mysegades*, Software als Beweiswerkzeug, S. 231 ff. zu standardisierten Verfahren im Strafprozess; aber auch in als standardisiert angesehenen forensischen Disziplinen (wie dem Baurecht und Familienrecht) wird immer wieder die Forderung laut – ein standardisiertes Qualitätssystem zu realisieren, das den berechtigten Forderungen nach Transparenz, Qualität der Gutachten gerecht wird; vgl. *Bleutge*, Sachverständigenrecht, S. 4; Erste Ansätze zu einer umfassenden Reform der Sachverständigenpraxis bieten ein „Qualitätszirkel NRW", dem die nordrheinwestfälischen OLGs, Vertreter der NRW-Betellungskörperschaften und das Instituts für Sachverständigenwesen (IfS) angehören.

275 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 320.

276 Vgl. die Ausführungen des BGH zu Polygraphen als ungeeignetes Beweismittel, BGH, Urt. v. 17.12.1998 – 1 StR 156/98 = BGHSt 44, 308, Rn. 54.

277 Hier wurde aufgrund einer Verdachtsmeldung einer privaten Institution „NCMEC" (aus dem nichteuropäischen Ausland) wegen des Besitzes oder des Verbreitens Kinderpornografischer Schriften in Sozialen Netzwerken Ermittlungsverfahren wegen §§ 184b StGB eingeleitet, AG Reutlingen, Beschl. v. 18.12.2022 – 5 Ds 52 Js 9104/22 jug.

hinein reproduzierbar sind. Denn für den Fall, dass vor Gericht ein unabhängiger Gutachter hinzugezogen wird, müssen dessen Ergebnisse mit den bereits dokumentierten übereinstimmen. Des Weiteren müssen die Ergebnisse von dem Gutachter auf dieselbe dokumentierte Art und Weise zu finden sein und auch so gefunden werden. Im Einzelfall bedarf es immer einer umfänglichen Abklärung eines zunächst angenommenen Anfangsverdachtes, ansonsten leidet der für die Verfahrenseinleitung und die Verfahrensfortführung notwendige Tatverdacht rechtlich an einem im Raum stehenden Beweisverwertungsverbot."

In der Rechtspolitik wird der Ruf nach Standards, v. a. beim Versuch der Handhabung von KI, immer lauter.[278]

Hinzu kommt, dass Standards dabei helfen könnten, eine Vergleichbarkeit von forensischem Vorgehen – v. a. innerhalb eines Deliktsbereiches (wie bspw. der §§ 184b ff. StGB) – zu schaffen. Verfahrensbeteiligte wären im Laufe der Zeit in der Lage mehr (kriminalistisches)[279] Erfahrungswissen aufzubauen, indem sie die Tätigkeit, das Vokabular und die zugrundeliegenden Stärken und Schwächen der Technologie und digitaler Beweismittel kennenlernen. Die Verteidigerinnen können die Fragen stellen, auf die es wirklich ankommt,[280] die Juristen bekommen mehr Selbstvertrauen im Umgang mit digitalen Daten und dem IT-Sachverständigenbeweis im Strafverfahren und die Beweiswürdigung kann optimiert werden. So kann ein gefühlter Kompetenzverlust vermieden werden.

Weiter würde ein standardisiertes Verfahren dem Tatgericht vereinfachte und beschleunigte Feststellungen (gerade bei Massenverfahren) ermöglichen: Auf Grundlage von weitgehend anerkannten und standardisierten Verfahren – inklusive der in ihnen verwendeten Software – darf das Tatgericht von deren Zuverlässigkeit ausgehen, ohne in jedem Fall eine Detailprüfung vorzunehmen (siehe hierzu vertiefter im 4. Teil, A. III. 4. b) cc) (2) (b)).[281]

---

278 Vgl. nur https://www.zeit.de/2023/27/ki-gesetz-eu-chatgpt-regulierung [26.6.2023] oder https://www.zeit.de/kultur/2023-05/kuenstliche-intelligenz-angst-zukunft-geoffrey-hinton-james-bridle [27.6.2023]; *Lorch/Scheler/Rieß*, Compliance Challenges in Forensic Image Analysis Under the Artificial Intelligence Act, https://doi.org/10.48550/arXiv.2203.00469 [26.6.2023].

279 Näher zu kriminalistischem Erfahrungswissen, vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 365, S. 370 ff.

280 Beispiel: Handelt es sich tatsächlich um A's Facebook-Account? Kann ausgeschlossen werden, dass jemand anderes diesen Account verwaltet hat und Inhalte eingestellt hat? Ist das hochgeladene Foto echt? Sind Manipulationen an A's Mobiltelefon erkennbar? Sind die Authentizität und die Integrität der Daten gesichert? Wurde Software verwendet, um die Daten zu analysieren?

281 *Mysegades*, Software als Beweiswerkzeug, S. 6, S. 231.

Schließlich kann die Einhaltung der Standards für die Anwender – die IT-Sachverständigen – selbst mehr Sicherheit in ihrem Vorgehen schaffen. So beschreibt Casey[282], dass durch die Einhaltung dieser Standards (insb. in Bezug auf die Sicherung der Integrität und Dokumentation) Fehler vermieden werden können, die letztlich Auswirkungen auf die Gerichtsverwertbarkeit der Beweise haben können. In der Praxis wurde z. B. davon berichtet, dass eine bestimmte Seriennummer eines Tools fehlerhaft war (v. a. in Bezug auf die Vollständigkeit der gesicherten und analysierten Daten) und mithilfe der eingehaltenen Dokumentation genau nachvollzogen werden konnte, in welchen Verfahren das Tool zum Einsatz gekommen ist und welche Schritte entsprechend falsch ausgewertet wurden, um diese letztlich zu korrigieren.[283]

Dabei können sich Standards auf ganz verschiedene Ebenen beziehen. So gibt es bspw. Ausbildungsstandards (Personal, Best Practice, etc.); Standards für Software-Tools (Auswahlkriterien, Test- und Validierungssystem, Tool Log, etc.); ethisch-rechtliche Standards (persönlicher Kernbereich, Schutz von Vertrauensbeziehungen (Arzt, Anwalt, Journalist) oder eben analytisch-methodische Standards zur Gewährleistung des Grundsatzes der Nachvollziehbarkeit und Transparenz in der Forensik („Standards der forensischen Informatik").[284] Auf Letztgenannte soll im Folgenden genauer eingegangen werden.

Die Mindeststandards der forensischen Informatik, die Einfluss auf die Stärke der tatrichterlichen Überzeugung im Rahmen des § 261 StPO nehmen, sind aus Sicht der Verfasserin die Folgenden: Sicherung der Authentizität und Integrität der analysierten digitalen Spuren, Verwendung von wissenschaftlich verifizierten Methoden (sowohl bei Erfahrungssätzen als auch bei der Befundermittlung mithilfe von Datenanalysemethoden) und eine korrekte Anwendung dieser Methoden, Sachkunde und Qualifikation des Sachbearbeiters im Rahmen der Tätigkeit (das kann auch im Sinne einer erforderlichen Sachkunde des Sachverständigen verstanden werden, s. o. im 2. Teil, B. II. 2. c) bb)), Wiederholbarkeit und Reproduzierbarkeit der Ergebnisse, Mitteilung an den Auftraggeber über die möglichen und nicht möglichen Schlussfolgerungen aus den Ergebnissen und über die möglichen Fehlerquellen sowie die Einhaltung der verfahrensrechtlichen Grenzen.[285] Die nachfolgenden Ausführungen

---

282 *Casey*, Digital Evidence and Computer Crime, S. 27.

283 Einschätzungen von Johannes Pollach, M. Sc., IT-Forensiker bei der ZCB.

284 Besonders interessant ist in diesem Zusammenhang die Betrachtung von *Stoykova*, die eine Standardisierung für die Ebenen der Methodik (wie Tools), der Anwendung und der rechtlichen Würdigung fordert, vgl. so ähnlich in *Stoykova/Franke*, Forensic Science International: Digital Investigation 2023 Vol. 45, 301554.

285 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 23 f., S. 665 ff., S. 673 ff. Zum Ganzen auch *Heinson*, IT-Forensik, S. 128 ff.; *Casey*, Digital Evidence and Computer Crime, S. 59 ff.; *Fröwis et al*., Forensic Science International: Digital

sollen jedoch verdeutlichen, dass v. a. aber die Dokumentation durch den IT-Sachverständigen der Schlüssel für die richterliche Beweiswürdigung und die Plausibilitätskontrolle durch die Verfahrensbeteiligten ist.

Dabei sind die eben aufgezählten Standards nicht abschließend und wohl auch nicht „gleich bedeutsam" für alle Unterkategorien der forensischen Informatik zu betrachten.[286] So haben sich methodische Leitfäden und in den verschiedenen Unterkategorien viele „best practices" auf internationaler Ebene entwickelt (vgl hierzu die Beispiele unter B. III. 4.). Nach dem jetzigen Stand bildet die Aufzählung aber jedenfalls den Mindeststandard für den Umgang mit dem IT-Sachverständigenbeweis und den digitalen Daten im Strafverfahren.

a) Die Integrität und Authentizität von digitalen Spuren

Zunächst verlangt ein forensisch sauberes Vorgehen nach den o. g. Anforderungen die Sicherung der Integrität und Authentizität digitaler Spuren, also der Ergebnisse der IT-Sachverständigentätigkeit.

Nur die Kombination von Integrität und Authentizität erlaubt es sicherzugehen, dass die Spur tatsächlich sinnvoll und hilfreich für die Wahrheitsfindung interpretiert werden kann. Deshalb haben auch die Verfahrensbeteiligten im Rahmen der Beweiswürdigung der vorgelegten digitalen Beweismittel darauf zu achten, dass diese beiden Merkmale im forensischen Prozess eingehalten wurden. Wenn die Integrität verloren geht (bzw. die Integrität unter ein bestimmtes Maß sinkt), dann kann man bestimmte Schlüsse nicht mehr aus den durch die Spur dargelegten Informationen ziehen. Ähnliches gilt für die Authentizität.[287]

Investigation, (2020) Volume 33, S. 200902; *Fährmann*, MMR2020, S. 228 (229); *Momsen*, in: FS Beulke, S. 871 (885 f.); *Jahn/Brodowski*, in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 67 (92 f.).

286 Eine Übersicht findet sich hier: *Casino et al.*, Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews, 2022 Vol. 10, S. 25468: Von Networks Traffic Analysis, über Multimedia, Cloud, Social Networks, Blockchain, IoT, und File Systems. Vgl. bspw. die Ausführungen für einen Spezialfall der digitalen Forensik hier: *Ottmann/Breitinger/Freiling*, Defining Atomicity (and Integrity) for Snapshots of Storage in Forensic Computing, DFRWS (2022).

287 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 34.

aa) Die Integrität digitaler Spuren

Integrität[288] bedeutet vereinfacht, dass die Spur seit ihrer Sicherung nicht verändert wurde. Die oben beschriebene Betonung der Spureninformation, wie sie digitalen Spuren eigen zu sein scheint, führt dazu, dass sich die Integrität auch hauptsächlich auf die Spureninformation beziehen und sicherstellen muss, dass die Information unverändert vorliegt.[289] So wird die Frage relevant, ob ein digitales Objekt (wie eine Datei auf einem Datenträger) seit bzw. mit der Sicherung verändert worden ist.[290] Veränderungen können dabei bereits durch den Sicherungsprozess geschehen (B. III. 1.) Die Veränderungen sollten jedoch so gering wie möglich gehalten werden. Erschwerend kommt hinzu, dass sich Daten während ihrer „Lebenszeit" fortwährend verändern. Teilweise sind diese Veränderungen auf bewusste, durch Menschen verursachte, Vorgänge zurückzuführen (bewusste Bearbeitung der Daten), zum Teil aber auch auf technikbedingte, dem Nutzer nicht bewusste Vorgänge (z. B. systembedingte Veränderungen an Daten bei einem Kopiervorgang, siehe Ausführungen oben bei B. II. 3. e)). Deshalb bedarf es unbedingt einer Dokumentation zu jedem Zeitpunkt, um diese Veränderung nachvollziehen zu können (später mehr dazu bei Dokumentation in B. III. 5. f)). Auch werden unter dd) weitere organisatorische und technische Maßnahmen zur Umsetzung der Intigrität digitaler Spuren beschrieben.

bb) Die Authentizität digitaler Spuren

Authentizität bedeutet, dass die vorgelegte Spur tatsächlich die Spur ist, die durch die mit ihr verbundenen Behauptungen beschrieben wird. Wenn von der Spur behauptet wird, dass es sich dabei um den blutigen Handschuh vom Tatort handelt, dann ist die Spur authentisch, wenn es sich tatsächlich um den blutigen Handschuh vom Tatort handelt. Bei physischen Objekten definiert sich Authentizität also hauptsächlich durch den Spurenträger.[291] Deshalb ist

---

288 Korrespondiert mit der semantischen Integrität aus der IT-Sicherheit, vgl. auch *Gollmann*, Computer Security.

289 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 32. Beispiel: Angenommen, die Spur behauptet, sie sei der blutige Handschuh vom Tatort, der unter der Leiche gefunden wurde. In Wirklichkeit ist sie aber der blutige Handschuh vom Tatort, der auf der Leiche gefunden wurde. Die Spur erfüllt (falls sie nicht verändert wurde) zwar Integrität aber nicht Authentizität.

290 Bei einer *engen* Verbindung zwischen Spureninformation und Spurenträger kann man den Spurenträger selbst untersuchen und diesen aus weiteren Perspektiven betrachten, etwa die Tinte eines Briefes, die Handschrift auf einem Zettel, oder das Alter des Papiers, vgl. oben in diesem Teil, B. II. 1.

291 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 32 f. Beispiel: Falls die Spur behauptet, der blutige Handschuh zu sein, der auf der Leiche gefunden wurde,

die Authentizität bei digitalen Spuren noch etwas schwieriger zu definieren als bei physischen Spuren. Bei digitalen Spuren verwendet man häufig den aus der IT-Sicherheit etablierten Begriff der Authentizität[292], wie er durch digitale Signaturen realisiert werden kann. Das kann anhand des folgenden Beispiels – Authentizität durch digital signierten Hashwert – verdeutlicht werden:[293] Um Nachrichten digital zu signieren, kann man ein asymmetrisches Verschlüsselungsverfahren verwenden. Bei einem asymmetrischen Verschlüsselungsverfahren besitzt jede Person einen öffentlichen Schlüssel und einen privaten Schlüssel. Der öffentliche Schlüssel ist allen anderen Personen bekannt. Von den privaten Schlüsseln kennt jede Person nur den eigenen. Mit diesem privaten Schlüssel kann man Nachrichten signieren.[294] Die Eigenschaften der Operation des Signierens sind analog zum Setzen der eigenen Unterschrift unter die Nachricht. Jede andere Person kann prüfen, ob die Unterschrift von der angegebenen Person stammt, und auch nur diese Person kann die Unterschrift geleistet haben. Man kann folglich eine digitale Spur als authentisch ansehen, wenn ein korrekter Hashwert vorliegt, der von der Person digital signiert wurde, die die Spurensicherung durchgeführt hat.[295]

cc) Die zugrundeliegenden Annahmen

Von den Verfahrensbeteiligten sollte jedoch berücksichtigt werden, dass die Prüfung von Authentizität und Integrität stark auf Annahmen basiert, etwa dass die mit der Spur betrauten Personen ordnungsgemäß und verlässlich gearbeitet haben,[296] oder dass der hinterlegte Hashwert (für die Integrität und Authentizität) verlässlich und korrekt berechnet wurde, bspw. zum Zeitpunkt der Sicherung der originalen Bitfolge, und dass der Hashwert selbst authentisch ist und nicht verändert worden ist.[297] Auch vertrauen wir in die mathematische Sicherheit des digitalen Signaturverfahrens.[298] Rein praktisch wird nicht in jedem Fall jeder Schritt der Echtheit und Unverfälschtheit von digitalen Dateien überprüfbar sein, sodass immer eine gewisse Grundskepsis bestehen sollte. Auch der Gesetzgeber hat dieses Problem schon erkannt und mit

---

und es sich tatsächlich um diesen Handschuh handelt, der jedoch nach der Sicherung einmal mit der Waschmaschine gewaschen worden ist, dann erfüllt die Spur Authentizität aber nicht Integrität (jedenfalls nicht in hohem Maße).

292 *Gollmann*, Computer Security.

293 Beispiel 4 aus *Dewald/Freiling*, Forensische Informatik, S. 59.

294 Aus Effizienzgründen wird jedoch regelmäßig nur der Hashwert der Nachricht signiert.

295 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 61.

296 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 34, 58.

297 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 58 f. m. w. N.

298 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 59 f.

§ 371a ZPO eine Vorschrift zur bindenden Beweiskraft elektronischer Dokumente eingeführt, wenn sie bestimmte kryptografische Bedingungen erfüllen.[299]

dd) Organisatorische und technische Maßnahmen

Nach dem Stand der Technik in der forensischen Informatik können die Authentizität und Integrität durch verschiedene organisatorische und technische Maßnahmen sichergestellt werden.

Zu den organisatorischen Maßnahmen gehören v. a. das Einhalten der sog. Verwahrungskette (chain of custody)[300], die Dokumentation aller Verarbeitungsschritte und die Beschränkung des Zugangs zu den gesicherten Daten. Durch die Verwahrungskette kann idealerweise der gesamte „Lebensweg" der Daten bis zur Quelle ihrer Erhebung zurückverfolgt und somit die Authentizität nachgewiesen werden (vgl. dazu gleich vertiefter). Die Dokumentation aller Verarbeitungsschritte ermöglicht die Nachvollziehbarkeit aller an den Daten vorgenommenen Veränderungen bzw. ihren Ausschluss.[301] Die Beschränkung des (physischen und elektronischen) Zugangs zu den Daten bzw. ihren Datenträgern flankiert beide vorgenannten Maßnahmen, weil sie nicht dokumentierte Veränderungen ausschließt.[302]

Die technischen Maßnahmen zur Sicherung der Authentizität und Integrität von Beweisdaten sind vielfältig. Besondere Bedeutung kommt dem Erhalt des Originalzustands der Originaldaten, Maßnahmen zur Vermeidung von Veränderungen durch Kopiervorgänge (wie die 1:1-Kopie des Originaldatensatzes, siehe oben)[303] und der Berechnung, der Speicherung und dem Abgleich von Hashwerten zum Ausschluss von Veränderungen an den Daten zu. Ob und ggf. welche Maßnahmen zur Vermeidung von Veränderungen am Originaldatensatz durch Kopiervorgänge (z. B. bei der erstmaligen Erhebung der Daten oder bei der Erstellung von Arbeitskopien) zur Verfügung stehen, hängt von der Art des Speichers, aus dem die Daten erhoben werden, und von der

---

299 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 58 m. w. N.

300 *Maras*, Computer Forensics, S. 238 ff.; *Momsen/Hercher*, Digitale Beweismittel im Strafprozess, S. 173, S. 184.

301 *Heinson*, IT-Forensik, S. 144 f.; *Dewald/Freiling*, Forensische Informatik, S. 217 ff.; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 678.

302 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 218; *Savic*, Die digitale Dimension des Strafprozessrechts, S. 197; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 666.

303 Vertiefter dazu *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 666 f.; *Heinson*, IT-Forensik, S. 31 ff., 147; *Casey*, Digital Evidence and Computer Crime, S. 26; *Eisenberg*, Beweisrecht der StPO, Rn. 1938e; *Savic*, Die digitale Dimension des Strafprozessrechts, S. 197.

jeweils verwendeten Erhebungs- bzw. Sicherungstechnik ab (siehe zu den verschiedenen Sicherungstechniken bei B. III. 1.).[304]

Zur Überprüfung der Integrität kann bei der reinen Betrachtung der Spureninformation auch eine Plausibilitätsprüfung des Inhalts durchgeführt und z. B. verglichen werden, ob die Informationen widersprüchlich sind zu den mit der Spur verbundenen Behauptungen.[305]

b) Die (korrekte) Verwendung von wissenschaftlich verifizierten Methoden

Die sachverständige Beantwortung der Beweisfragen im Sinne der drei Aussagekategorien und die dabei zur Anwendung kommenden Datenverarbeitungs- und -analysemethode müssen auf präzisen definierten und wissenschaftlich bestätigten Methoden basieren.[306] Diese müssen außerdem von dem verantwortlichen Sachbearbeiter korrekt angewendet werden.[307] Wissenschaftlichkeit erfordert dabei stets die diskursive Angreifbarkeit und Falsifizierbarkeit von Erkenntnissen und Methoden (siehe zur wissenschaftlichen Methode bei A. I.).[308] Was als wissenschaftlich bestätigt zu sehen ist, bestimmt die jeweilige Fachgemeinschaft (z. B. „begutachtete Publikationen", siehe oben bei A. I.) und die Rechtspraxis (siehe unten bei gesicherte wissenschaftliche Erfahrungssätze im 4. Teil, A. III. 4. b) cc) (2) (a)). Hier spielen ebenfalls die Ausführungen zum Vorrang der Methodik mit bekannter Funktionalität eine Rolle (siehe dort im 2. Teil, B. VII. 3.).

c) Erforderliche Sachkunde des Forensikers

Unter diesem Punkt wird verlangt, was auch die StPO als Grundvoraussetzung von einem IT-Sachverständigen verlangt: die entsprechende erforderliche Sachkunde – für den Sachverständigenbeweis sogar eine besondere Sachkunde – auf dem Gebiet der forensischen Informatik, die für die Beantwortung der Beweisfrage gebraucht wird. Ist dieser in der Anwendung der jeweiligen forensischen Methode ausgebildet und/oder verfügt durch ein entsprechendes

---

304 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 665 ff.

305 Falls die Spur z. B. 2015 gesichert wurde, wäre es merkwürdig, wenn sich die Spureninformationen auf Ereignisse aus 2016 beziehen. Beispiel aus *Dewald/Freiling*, Forensische Informatik, S. 58.

306 *Neumann et al.*, Chance 29 (2016), S. 37 ff.; *Heinson*, IT-Forensik, S. 130 f.; *Jahn/Brodowski*, in: Hoven/Kudlich (Hrsg.), Digitalisierung und Strafverfahren, S. 67 (92 f.).

307 *Heinson*, IT-Forensik, S. 131 f.

308 Vgl. dazu auch *Mysegades*, Software als Beweiswerkzeug, S. 126 ff., S. 136.

Studium über das notwendige Wissen zur korrekten Anwendung der Methode, ist die Wahrscheinlichkeit größer, dass die erzielten Ergebnisse korrekt sind und etwaige Fehlerquellen gefunden und beseitigt werden.[309] Im Übrigen kann auf die Ausführungen oben zur besonderen Sachkunde verwiesen werden (2. Teil, B. II. 2. c) bb)).

d) Die Wiederholbarkeit und Reproduzierbarkeit der Ergebnisse

Im Bereich der Beweiswürdigung nach § 261 StPO ist anschließend an Rückert[310] von entscheidender Bedeutung für den Beweiswert von IT-Sachverständigenaussagen (und den zugrundeliegenden Datenverarbeitungs- und -analyseergebnissen), dass diese Ergebnisse reproduzierbar und wiederholbar sind.[311] Wiederholbar bedeutet dabei, dass die Ergebnisse bei erneuter Durchführung derselben Datenbearbeitungsmethode durch denselben Sachbearbeiter auf denselben Computersystemen zu denselben Ergebnissen führen.[312] Reproduzierbarkeit bedeutet, dass dieselben Ergebnisse bei Anwendung derselben Methode durch einen anderen Sachbearbeiter auf einem anderen (geeigneten) Computersystem erzielt werden.[313] Da die Wiederholbarkeit und Reproduzierbarkeit[314] sehr starke Indizien für die Richtigkeit eines forensischen Analyseergebnisses sind, haben diese Faktoren Einfluss auf die Beweiskraft und die Würdigung.

e) Die Mitteilung über mögliche und nicht mögliche Schlussfolgerungen und Fehlerquellen

Eine der wichtigsten Qualitätskriterien (auch im Rahmen der forensischen Dokumentation) bezieht sich auf die Plausibilität der einzelnen Untersuchungsschritte.[315] Schließlich wird die Beweiskraft der Ergebnisse davon beeinflusst, ob der zur Entscheidung berufene Jurist nachvollziehen kann, welche Schlussfolgerungen aus der Befundermittlung gezogen werden können und welche nicht, sowie die möglichen Fehlerquellen und ob er die Auswir-

309 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 376.

310 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 377, 665 ff.

311 *Casey*, Digital Evidence and Computer Crime, S. 25; *Maras*, Computer Forensics, S. 48 f.; *Heinson*, IT-Forensik, S. 132.

312 *Maras*, Computer Forensics, S. 48 f.

313 *Maras*, Computer Forensics, S. 48 f.

314 Dass dieses Erfordernis besonders schwierig ist für die Wissenschaft der forensischen Informatik, wird hier verdeutlicht: *Garfinkel/Farrell/Roussec/Dinolt*, Digital Investigation (2009) Vol. 6, S. 2 (3).

315 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 320 f.

kungen auf die Richtigkeitsgewähr kennt.[316] Daraus ergibt sich, dass die Anknüpfungstatsachen, die jeweiligen Aussagekategorien, die zugrundeliegenden Methodiken sowie Erfahrungssätze, die zugrundeliegenden Annahmen, Anfangswahrscheinlichkeiten und Richtigkeitswahrscheinlichkeiten bzw. Unsicherheiten auszuweisen sind. Hilfreich in diesem Zusammenhang sind ebenfalls Begründungen der einzelnen Untersuchungsschritte.

Nur so kann eine unabhängige Plausibilitätskontrolle und Nachprüfbarkeit der angewendeten wissenschaftlichen Methoden durch den juristischen Betrachter erfolgen und bei der tatrichterlichen Entscheidung im Hinblick auf die Wahrheitsfindung richtig eingeordnet und subsumiert werden. Auch die wissenschaftliche Methode selbst verlangt, dass jeder Schluss hinterfragt wird und Vermutungen als solche gekennzeichnet werden.

In der Praxis wird eine derart umfangreiche Dokumentation der einzelnen Untersuchungsschritte kaum möglich, noch angebracht sein (Verhältnismäßigkeit, Prozessökonomie und Beschleunigungsgrundsatz).[317] Nicht zu vergessen, dass Untersuchungen in der Praxis auch immer an einen Kostenrahmen gebunden sind, der es verbietet, mehr als nur einen minimalen Dokumentationsaufwand zu investieren.[318] So wird es z. B. ausreichen, wenn das Beweisthema lautet, die Existenz einer Datei auf einem Datenträger zu überprüfen, den Fundort der Datei anzugeben (Dateiname und -pfad, ggf. Sektornummer, etc.). Für die Nachprüfbarkeit ist es dann nicht notwendig, im Detail nachvollziehen zu können, auf welche Weise die Datei gefunden wurde (vorausgesetzt es gibt keine Beanstandungen dahingehend von den Verfahrensbeteiligten).[319] Im Zweifelsfall muss das im Nichhinein jedoch möglich sein (bspw. durch Einsicht in die Arbeitsunterlagen des IT-Sachverständigen).

f) Die Dokumentation

Aus den obigen Ausführungen soll sich verdeutlichen, wie wichtig die Dokumentation des forensischen Prozesses ist. So ergibt sich unmittelbar aus dem Grundsatz der Nachvollziehbarkeit und Transparenz der Forensik, dass die Dokumentation des Vorgehens und der Ergebnisse der Untersuchung eine zentrale Rolle spielt. Auch das bestätigt wohl die Erforderlichkeit, von IT-Sachverständigen in einem Strafverfahren ein vorbereitendes schriftliches Gutachten zu verlangen und dieses allen Verfahrensbeteiligten zur Vorbereitung der Verhandlung zugänglich zu machen. Denn die Dokumentation ist

316 *Fröwis et al*., Forensic Science International: Digital Investigation (2020) Vol. 33, S. 200902.

317 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 321.

318 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 321.

319 Vgl. Beispiel 34 in *Dewald/Freiling*, Forensische Informatik, S. 321.

v. a. deshalb erforderlich, um die Einhaltung all der anderen Standards überprüfen zu können: So kann bspw. überprüft werden, ob die Errechnung und der Abgleich von Hash-Summen, die Verwendung von WriteBlockern bei Kopiervorgängen, die Einhaltung der Verwahrungskette oder die engmaschige Dokumentation aller Verarbeitungsschritte erfolgte.

Im Hinblick auf die Sicherung der Integrität und Authentizität (v. a. im Hinblick auf die leichte Veränderung digitaler Spuren) werden z. B. bei der Live-Analyse eines zu untersuchenden Systems viele Zeitstempel und Hauptspeicherinhalte verändert. In solchen Situationen muss man alle Schritte genauestens dokumentieren, um auch diese Änderungen stets nachvollziehbar machen zu können. Dazu gehört auch eine Begründung, warum diese Veränderung notwendigerweise vorgenommen werden musste.[320]

Auch um zu überprüfen ob wissenschaftlich verifizierte Methoden angewendet wurden, bedarf es der Dokumentation.

Ob der IT-Sachverständige die besondere Sachkunde aufweist, ergibt sich u. a. auch aus den schriftlichen Ausführungen (Nachweis von Abschlüssen, etc.). Auch die Qualität der konkreten Analyseergebnissen und der daraus gezogenen Schlussfolgerungen in Bezug auf die Beantwortung des Beweisthemas und die Anwendung von ausgeprägtem und fundiertem Erfahrungswissen ergibt sich aus der Dokumentation. Indizien sind z. B. Quellenangaben bei angewendeten Erfahrungssätzen, das Ausweisen von Hypothesen und dazugehörigen Gegenhypothesen sowie das Kenntlichmachen von Unsicherheiten.

Auch um eine Wiederholbarkeit und Reproduzierbarkeit zu ermöglichen, müssen die Anknüpfungstatsachen, die verwendeten Tools, die zugrundeliegenden Annahmen und Daten offengelegt und mitgeteilt werden.

Zuletzt ergibt sich aus der Anforderung der *Mitteilung* über mögliche und nicht mögliche Schlussfolgerungen und Fehlerquellen schon, dass diese dokumentiert, also zugänglich gemacht werden müssen.

Es werden sowohl handschriftliche (wie etwa ein Logbuch) als auch automatische (mithilfe entsprechender Werkzeuge wie forscript) Dokumentationen empfohlen.[321]

aa) Exkurs: Die Zeitstempel

V. a. die Dokumentation von Zeit spielt eine große Rolle. Das betrifft sowohl die Zeitpunkte der Ereignisse, die den Tathergang ausmachen, als auch die Zeitpunkte, an denen der Ermittler bestimmte Aktivitäten durchgeführt hat

320 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 314.
321 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 316.

(Auswertungszeit). Der Vorgang basiert i. d. R. auf Zeitstempeln, die Computer hinterlassen. Zeitstempel sind eine spezifische Eigenart digitaler Spuren. Ihre Interpretation kann aber aus verschiedenen Gründen schwierig sein und besondere Sachkunde im Bereich der forensischen Informatik voraussetzen. Ein wesentlicher Grund ist, dass der Zeitpunkt, der durch den Zeitstempel dokumentiert wird, nicht der Zeitpunkt sein muss, zu dem der Zeitstempel gesetzt worden ist. Bei der Rekonstruktion von Ereignissen muss man demnach mindestens zwei verschiedene Zeiten unterscheiden: Die Zeit des Untersuchungsobjekts (den Wert der internen Uhr des beschlagnahmten Rechners) und die „echte" Zeit (die Zeitpunkte, zu denen die Ereignisse tatsächlich stattfanden), wobei die Zeiten nicht übereinstimmen müssen.[322] Weitere Gründe für die Schwierigkeit der Interpretation von Zeitstempeln können bspw. die vielen verschiedenen Zeitformate sein, in denen Zeitstempel in Dateisystemen abgelegt werden; oder oft wird auch die Zeitzone nicht mit abgespeichert.[323] Das Vorhandensein von Zeitstempeln darf also nicht dazu verleiten, die Zeitpunkte von Ereignissen mit wissenschaftlicher Exaktheit auf einer absoluten Zeitskala einzuordnen. Wie auch in der klassischen Forensik kann der Zeitpunkt eines Ereignisses auch in der digitalen Forensik bestenfalls eingegrenzt werden.[324]

bb) Exkurs: Chain of custody

Authentizität und Integrität beruhen stark auf Annahmen, etwa dass die mit der Spur betrauten Personen ordnungsgemäß und verlässlich gearbeitet haben (siehe bei B. III. 5. a) cc)). Neben der Gefahr einer Modifikation bei der Spurensicherung müssen im folgenden Verlauf der Untersuchung alle weiteren Ursachen, welche die Spur verändern können, eingedämmt werden. Das kann bspw. dadurch erreicht werden, dass möglichst wenige und auch nur fachlich besonders qualifizierte Personen Zugang zu der Spur erhalten. Das wird in der sog. Verwahrungskette (chain of custody) dokumentiert. Die Verwahrungskette ist Teil der Dokumentation der Spurenherkunft, also Teil der mit der Spur verbundenen Behauptungen. Sie dokumentiert lückenlos, wann welche Personen Zugang zur Spur hatten sowie den Aufbewahrungsort. Eine gute Verwahrungskette dokumentiert somit den örtlichen und zeitlichen Verlauf und auch den Zustand der Spur.[325] Idealerweise kann hierdurch der gesamte

322 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 318.

323 Vgl. *Dewald/Freiling*, Forensische Informatik, S. 319.

324 So *Dewald/Freiling*, Forensische Informatik, S. 319; hier sollen Uhrensynchronisationsprotokolle wie NTP helfen.

325 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 34, 315 f.; *Heinson*, IT-Forensik, S. 145.

„Lebensweg" der Daten bis zur Quelle ihrer Erhebung zurückverfolgt und somit die Authentizität nachgewiesen werden.[326]

Bei digitalen Spuren bezieht sich die Dokumentation der Verwahrungskette nicht nur auf den physischen Spurenträger (Datenträger). Das kann mit dem klassischen Bild des Asservates, das in der Asservatenkammer aufbewahrt wird, verglichen werden. Digitale Spuren werden aber häufig dupliziert und anschließend auf großen Datenspeichern im Netzwerk vorgehalten. Deshalb müssen diesbezüglich Zugriffsprotokolle angefertigt werden.[327] Daneben muss es auch eine Verwahrungskette der Beweisdaten geben („digital chain of custody"). Idealerweise muss der gesamte „Lebensweg" der Daten bis zur Quelle ihrer Erhebung zu jeder Zeit zurückverfolgt werden können; so gab es erst kürzlich Versuche das mithilfe von Blockchain-Technologie umzusetzen.[328]

g) Einhaltung der verfahrensrechtlichen Grenzen

Schließlich ist es wichtig, dass beim forensischen Prozess die oben erläuterten verfahrensrechtlichen Grenzen der IT-Sachverständigentätigkeit eingehalten werden, wie sie im 2. Teil, B. VI. dargestellt wurden: 1) Tätigkeit im Rahmen des Untersuchungsauftrages, 2) keine eigenen Ermittlungen, und 3) Einhaltung der rechtstaatlichen Bindung.

h) Die Bedeutung für das Beweisrecht

In der internationalen Literatur findet sich etwa die Darstellung, derzeit entscheide „häufig der ‚gute Ruf einer Forensiksoftware' über ihren Beweiswert".[329] Wie oben bereits ausgeführt, hat jedoch vielmehr die Einhaltung der wissenschaftlichen und forensischen Standards Einfluss auf den Beweiswert und die tatrichterliche Überzeugung im Sinne des § 261 StPO.

Vertieft auseinandergesetzt haben sich damit bereits Heinson[330] und Savic[331], und darauf aufbauend Rückert[332]. Erstgenannte Autoren argumentieren, dass die Wahrscheinlichkeit, den Richter durch die Beweisdaten zu überzeu-

---

326 Vgl. auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 665 f.

327 Vgl. auch *Dewald/Freiling*, Forensische Informatik, S. 315.

328 Vgl. *Sakshi et al.*, Journal of Information Security and Applications 2023 Vol. 77, 103579 f.

329 *Garfinkel/Farrell/Roussec/Dinolt*, Digital Investigation (2009) Vol. 6, S. 2 (9); *Heinson*, IT-Forensik, S. 417.

330 IT-Forensik.

331 Die digitale Dimension des Strafprozessrechts.

332 Digitale Daten als Beweismittel im Strafverfahren.

gen, mit dem Beweiswert der Daten und des forensischen Verfahrens zur Sicherung und Auswertung der Daten steige.[333] Savic[334] zieht sodann überzeugend die Standards der forensischen Informatik zur Maximierung des Beweiswerts heran. Heinson[335] knüpft die Frage des Beweiswerts präzise an die Pflicht des Tatgerichts zur Beachtung von bestehenden Erfahrungssätzen und zur Befolgung der Denkgesetze und der Logik als Beschränkungen der freien richterlichen Beweiswürdigung i. S. d. § 261 StPO. Nach ihm käme es bei der Beweisführung mit digitalen Spuren darauf an, ob und inwieweit die Beweisführung mit den Daten „objektiv und logisch begründbar die gezogenen Schlussfolgerungen zulässt". Rückert[336] gibt jedoch zu bedenken, dass die Frage der Maximierung des Beweiswerts problematisch ist, denn der Wert eines Beweises wird nach der Regel des § 261 StPO im Wege freier Beweiswürdigung durch das Tatgericht festgelegt. Den Wert von Beweismitteln könne man gerade nicht abstrakt messen oder festlegen.[337] Die zu beantwortende Frage lautet vielmehr, ob die vom BGH bislang formulierten Einschränkungen (siehe Regeln der praktischen Rationalität im 4. Teil, A. III.) der freien Beweiswürdigung das Tatgericht zwingen, die Einhaltung der Standards der forensischen Informatik (v. a. die Gewährleistung der Authentizität und Integrität der Beweisdaten) bei der Würdigung der Beweisdaten zu berücksichtigen. Nach Rückert[338] ist für eine Beantwortung insbesondere an der Lückenlosigkeit der Beweiswürdigung und Argumentation, der Beachtung existenter und die Nichtbeachtung nicht existenter Erfahrungssätze und der Pflicht zur erschöpfenden Beweiswürdigung anzuknüpfen (siehe dazu im 4. Teil).

IV. Zusammenfassung „Die forensische Informatik (als Teil der klassischen Forensiken)"

Ziel dieses Kapitels ist es, zunächst eine Übersicht zu geben über grundlegende Begriffe, typische Aufgaben, verschiedene Gebiete und die einzelnen Schritte der Sicherung, Analyse, Interpretation (i. S. d. Assoziation) und abschließenden Präsentation der forensischen Informatik. Auch sollen die Besonderheiten digitaler Spuren und der Kategorisierung der zugrundeliegenden Datenverarbeitungs- und analysemethoden hervorgehoben werden. Letztlich sollen die Mindeststandards der forensischen Informatik beschrieben werden, die eine wichtige Rolle für das Beweisrecht spielen.

---

333 Bspw. *Savic*, Die digitale Dimension des Strafprozessrechts, S. 175.

334 Die digitale Dimension des Strafprozessrechts, S. 176 ff.

335 IT-Forensik, S. 101.

336 Digitale Daten als Beweismittel im Strafverfahren, S. 669.

337 Löwe/Rosenberg/*Sander* § 261 Rn. 44 m. w. N.

338 Digitale Daten als Beweismittel im Strafverfahren, S. 674 f.

Es soll ein interdisziplinäres Verständnis dafür geschaffen werden, welche digitalen Spuren besonders wertvoll für ein Strafverfahren sind, was bei der Formulierung der Beweisfragen im Untersuchungsauftrag berücksichtigt werden sollte, und welche Punkte in einem IT-Sachverständigengutachten enthalten sein sollten.

Die Ausführungen sollen auch verdeutlichen, dass für die einzelnen Schritte – schon bei der Sicherung angefangen – häufig eine besondere Sachkunde auf dem Gebiet der forensischen Informatik erforderlich wird; in dieser Hinsicht ist v. a auch die Trennung der Analyse in einen technischen und inhaltlichen Teil dienlich. Darüber hinaus soll noch einmal hervorgehoben werden, wie wichtig es ist, die einzelnen Aussagekategorien, die Anknüpfungstatsachen, die verwendeten Datenverarbeitungs- und -analysemethoden, die zugrundeliegenden Annahmen sowie Richtigkeitswahrscheinlichkeiten bzw. Unsicherheiten einzeln auszuweisen und zu dokumentieren. Es ist stets über Klarheit im Umgang mit Wahrscheinlichkeiten zu sorgen. Ziel soll es sein, dass sowohl die eingesetzten Datenverarbeitungs- und -analysemethoden als auch die untersuchenden IT-Sachverständigen fähig sind, exakte Angaben darüber machen zu können, welche Informationen (i. S. v. Fakten) aus der forensischen Untersuchung abzuleiten sind und welche daraus entspringenden Schlussfolgerungen gezogen werden können bzw. welche nicht.[339]

Ob die Praxis so weit ist, einheitliche Standards einzuhalten und umzusetzen, lässt sich schwer beurteilen, da die Praktiker der Strafverfolgungsbehörden dieser Diskussion keine transparenten Falldaten oder Einschätzungen zur Verfügung stellen.[340]

Jedenfalls wird (Stand jetzt) noch nicht von einer einheitlichen Standardisierung im forensischen Prozess gesprochen werden können (dazu auch so-

---

339 Vgl. auch BSI, Leitfaden „IT-Forensik“, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1 S. 63 [26.6.2023].

340 Mehrere Nachfragen bei der bayer. Polizei durch die Verfasserin ergaben leider keine Antworten. Auch bei einer schriftlichen Anfrage an die Staatsregierung aus 2017 wurde zwar Auskunft darüber gegeben, dass Standards eingehalten werden, aber nicht welche: „Die Bearbeitung von Aufträgen von Cybercrime-Verfahren erfolgt, wie auch die Bearbeitung der Aufträge aus anderen Deliktsbereichen, nach dem aktuellen Stand der Technik, dem *wissenschaftlichen Standard der IT-Forensik* und anhand der Fragestellungen der jeweiligen beauftragenden Ermittlungsdienststelle. Das Bayerische Landeskriminalamt hat für die RBA *einheitliche Standards* hinsichtlich der Verfahrensweise zur Auswertung und Sicherung von digitalen Spuren festgelegt“, abrufbar unter https://www.bayern.landtag.de/www/ElanTextAblage_WP17/Drucksachen/Schriftliche%20Anfragen/17_0016300.pdf [29.6.2023].

gleich im 4. Teil, A. III. 4. b) cc) (2) (b));[341] ob das jemals der Fall sein wird für die forensische Informatik, ist unter Anbetracht der ihr inhärenten Besonderheiten (der Abgekoppeltheit von der physischen Welt und der Universalität) eher skeptisch zu sehen. Wie schwierig eine Handhabung in Bezug auf die Nachvollziehbarkeit im Kampf gegen den gefühlten Kompetenz- und Kontrollverlust ist, zeigt auch die gesellschaftliche Diskussion um die Regulierung von KI[342] – das spitzt sich zu, wenn KI-Tools in Strafverfahren, in denen es regelmäßig zu erheblichen Grundrechtseinschränkungen kommt, eingesetzt werden sollen.[343]

C. Zusammenfassung „Die Beschaffung des Tatsachenstoffes: Die forensische Informatik“

Ziel des 3. Teils der Untersuchung ist es, die Verfahrensbeteiligten eines Strafverfahrens v. a. auf die Vorteile und Schwachstellen der forensischen Informatik aufmerksam zu machen. Mithilfe der Darstellungen der forensischen Wissenschaften im Allgemeinen soll der Anspruch und die Erwartungshaltung aus juristischer Sicht an die ermittelten Ergebnisse der forensischen Informatik geklärt werden. Die Juristen, die zur Würdigung digitaler Beweise berufen sind, sollen ein differenziertes Verständnis für die IT-forensische Wissenschaft bekommen, um sich von einer „Technik- und Wissenschaftshörigkeit“ distanzieren zu können – zurück zur verfahrensrechtlichen Entscheidungsautorität der juristischen Auftraggeber i. S. v. § 261 StPO. So sollen die Verfahrensbeteiligten v. a. dahingehend sensibilisiert werden, dass bei der forensischen Informatik (noch) nicht standardisierte forensische Methoden angewendet werden, daher auch nicht zum gesicherten Erfahrungswissen gezählt werden können, und deren Vorgehensweise und die dadurch produzierten Ergebnisse als richtig unterstellt werden können (vertiefter zu standardisierten Verfahren im 4. Teil, A. III. 4. b) cc) (2) (b)). Im Umgang mit dem IT-Sachverständigenbeweis ist darauf besonders Acht zu geben, denn für diese forensische Wissenschaft gilt der wissenschaftliche Wandel noch stärker als für andere forensische Disziplinen. Auch ergibt sich für digitale Beweismittel die weitere Be-

---

341 So auch die Ergebnisse von *Sunde*, Non-technical Sources of Errors; und Eindrücke der Verfasserin vom Stimmungsbild der Praktiker im Rahmen eines Erfahrungsaustausches von bei Staatsanwaltschaften angesiedelten IT-Sachverständigen.

342 Vgl. nur https://www.zeit.de/2023/27/ki-gesetz-eu-chatgpt-regulierung [26.6.2023] oder https://www.zeit.de/kultur/2023-05/kuenstliche-intelligenz-angst-zukunft-geoffrey-hinton-james-bridle [27.6.2023]; *Lorch/Scheler/Rieß*, Compliance Challenges in Forensic Image Analysis Under the Artificial Intelligence Act, https://doi.org/10.48550/arXiv.2203.00469 [26.6.2023].

343 *Lorch/Scheler/Rieß*, Compliance Challenges in Forensic Image Analysis Under the Artificial Intelligence Act, https://doi.org/10.48550/arXiv.2203.00469 [26.6.2023].

sonderheit, dass die zugrundeliegenden Annahmen und Heuristiken der Datenverarbeitungs- und -analysemethoden bzw. deren Richtigkeit im Bereich der Befundermittlung (dritte Aussagekategorie) zum Teil überhaupt nicht nachprüfbar sind (Stichwort „Blackbox-Tools", siehe dazu unten im 4. Teil, A. III. 4. b) cc) (2) (f)). Also ganz im Gegenteil zur unterstellten „Wahrheit" der dabei produzierten digitalen Beweismittel, muss zunächst des Öfteren davon ausgegangen werden, dass es sich vllt. sogar um Beweismittel von geringerem Wirklichkeits- bzw. Beweiswert handelt (vgl. dazu auch im 2. Teil, B. I. 1.). Denn hier können viele potentielle Fehlerquellen liegen – wie in anderen forensischen Disziplinen auch.[344]

Weiter soll mehr Transparenz und Verständnis in den IT-forensischen Prozess gebracht werden, indem einzelne Schritte und Begriffe (v. a. am Beispiel der Datenträgerforensik) erklärt werden. Dabei soll auch die Frage beleuchtet werden, was die Besonderheiten digitaler Spuren sind und welche forensischen, kunstgerechten Standards bei der Auswertung zu beachten sind. Im Bereich von DNA-Analysen hat es Jahrzehnte gedauert, diese Standards zu entwickeln. Es ist zu hoffen, dass die Wissenschaft und Praxis nicht zu lange benötigt, um die Standards der forensischen Informatik in die gerichtliche Praxis zu bringen (v. a. im Hinblick auf die Schnelllebigkeit der Technologie und dem Erfordernis, damit Schritt halten zu können).[345] Dabei müssen die Juristen diese Standards aufmerksam begleiten; die Standards zu formulieren, ist Aufgabe des jeweiligen Fachbereichs.[346]

So soll dieser Teil dazu beitragen, die Unsicherheit, die in Bezug auf den strafprozessualen Umgang mit IT-forensischen Gutachten herrscht, zu minimieren und das Selbstbewusstsein der Verfahrensbeteiligten und deren (oben angesprochenes) Grundlagenwissen im Bereich der forensischen Informatik zu stärken. Ohne sich auch mit den technischen Möglichkeiten, Funktionen und Grenzen der forensischen Informatik auseinanderzusetzen, bliebe sie für Strafverfahrensbeteiligte unverständlich.

344 *Garrett*, Autopsy of a Crime Lab.

345 *Rückert/Wüst*, KriPoZ 2021, S. 67.

346 So auch die These des Referenten Dr. Eren Basar auf dem „Erlanger Cybercrime Tag 2022".

4. Teil

Die Beweiswürdigung des IT-Sachverständigenbeweises

Nach der forensischen Sachverständigentätigkeit (Sicherung, Analyse, Spureninterpretation und Anfertigung des vorbereitenden schriftlichen Gutachtens) erstattet der IT-Sachverständige schließlich sein mündliches Gutachten im Rahmen der Hauptverhandlung. Seine Aussagen werden damit Teil des Inbegriffs der Verhandlung i. S. d. § 261 StPO. Damit kann die Integration dieses zusätzlichen Materials in den Prozess der rechtlichen Beurteilung und der damit im engen Zusammenhang stehenden Sachverhaltsdarstellung durch die dafür zuständigen Gerichtspersonen beginnen.[1] Dabei bestimmen die Richterinnen zunächst das Gewicht der vom IT-Sachverständigen ausgesagten Ergebnisse für die bevorstehende juristische Entscheidung („Bewertung"[2]). Früher galt diesbezüglich das gemeinrechtliche Bindungsprinzip des Gutachtens. Danach war der Richter an das Gutachten gebunden.[3] So war man der Ansicht, als „iudex facti" könne der Sachverständige nicht vom Richter überprüft werden.[4] Nach und nach setzte sich jedoch durch, dass dem Richter eine Überprüfung der Widerspruchsfreiheit und der zugrundeliegenden Tatsachen zustehen sollte,[5] bis hin zum heute geltenden Grundsatz der freien richterlichen Beweiswürdigung nach § 261 StPO.[6] Nach Schluss der mündlichen

---

1 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 138.

2 Vgl. zur Unterscheidung zwischen Bewertung und Verwertung der sachverständigen Ergebnisse i. R.d Beweiswürdigung *Hess*, Digitale Technologien und freie Beweiswürdigung, S 203 ff.

3 Vgl. *Stinshoff*, Operative Fallanalyse, S. 104; *Mittermaier*, AcP 2 (1819), S. 119 f.; *Poppen*, Die Geschichte des Sachverständigenbeweises, S. 116 ff.; so auch *Sass*, DS 2010, 132 (137); *Crefeld*, R&P 1994, 102 (108) bezeichnet den Sachverständigen als „eigentlichen Herren der Szene"; oder vgl. *Detter*, NStZ 1998, 57; *Eisenberg*, NStZ 2006, 268, 369, bei denen von „Richtern in Weiß" die Rede ist.

4 *Gönner*, Handbuch des deutschen gemeinen Prozesses, S. 445; *Birnbaum*, Neues Archiv des Criminalrechts, Band 14, S. 182 (243 ff.); *Grolmann*, Theorie des gerichtlichen Verfahrens, § 513.

5 Vgl. *Mittermaier*, AcP 2 (1819), 119, 139 f.; *Mittermaier*, GA 1853, 107 ff., 113.

6 *Mittermaier*, Strafverfahren, S. 475 ff. unter Beachtung des englischen und französischen Rechts; vgl. auch *Stinshoff*, Operative Fallanalyse, S. 105; *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 65 ff. zur rechtshistorischen Entwicklung der freien richterlichen Beweiswürdigung.

Verhandlung wird über den Wert der Sachverständigenaussage, ihre Bedeutung und entsprechende Verwertung für den Tatvorwurf und die darauf aufbauende tatrichterliche Überzeugung beraten und abgestimmt („geheime Beratung", vgl. §§ 43, 45 DRiG, §§ 193 – 197 GVG) und schließlich in den Urteilsgründen niedergeschrieben (vgl. § 267 Abs. 1 S. 1, 2 StPO, siehe vertiefter dazu bei A. III. 5.). Der Einschätzungsvorgang wird als Würdigung des Beweises bezeichnet, § 261 StPO.[7] Dieser findet unter dem Aspekt statt, zu prüfen, ob der Beweis als gelungen anzusehen ist. Die Vorgabe, die umschreibt, wie sicher ein Beweisthema nach der Erhebung des Beweises feststehen muss, um den Beweis als erfolgreich durchgeführt betrachten zu können, wird als „Beweismaß" bezeichnet.[8] Eine allgemein anerkannte Theorie des Beweises im Strafverfahren, d. h. eine solche, die diejenigen Bedingungen anzugeben vermag, unter denen der Beweis als gelungen anzusehen ist, besteht nicht.[9] Die geltenden Grundsätze der Beweiswürdigung besagen, dass das Gericht auf Grund eigener[10], persönlicher Überzeugung zwar unabhängig von Beweisregeln zu entscheiden hat, dass es dabei jedoch an inhaltliche Voraussetzungen gebunden ist (vgl. hierzu insbesondere die Regeln der praktischen Rationalität unter A. III.).[11]

Es geht also um ein Zusammenspiel von objektiven und subjektiven Elementen.

Eine Schwierigkeit der Würdigung des Sachverständigenbeweises besteht zunächst darin, dass der Richter eine Würdigung von Beweisen auf einem Gebiet vorzunehmen hat, auf dem er nicht die erforderliche Sachkunde hat. In diesem Zusammenhang wird die Sorge des „Unkontrollierten und Unkontrollierbaren"[12] bzw. die „Krise des Sachverständigenbeweises"[13] deutlich. Es wird befürchtet, dass sich aus der Wissensvermittlung und Begutachtung durch den Sachverständigen ein Spannungsverhältnis zu der freien richterlichen Beweiswürdigung ergeben kann. Im Zusammenhang mit anderen foren-

---

7 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 138.

8 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 138 m. w. N.

9 Vgl. *Eisenberg*, Beweisrecht der StPO, Rn. 88, 91 ff., 97 ff.

10 Wichtig an dieser Stelle ist, dass die Sammlung des Beweisstoffs von der Würdigung der Beweise streng unterschieden werden muss: Während alle Beteiligten einen Anspruch auf Teilhabe an der Stoffsammlung haben, ist die Würdigung der erhobenen Beweise allein Sache des Gerichts.

11 *Eisenberg*, Beweisrecht der StPO, Rn. 88.

12 So in *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 25 f.

13 *Gerchow*, Arch. Krim. 134, 155; bzw. „Krise der richterlichen Urteilsbildung" in *Kaiser*, Kriminologie, S. 76: Entweder durch Kompetenzüberschreitung des Sachverständigen oder Kompetenzübertragung auf den Sachverständigen durch die Justiz, indem sie die Aussagen einfach übernimmt bzw. Beurteilung dem Sachverständigen überlässt.

sischen Disziplinen (wie des psychiatrischen bzw. psychologischen Sachverständigen) hat man oft von der „Abdankung richterlicher Beweiswürdigung", „Unterwerfung des Gerichts unter die Auffassung des Sachverständigen" bis hin zur „schrittweisen Entmachtung"[14] gehört.[15] Für IT-Sachverständigengutachten kommt verschärfend hinzu, dass regelmäßig nicht nachvollziehbare Datenverarbeitungs- bzw. -analysemethoden verwendet werden, wodurch die Gefahr einer faktischen Bindung des Gerichts an das Auswertungsergebnis potentiell verstärkt wird. Hat das Tatgericht keine hinreichende Kompetenz oder faktische Möglichkeit zur kritischen Prüfung der nicht nachvollziehbaren Methodik des IT-Sachverständigen, kann das zu einer faktischen Abhängigkeit der gerichtlichen Entscheidung von der sachverständigen Methodik führen.[16] Aber kann man wirklich von einer so „dramatischen" Entmachtung sprechen, wie oben angedeutet?

Zunächst ein Blick in die Praxis am Beispiel des Kemptener Bitcoin-Falles[17]: In den Urteilsgründen liest man Sätze wie „Die Feststellungen zur Funktionsweise, den Eigenschaften der Schadsoftware sowie zur Menge und Art der ausgespähten Daten beruhen auf den kompetenten, verständlichen und in allen Punkten überzeugenden Ausführungen des Sachverständigen …"[18] Solche Ausführungen sind jedenfalls geeignet, diesen gefühlten Kompetenzverlust zu unterstreichen, denn mit einer eigenen richterlichen Plausibilitätskontrolle der sachverständigen Aussagen in Bezug auf die Beweisfrage hat das wenig zu tun – sondern macht eher den Anschein einer ungeprüften Übernahme der Sachverständigenaussage in die Urteilsgründe aufgrund einer bloßen Reputationsprüfung.

Zunächst ist in diesem Zusammenhang festzuhalten, dass die Rechtsprechung den Tatgerichten ausnahmsweise gestattet, sich den fachgutachterlichen Ausführungen ohne eigene inhaltliche Auseinandersetzung anzuschließen[19] und die eigene Prüfung auf die Frage zu beschränken, ob die Sachverständige über die ausreichende fachliche Befähigung verfügt und auf ihre Sachkunde

---

[14] *Krauß*, ZStW 85 (1973), 321 f., 334; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 29, S. 47; *Geerds*, ArchKrim 137 (1966), 61; ausführlich *Plewig*, Funktion und Rolle des Sachverständigen, S. 27 ff.; Löwe/Rosenberg/*Krause*, Vor § 72 Rn. 18 spricht bspw. von der „Problematik des Sachverständigenbeweises".

[15] Vgl. *Walter*, Sachverständigenbeweis, S. 157.

[16] *Mysegades*, Software als Beweiswerkzeug, S. 132 f.

[17] Zum Verfahrensgang: LG Kempten, 29.10.2014 – 6 KLs 223 Js 7897/13; BGH, 21.07.2015 – 1 StR 16/15; LG Kempten, 13.4.2016 – 13 Ss 360/16; BGH, 27.7.2017 – 1 StR 412/16.

[18] LG Kempten als Vorinstanz KLs 223 Js 7897113 jug, bestätigt in: BGH 1 StR 412/16 v. 27.07.2017 = NStZ 2018, 401.

[19] BGHSt 12, 311 (314).

vertraut werden darf (dazu unter A. III. 5. vertiefter).[20] Für die Bewertung der Beweiskraft der Gutachtenergebnisse hat das Tatgericht aber anerkanntermaßen unabhängig von der inhaltlichen Nachprüfbarkeit der Ergebnisse, die Absicherung der wissenschaftlichen Erkenntnisse bspw. in Fachkreisen festzustellen oder zumindest eine oberflächliche Fehlerkontrolle in Bezug auf auffällige Unstimmigkeiten (wie methodische Fehler und Widersprüchlichkeiten) vorzunehmen.[21] In allen anderen Fällen, in denen den Tatgerichten eine Nachvollziehbarkeit nicht vollständig unmöglich ist, muss es die Möglichkeit der eigenen Plausibiltätsprüfung aber auch nutzen.[22] So lautete auch die Aufforderung des BGH[23] in der nächsten Instanz des Kemptener Bitcoin-Falles, die Handlungsabläufe in technischer Hinsicht umfassender als bislang aufzuarbeiten. Dabei machte er deutlich, dass erst die hinreichend genaue Feststellung der technischen Gegebenheiten die strafrechtliche Bewertung ermögliche. Daran anschließend haben sich die Richter zwar zunächst vertiefter mit der Funktions- und Wirkweise der verfahrensgegenständlichen Schadsoftware auseinandergesetzt[24], allerdings im Hinblick auf die Anzahl der infizierten Rechner eine Art „Daumenregel“ im Rahmen der Würdigung der sachverständigen Erfahrungssätze angewendet. So hatte das Gericht zur Frage, ob § 202a StGB gegeben ist, die Aktivität der Firewall der angegriffenen Rechner zu prüfen.[25] Dazu ist folgendes in der Entscheidungsbegründung zu lesen: „Insbesondere erläuterte der Sachverständige aus seiner langjährigen Tätigkeit als Sicherheitsexperte für das Internet die Erkenntnis gewonnen zu haben, dass auch im relevanten Tatzeitraum die Wahrscheinlichkeit, dass Computernutzer ohne aktivierte Firewall das Internet benutzen, äußerst gering sei“.[26] Der Sachverständige verglich das mit dem Fahren eines PKWs ohne Windschutzscheibe und führte aus, dass dieser Erfahrungssatz umso mehr für Computernutzer gelte, die mit dem „Usenet“[27] vertraut sind. Um der geringen Wahrscheinlichkeit zu begegnen, dass dennoch infizierte Computersysteme zumindest keine Windows-Firewall aktiviert hatten, hat das Gericht von der Anzahl der infizierten Computer einen Abschlag von 25 % vorgenommen und so die

---

20 BGHSt 7, 238 (239 f.); BGH NJW 1989, 179 (178); vgl. auch *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 204 f.

21 BGHSt 38, 320 (322) am Beispiel der DANN-Analyse; MüKo-StPO/*Miebach*, § 261 Rn. 318.

22 Vgl. BeckOK-StPO/*Eschelbach*, § 261 Rn. 66; *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 205.

23 BGH, Beschl. v. 21.7.2015 – 1 StR 16/15.

24 Vgl. LG Kempten, 13.4.2016, Az: 13 Ss 360/16.

25 Die Zugangssicherung im Sinne von § 202a Abs. 1 StGB muss darauf angelegt sein, den Zugriff Dritter auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren; MüKo-StGB/*Graf*, § 202a, Rn. 35 f.

26 Vgl. LG Kempten, 13.4.2016, Az: 13 Ss 360/16.

27 Siehe https://usenet.de/ [23.1.2024] für weitere Erläuterungen.

Zahl der Computersysteme auf 75 % geschätzt, bei denen die Schadsoftware die Firewall umging und damit der Tatbestand des § 202a StGB erfüllt war. Konkreter auseinandergesetzt mit den zugrunde gelegten sachverständigen Erfahrungssätzen (wie der Glaubwürdigkeit bzw. einer Richtigkeitswahrscheinlichkeit) hat sich das Gericht aber nicht. Es wirkt so, als hätten sie mit diesem Sicherheitsabschlag von 25 % per Daumenregel versucht, das „äußerst gering" des Sachverständigen in eine Häufigkeitsverteilung zu übersetzen und zu quantifizieren; oder haben sie den Sachverständigenaussagen einfach doch nicht so ganz getraut? Denn der Vergleich mit „Fahren ohne Windschutzscheibe" würde doch eigentlich gegen einen Sicherheitsabschlag von 25 % sprechen. Das haben sie jedoch nicht weiter ausgeführt.[28] Man könnte hier also von „Schätzung statt Beweisaufnahme bzw. eigener Plausibilitätskontrolle" sprechen.[29] Aus Sicht des BGH lässt die Vorgehensweise des LG jedenfalls keinen Rechtsfehler erkennen und hält diesen indiziellen Schluss auf das Vorhandensein einer aktiven Firewall bei 75 % der betroffenen Rechner für gerechtfertigt.[30] Allerdings ist anzumerken, dass auch bei Schätzungen durch die Strafverfolgung die Grundlage, die Methode und die Wahrscheinlichkeitsüberlegungen ermittelt werden müssen (dazu auch gleich allgemein zum Beweiswert von Indizien unter III. 4. b)).[31] Auch die „knappe" Definition der

---

[28] Lediglich: „Die Ausführungen beider Sachverständigen zeugten von entsprechender Kompetenz, korrespondierend mit ihrem bekundeten tatsächlichen Tätigkeitsfeld bei dem BKA Wiesbaden und der Firma G-DATA Software GmbH.".

[29] So auch die Kritik aus der Literatur, *Brodowski*, StV 2019, S. 385 (386).

[30] Deswegen wäre das Landgericht befugt gewesen, auf das Vorhandensein einer aktiven Firewall indiziell zu schließen. „Die tatsächlichen Umstände, aus denen es auf das Vorhandensein einer aktiven Firewall bei 75 % der betroffenen Computersysteme geschlossen hat, hat es nachvollziehbar dargelegt. Insoweit hat es sich auf die sachverständigen Darlegungen gestützt, wonach die Wahrscheinlichkeit, dass Internetnutzer keine aktivierte Firewall benutzten, äußerst gering sei. Darauf aufbauend hat das Landgericht zudem berücksichtigt, dass es sich bei den betroffenen Nutzern um solche handelte, die immerhin mit dem Usenet vertraut gewesen seien und einen eigenen kostenpflichtigen Zugang hierzu unterhielten. Um der geringen Wahrscheinlichkeit zu begegnen, dass dennoch infizierte Computersysteme zumindest keine Windows-Firewall aktiviert hatten, hat es von der Anzahl der infizierten Computer einen Abschlag von 25 % vorgenommen und so die Zahl der Computersysteme auf 75 % geschätzt, bei denen die Schadsoftware die Firewall umging. Auch vor dem Hintergrund, dass die Schadsoftware für Betriebssysteme bestimmt war, bei denen die Firewall standardmäßig aktiviert war, lässt diese Vorgehensweise einen Rechtsfehler nicht erkennen. Hierdurch hat das Landgericht pflichtgemäß diejenigen Tatsachen ermittelt, von deren Richtigkeit es überzeugt ist und ist damit der Abbildung der tatsächlichen Verhältnisse möglichst nahegekommen (vgl. zur Schätzung im Steuerstrafverfahren BGH, Beschluss vom 6. April 2016 – 1 StR 523/15, wistra 2016, 363)". Vgl. zu den Schätzklauseln oben Fn. 229.

[31] Beispiel aus dem Steuerverfahrensrecht: So setzt die Schätzung im Steuerstrafverfahren voraus, dass feststeht, dass der Steuerpflichtige einen Besteuerungstatbe-

Tatrichter von Bitcoins als „hochspekulative virtuelle Währung“ (zumindest „beim ersten Versuch“)[32] zeugt von einer nicht angemessenen fundierten technischen Würdigung des Sachverhalts.[33]

Aus einem Aktenstudium von IT-Sachverständigengutachten in Strafverfahren aus dem Deliktsfeld der §§ 184b ff. StGB, in denen diese oft das einzige Beweismittel sind, kann berichtet werden, dass eine tatrichterliche Würdigung der Gutachten teilweise gänzlich ausgeblieben ist,[34] oder die Sachverhaltsschilderungen im Urteil die Ausführungen des IT-Sachverständigen (Befundermittlung der festgestellten „KIPOS“ und ihre Klassifizierung) wortgleich in das Urteil übernommen wurden.[35]

Im Folgenden soll versucht werden herauszuarbeiten, dass, wenn die Verfahrensbeteiligten ihre verfahrensrechtlichen Möglichkeiten in Bezug auf den Sachverständigenbeweis ernst nehmen – v. a. in Bezug auf §§ 78, 244 Abs. 2, 261 StPO und das Fragerecht – kein Kompetenzverlust eintritt und bei Einhaltung der forensischen und wissenschaftlichen Prinzipien eine gute Würdigung möglich ist.

Um die Wirkung und ihre rechtstheoretische Beständigkeit und somit auch allgemein Wert und Bedeutsamkeit von IT-Sachverständigengutachten im Rahmen des richterlichen Entscheidungsfindungsprozesses bestimmen zu können, sind zunächst einige Überlegungen zur Überzeugungsbildung des Richters, zu den dabei möglichen Fehlern und der Nachprüfbarkeit der Überzeugungsbildung notwendig.

A. Grundlage der tatrichterlichen Überzeugung

Nach § 261 StPO hat der Richter nach seiner freien, aus dem Inbegriff der Verhandlung geschöpften Überzeugung über das Ergebnis der Beweisauf-

---

stand erfüllt hat, jedoch das Ausmaß der Besteuerungsgrundlagen ungewiss ist. Der Tatrichter muss die Überzeugung gewonnen haben, dass überhaupt eine entsprechende Tat vorliegt. Sodann muss er im Zuge einer Schätzung den konkreten Schuldumfang bestimmen. Da für das Steuerstrafverfahren der Grundsatz in dubio pro reo gilt, muss der gefundene Schätzungswert unter Berücksichtigung von § 385 Abs. 1 AO i. V. mit § 261 StPO nicht nur der Wahrscheinlichkeit wie im Besteuerungsverfahren nahe kommen, sondern er muss nach seiner vollen Überzeugung mit an Sicherheit grenzender Wahrscheinlichkeit den tatsächlich zutreffenden Wert abbilden bzw. darf diesen nicht überschreiten.

32 LG Kempten, 29.10.2014, Az: 6 KLs 223 Js 7897/13 jug.

33 Jedenfalls in einem zweiten Versuch dann konkretisiert, vgl. LG Kempten, 13.4.2016, Az: 13 Ss 360/16.

34 Bspw. Urt. Az 855 Ls 410 Js 1163/17.

35 Vgl. Urt. Az. 08 Ls 420 Js 547/18.

nahme zu entscheiden.[36] Dabei ist das Gericht nicht an fallunabhängige Beweisregeln gebunden, vielmehr ist die Würdigung von Beweisen, gleich ob digital oder analog, frei (vgl. Art. 92 GG).[37] Darin ist aber nicht nur ein mutmaßlich hohes Fehlerpotenzial zu sehen, sondern eben v. a. ein noch höheres Rationalitätspotenzial. Denn „Freiheit" der Beweiswürdigung bedeutet nicht Beliebigkeit. So genügt die bloße innere Überzeugung der Tatrichter nicht, um eine Sachverhaltsfeststellung zu begründen.[38] Sie sind vielmehr gehalten, ihre subjektive „Überzeugung" auf der Grundlage möglichst breiten Wissens über die Welt und auf der Basis von Argumenten zu bilden, die sich kommunikativ vermitteln lassen.[39] Genau darin besteht aber auch die Schwierigkeit des Beweisproblems[40]: Einen objektiven Maßstab zu finden, anhand dessen das subjektive „Fürwahrhalten ohne Zweifel", als das sich die Überzeugung des Gerichts darstellt, überprüft werden kann.[41] Wie oben angedeutet, geht es also um das Zusammenspiel von objektiven (Verstandestätigkeit der obj. Tatsachenfeststellung und wissenschaftlichen Forschung) und subjektiven Elementen (rational nicht erfassbaren Eindrücken und dem emotionalen Element der Willensentschließung).[42]

I. Das Beweismaß der tatrichterlichen Überzeugung

Das Beweismaß ist derjenige Grad an Gewissheit, der für eine richterliche Entscheidung erforderlich ist.[43] Nach dem Gesetz gilt im Strafprozess gem.

---

[36] Vertiefter zur Beweiswürdigung *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 65 ff.

[37] BGHSt 12, 311, 314 ff.; 8, 113, 118; 7, 238; 2, 14, 16.

[38] Vgl. dazu auch *Böhme*, DRiZ 1960, 20: „Die freie Überzeugung des Richters darf keinesfalls nur das Ergebnis eines dunklen Gefühlsvorgangs … sein"); *Rieß*, GA 1978, 262, 271; *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 24.

[39] https://www.zeit.de/gesellschaft/zeitgeschehen/2015-09/strafprozessrecht-beweisueberzeugung/seite-3 [29.6.2023].

[40] Vgl. Alsberg/Nüse/Meyer, Der Beweisantrag im Strafprozess, Vorwort S. III, die das Beweisproblem als „das Zentralproblem des Strafprozesses schlechthin" bezeichnen.

[41] *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 24.

[42] *Henkel*, Strafverfahrensrecht, S. 351; siehe auch *Schmidhäuser*, in: FS-Henkel, S. 231 ff.; *H. J. Schneider*, JuS 1970, 271; *Wimmer*, DRZ 1950, 192; *Rogall*, ZStW 91 (1979), 43, demnach die Urteilsfindung letztlich doch ein rationaler Vorgang sei; *Ostermeyer*, Die bestrafte Gesellschaft, S. 89, meint dagegen, dass der Beweiswürdigung rationale Grundlagen fehlen, so wie sie heute gehandhabt würde.

[43] *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 524.

§ 261 StPO für Verurteilungen[44] nur ein einziges Beweismaß: die tatrichterliche Überzeugung.[45]

Die Überzeugung wird auch umschrieben als „das Durchdrungensein von der Gültigkeit eines Urteils“[46]. Ebenso kann man sie auch als „Fürwahrhalten [ohne Zweifel[47]]“[48] bezeichnen.[49]

Die Praxis verfährt bei den Anforderungen an die Überzeugung im Einzelfall, aber differenzierter.[50] So berücksichtigt der Strafrichter, ob er eine eher unbedeutende Sanktion verhängt, wie bspw. ein Bußgeld bei einer Verkehrsordnungswidrigkeit, oder ob er eine langjährige Freiheitsstrafe ausspricht, wie etwa bei Verbrechen.[51] Das entspricht nicht nur dem richterlichen Bauchgefühl, sondern ist auch von den Verfahrensvorschriften gedeckt: Für die Bußgeldrichter gelten die strengen Beweisantragsregeln der StPO nicht, er darf auch die Bedeutung der Sache berücksichtigen (§ 77 OWiG). Aber auch in der StPO darf die Bedeutung der Sache berücksichtigt werden (etwa die Ladung eines Auslandszeugen, § 244 Abs. 5 S. 2 StPO).[52] Eine gesetzliche Beweismaßreduzierung hat sich aber nach wie vor nicht durchgesetzt.[53] Maßstab ist die tatrichterliche Überzeugung, § 261 StPO, die auf einer objektiven Tatsachengrundlage beruht. Beruht die richterliche Überzeugung auf einer tatsachengestützten und rationalen Beweisführung, ergibt dies zugleich eine objektiv hohe Wahrscheinlichkeit für die Richtigkeit des Beweisergebnisses[54]; d. h., durch rationale Argumentation wird die objektive hohe Wahrscheinlichkeit (dazu sogleich) bestätigt.[55] Damit soll verdeutlicht werden, dass die oben angesprochene „Daumenregel“ im Kemptener Bitcoin-Fall bzw. die wörtliche Übernahme der Sachverständigenaussagen sowie das blinde Verlassen auf die „überzeugende Kompetenz“ der Sachverständigen, nicht zuletzt ein gänzli-

---

44 Für andere Entscheidungen als Verurteilungen reichen nach dem Gesetz auch niedrigere Beweismaße, bspw. für die Glaubhaftmachung (§ 45 Abs. 2 StPO), den Anfangsverdacht (§ 152 Abs. 2 StPO, § 160 Abs. 1 StPO), den qualifizierten Anfangsverdacht (bspw. §§ 100a ff. StPO), den hinreichenden Tatverdacht (§ 170 Abs. 1 StPO), oder den dringenden Tatverdacht (§ 112 Abs. 1 StPO).

45 *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 525.

46 *Bohne*, Zur Psychologie der richterlichen Überzeugungsbildung, S. 43.

47 Wenn man das Moment der Zweifelsüberwindung stärker betonen will.

48 Vgl. *Ehrenzweig*, JW 1929, 85; *Niese*, GA, 1954, 152; *Gutmann*, JuS 1962, 371.

49 *Walter*, Sachverständigenbeweis, S. 83.

50 *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 527.

51 *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 528.

52 *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 528.

53 Vgl. dazu vertiefend *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 533.

54 BVerfG NJW 2003, 2444 (2445) m. w. N.

55 Vgl. KK/*Tiemann*, § 261 (9. Auflage) Rn. 11.

ches Ausbleiben der Beweiswürdigung im Urteil, den Voraussetzungen des § 261 StPO gerade nicht genügt – auch wenn es sich dabei vllt. um „Massendelikte“ und nicht langjährige Freiheitsstrafen handeln mag.

II. Die persönliche Gewissheit

Nach § 261 StPO entscheidet der Strafrichter über das Ergebnis der Beweisaufnahme nach seiner freien Überzeugung. Die Überzeugung ist zunächst nur die persönliche, subjektive Gewissheit des Richters von der objektiven Wahrheit der entscheidungserheblichen Tatsachen.[56] Diese Gewissheit ist eine bestimmte, aus dem Inbegriff der Verhandlung erwachsene innere Stellungnahme des Richters zum Gegenstand der Untersuchung, die nicht nur vom logisch geschulten Verstand getragen, sondern auch vom Gefühl beeinflusst ist. Der Richter muss die beweiserheblichen Tatsachen, mithin alle Tatsachen, die den Schuld- und Rechtsfolgenausspruch tragen, „für wahr halten“; selbst ein sehr hohes Maß an Wahrscheinlichkeit bedarf zusätzlich der inneren Gewissheit des Richters von der Wahrheit des Geschehens. Es handelt sich danach um eine subjektive Wahrscheinlichkeit. Diese subjektive Wahrscheinlichkeit schätzt der Richter jedoch mit gedachten objektiven Wahrscheinlichkeiten ab. Dazu greift er auf Erfahrungssätze zurück, die in der Regel weder empirisch abgesichert noch statistisch belegt sind.[57]

In der älteren Rspr. hat der BGH für eine Verurteilung noch allein die persönliche Gewissheit für ausreichend gehalten. Die dort aufgestellten Kriterien für die persönliche Gewissheit haben auch nach wie vor Gültigkeit.[58] So ist nach st. Rspr. Voraussetzung für die Überzeugung des Tatgerichts von einem bestimmten Sachverhalt nicht eine absolute, von niemanden anzweifelbare und das Gegenteil denknotwendig ausschließende Gewissheit;[59] Schlussfolgerungen müssen nur möglich, nicht zwingend sein.[60] Es genügt ein nach der

---

[56] BGH NStZ 1983, 277; KK/*Ott*, § 261 Rn. 2; *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 534; *Eisenberg*, Beweisrecht der StPO, Rn. 89; Löwe/Rosenberg/*Gollwitzer*, § 261 Rn. 7; KK/*Tiemann*, § 261 (9. Auflage) Rn. 2.

[57] Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 535 ff.

[58] Auf die wichtigsten Grundsatzentscheidungen bezieht sich der BGH heute noch: BGH, Urt. v. 9.2.1957 – 2 StR 508/56 –, BGHSt 10, 208 – 217 und BGH, Urt. v. 17.2.1970 – III ZR 139/67 –, BGHZ 53, 245 – 264 (sog. Anastasia-Urteil). Vertiefend vgl. auch *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 538 f.

[59] Vgl. BGH NStZ-RR 2010, 144 (145) m. w. N.; BGH NJW 1993, 605 (607): Eine absolute bzw. mathematische, jede Möglichkeit eines abw. Geschehensablaufs ausschließende und von niemanden mehr anzweifelbare Gewissheit ist nicht erforderlich; die bloße gedankliche Möglichkeit, dass der Tathergang auch anders gewesen sein könnte, darf die Verurteilung nicht hindern.

[60] BGH NStZ 2012, 110 (111).

Lebenserfahrung ausreichendes Maß an Sicherheit, das vernünftige und nicht bloß auf denktheoretische Möglichkeiten begründete Zweifel schweigen lässt.[61] Die Aufgabe besteht also darin, die Zweifel, die eine Absicherung der Aussage verlangen, präzise umschreiben zu können.[62] Dieser formulierte Mindeststandard einer Verurteilung „jenseits eines vernünftigen Zweifels" hält dazu an, einerseits bei vernünftig begründbaren Zweifeln von einer Verurteilung abzusehen und unter Anwendung des Zweifelssatzes freizusprechen; andererseits zu verurteilen, wo Zweifel nicht vernünftig begründbar sind. Mit den vom BGH entwickelten Anforderungen an das erforderliche (aber auch ausreichende) Maß der Gewissheit hat er sich also ein „Kontrollinstrument" geschaffen.[63]

Wie im Kapitel der Wahrheitsfindung im Strafverfahren, v. a. am Beispiel der streng subjektiven Theorien zum Wahrheitsbegriff dargestellt, bleibt bei der Ermittlung der prozessualen Wahrheit wohl immer ein Restzweifel – ob es die Unmöglichkeit einer hundertprozentigen Wahrheit oder die eines hundertprozentigen Ausschlusses ist. So liegt es nach § 261 StPO in der Verantwortung des Richters zu entscheiden, wann seine Zweifel schweigen. In diesem Sinne wird die Überzeugungsbildung auch als ein „Persönlichkeitsakt" bezeichnet, der alle Schichten der richterlichen Persönlichkeit berührt.[64] Das setzt ein gewisses Maß an Selbstwahrnehmung und Selbsterfahrung des Richters voraus und die Fähigkeit, persönliche Eigenanteile zu reflektieren. Das darf aber nicht bedeuten, dass das Ergebnis der Überzeugungsbildung keiner Kontrolle unterzogen werden sollte. Das haben auch die Revisionsgerichte verdeutlicht.[65] Diese subjektive Komponente ist deshalb zwar eine notwendige, aber noch keine hinreichende Voraussetzung für eine Verurteilung. Eine Verurteilung erfordert vielmehr auch, dass die persönliche Gewissheit auf objektiven Elementen aufbaut.[66]

---

[61] St. Rspr., vgl. BGH StV 1994, 580; NStZ-RR 1999, 332 (333); 2007, 43 (44) m. w. N.; NStZ-RR 2010, 144 (145); NStZ 2012, 110 (111); Zweifel der Strafkammer sind theoretischer Natur, welche sich als bloße Vermutungen ohne gesicherte Tatsachengrundlagen erweisen. Das, was völlig abseits liegt, wie z. B. das gleichzeitige Versagen von Lenkung und Bremsen, darf und muss außer Betracht bleiben (vgl. auch BGH 11.10.1968 – 4 StR 385/68; BeckRS 1975, 30403039; OLG Hamm VRS 41, 30); in der Literatur wurde die Formel insbes. von *Herdegen* kritisiert; vgl. NStZ 1987, 196; StV 1992, 531 (532); NStZ 1999, 177; NJW 2003, 3515.

[62] *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 147, 151; vgl. auch eingehend zum Verhältnis „Überzeugung" und „in dubio pro reo" *Stuckenberg*, Untersuchungen, S. 522 ff.; *Zopfs*, Der Grundsatz „in dubio pro reo", S. 278 ff.

[63] Vgl. *Herdegen*, StV 1992, 527 (531); KK/*Tiemann*, § 261 (9. Auflage) Rn. 2.

[64] *Walter*, Sachverständigenbeweis, S. 84 ff.

[65] *Walter*, Sachverständigenbeweis, S. 87, 99 ff. m. w. N.

[66] Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 536.

III. Die Regeln der praktischen Rationalität

Wie bereits beschrieben, ist die richterliche Überzeugung „frei", d. h. sie ist nicht an gesetzliche Beweisregeln gebunden, wie sie bspw. das anglo-amerikanische oder noch das gemeine Recht kannte.[67] Will ein Richter nicht willkürlich entscheiden, so bleibt ihm der Rückgriff auf die Regeln der praktischen Rationalität.[68] Das Gesetz weist nicht explizit darauf hin, weil es voraussetzt, dass sich Gerichtspersonen bemühen, das gewonnene Material rational auszuwerten.[69]

1. Vollständige Beweiswürdigung

So wie § 244 Abs. 2 StPO das Gericht verpflichtet, alle entscheidungserheblichen und bekannten Beweismittel vollständig zu erheben, ordnet § 261 StPO an, über alle auf der Grundlage des materiellen Rechts entscheidungserheblichen Beweisfragen eine vollständige Beweiswürdigung vorzunehmen und diese dem Urteil zu Grunde zu legen.[70] In diesem Rahmen verpflichtet der BGH das Tatgericht u. a. dazu, dass es im Wege einer Gesamtschau eine „erschöpfende" und „lückenlose" Beweiswürdigung vornehmen muss.[71] Das setzt zunächst voraus, dass das Tatgericht alle in die Hauptverhandlung eingeführten Beweistatsachen wahrnimmt und sie im Rahmen der späteren Würdigung in dieser Vollständigkeit auch berücksichtigt[72]; zugleich aber auch, dass sich die Würdigung nur auf solche Tatsachen stützt, die ordnungsgemäß in die Hauptverhandlung eingeführt wurden (sog. Inbegriff der Hauptverhandlung).[73]

Hierbei spielen die Ausführungen zum IT-Sachverständigen als sachnächstes und bestmögliches Beweismittel (siehe dazu im 2. Teil, A. IV.), der Umfang Wahrheitserforschungspflicht nach § 244 Abs. 2 StPO (siehe dazu im 2. Teil, B. I. 2.), die Grenzen der eigenen Sachkunde des Auftraggebers (siehe dazu im 2. Teil, B. II. 2. a)) sowie dem Stattgeben von Beweisanträgen auf

---

67 Dazu *Kusch*, Indizienbeweis, S. 80 ff.; für einen rechtsvergleichenden Blick in das U.S.-amerikanische Beweisrecht bzgl. Software als Beweiswerkzeug vgl. *Mysegades*, Software als Beweiswerkzeug, S. 185 ff.

68 Vgl. zur mittelbaren Annäherung auch *Baur*, ZIS (2019), S. 119 (123).

69 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 139.

70 BVerfG NJW 2003, 2444 (2445); vgl. *Fezer*, StV 1995, 95 (97).

71 Vgl. BGHSt 44, 153 (158 f.); 49, 112 (122 f.)); BGH NJW 1980, 2423; BGH StV 1997, 8; *Eisenberg*, Beweisrecht der StPO, Rn. 100; Meyer-Goßner/*Schmitt* § 261 Rn. 11a; Löwe/Rosenberg/*Sander*, § 261 Rn. 72.

72 *Fezer*, StV 1992, 95 (97); *Herdegen*, in: FS Eisenberg, 2009, S. 528.

73 Vertiefend dazu KK/*Tiemann*, § 261 (9. Auflage) Rn. 7; Löwe/Rosenberg/*Sander*, § 261 Rn. 48 ff.; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 673.

Vernehmung einer IT-Sachverständigen (siehe dazu im 2. Teil, B. II. 2. a) und V. 2. a)) eine Rolle.

2. Allgemeine Regeln des schlussfolgernden Denkens

Die Würdigung der Beweistatsachen selbst verlangt als ein Akt des schlussfolgernden Denkens eine Rationalität der Gedankenführung und unterliegt insoweit Grundsätzen der Logik als auch Gesetzen des Denkens und der Erfahrung.[74] Dabei ist im Rahmen der Denkgesetze auf klare, folgerichtige und lückenlose Argumentation zu achten.[75] Zudem dürfen keine Fehler wie Begriffsverwechslungen, Rechenfehler, Widersprüche und Kreis- oder Zirkelschlüsse enthalten sein.[76] Lückenhaftigkeit würde sich z. B. dadurch auszeichnen, dass Blickwinkel oder Tatsachen völlig außer Acht gelassen wurden.[77] Ebenso wenig dürfen Schlussfolgerungen aus Gegebenheiten gezogen werden, die selbst nicht erwiesen sind.[78]

Für den hiesigen Kontext besonders bedeutsam ist, dass der Tatrichter auch anerkannte Erfahrungssätze berücksichtigen muss und widerlegte Erfahrungssätze nicht einbeziehen darf. Solche Erfahrungssätze lassen sich anhand empirischer Beobachtungen und Verallgemeinerungen von Einzelfällen aufstellen, insbes. aus kriminalistischen, forensischen und aussagepsychologischen Untersuchungen.[79] Wissenschaftliche Erkenntnisse basieren auf rational geschlossenen Gesetzmäßigkeiten und empirisch gewonnenen Erfahrungssätzen.[80] Bindung besteht diesbezüglich auch dann, wenn das Gericht selbst nicht in der Lage ist, diese zu überprüfen[81], sofern es sich um hinreichend sichere Ergebnisse handelt und nicht um bloße Wahrscheinlichkeitsaussagen.[82] In dieser Untersuchung werden die wissenschaftlichen Erkenntnisse nach ih-

---

[74] *Eisenberg*, Beweisrecht der StPO, Rn. 102; MüKo-StPO/*Miebach*, § 261 Rn. 95 ff.; *Heger/Pohlreich*, Strafprozessrecht, Rn. 408.

[75] Vgl. BGH NJW 2019, 945 (945); MüKo-StPO/*Miebach*, § 261 Rn. 96; Löwe/Rosenberg/*Sander*, § 261 Rn. 47.

[76] BGHSt 3 213 (215); Meyer-Goßner/*Schmitt* § 261 Rn. 2; Löwe/Rosenberg/*Sander*, § 261 Rn. 47.

[77] Löwe/Rosenberg/*Sander*, § 261 Rn. 48.

[78] BGH NStZ-RR 2004, 238 (240); MüKo-StPO/*Miebach*, § 261 Rn. 96.

[79] BGH NJW 1982, 2455 (2456); MüKoStPO/*Miebach*, § 261 Rn. 28.

[80] Löwe/Rosenberg/*Sander*, § 261 Rn. 67.

[81] BGHSt 10, 208 (211); BGHSt 21, 157 (159); Erb ZStW 121 (2009) 882, (883, 888 ff.); Löwe/Rosenberg/*Sander*, § 261 Rn. 69.

[82] BGH NJW 1973 1411 (1411); vgl. BGHSt 38 320 (324); Löwe/Rosenberg/*Sander*, § 261 Rn. 70.

rer jeweiligen Zuverlässigkeit differenziert (siehe die Zuverlässlichkeitsskala bei A. III. 4. b) cc) (2)).[83]

3. Auswirkungen der Einhaltung der forensischen Standards

Wie bereits angedeutet, ist nach Rückert[84] für eine Beantwortung der Frage – ob die eben beschriebenen Regeln der praktischen Rationalität im Rahmen des § 261 StPO das Tatgericht zwingen, die Einhaltung der Standards der forensischen Informatik (v. a. Authentizität und Integrität) bei der Würdigung der Beweisdaten zu berücksichtigen – insbesondere an der Lückenlosigkeit der Beweiswürdigung und Argumentation, der Beachtung existenter und die Nichtbeachtung nicht existenter Erfahrungssätze sowie an der Pflicht zur erschöpfenden Beweiswürdigung anzuknüpfen.

Dahingehend führt er folgendes aus: Eine Nichtberücksichtigung der Frage, ob die Authentizität und Integrität der Daten gewahrt wurde, würde die aus den Daten gezogenen Schlussfolgerungen und die darauf aufbauende Argumentation für die Schuld oder Unschuld des Angeklagten lückenhaft machen.[85] Wenn die Authentizität und Integrität der Daten nicht nachweisbar sind, muss ggf. davon ausgegangen werden, dass eine Veränderung der beweiserheblichen Daten stattgefunden hat. Dabei könnte die Ursprungsechtheit und die Nichtveränderung der Daten mit organisatorischen und technischen Mitteln mit hoher Wahrscheinlichkeit gewährleistet werden. Darüber hinaus sieht Rückert[86] in dem Ausbleiben der Frage, ob die Authentizität und Integrität der Daten gewahrt wurde, in der richterlichen Würdigung einen Verstoß gegen die Regel, dass nicht existente Erfahrungssätze vom Gericht nicht als Erfahrungssatz der Beweiswürdigung zugrunde gelegt werden dürfen. Das soll für die Fälle gelten, in denen das Gericht sich darauf zurückzieht, dass Daten, die von den Strafverfolgungsbehörden erhoben, ausgewertet und als Beweismittel vorgelegt werden, „in der Regel“ aus der angegebenen Quelle stammen und weder absichtlich noch unabsichtlich verändert wurden. Ein solcher Erfahrungssatz existiert nicht. Insbesondere wurde bereits gezeigt (siehe im 3. Teil, B. II. 3.), dass die Verhinderung unbeabsichtigter Veränderung alles andere als trivial ist.[87] Aufgrund der volatilen Natur von Daten besteht vielmehr stets die Möglichkeit, dass diese absichtlich oder unabsichtlich verändert wurden. So verstößt eine Nichtberücksichtigung der Gewährleistung

---

83 Löwe/Rosenberg/*Sander*, § 261 Rn. 58, 61.

84 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 665 f.

85 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 666.

86 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 666 f.

87 So auch *Heinson*, IT-Forensik, S. 43 für die Live-Sicherung; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 666 f.

der Authentizität und Integrität der als Beweismittel verwerteten Daten gegen die Pflicht zur erschöpfenden Beweiswürdigung.[88] Nach den bereits oben dargestellten und belegten Grundsätzen muss das Gericht dabei nicht nur dann weitere Beweismittel oder Erkenntnisse heranziehen, wenn erkennbare oder bekannte Umstände die Heranziehung des Beweismittels oder der Erkenntnisse nahelegen, sondern bereits dann, wenn auch nur die entfernte Möglichkeit besteht, dass sich die Perspektive des Gerichts auf die Frage der Schuld oder Unschuld durch das neue Beweismittel oder die neue Erkenntnis verändern könnte.[89] Die Authentizität und Integrität der Daten sind diejenigen Eigenschaften, welche die Zuverlässigkeit der aus den Daten gewonnenen Informationen maßgeblich bestimmen. Wegen der in Abwesenheit entsprechender technischer und organisatorischer Maßnahmen häufig auftretenden, unbeabsichtigten Veränderungen an Daten, liegt eine Überprüfung zumindest des Ausschlusses solcher Veränderung stets nahe. Hinsichtlich absichtlicher Veränderungen oder der fehlenden Ursprungsechtheit wäre das zwar nicht stets der Fall, es besteht jedoch regelmäßig die Möglichkeit, dass sich die Perspektive des Gerichts auf die Zuverlässigkeit der aus den Daten gewonnenen Informationen und auf die Schuld oder Unschuld des Angeklagten insgesamt verändert, wenn sich bei der Überprüfung der Authentizität und Integrität der Daten Hinweise auf solche Manipulationen finden lassen.[90]

Das zugrunde gelegt, ist das Tatgericht also nach § 261 StPO dazu verpflichtet, die Gewährleistung der Authentizität und Integrität der als Beweismittel verwendeten Daten im Rahmen des IT-Sachverständigengutachtens in seine Beweiswürdigung mit einzubeziehen. Rückert merkt dabei jedoch an, dass allerdings auch kein Erfahrungssatz dahingehend besteht, dass Daten stets (beabsichtigt oder unbeabsichtigt) in einer Art und Weise verändert werden, die den für das jeweilige Verfahren relevanten Informationsgehalt verwandeln, wenn Maßnahmen zur Sicherung der Ursprungsechtheit und Unveränderbarkeit nicht oder nach dem Stand der Technik der forensischen Informatik nicht hinreichend getroffen werden. So kann das Tatgericht auch solche Daten als Beweismittel verwerten und würdigen, bei denen das eben nicht der Fall ist. Dann muss das Tatgericht jedoch erkennen lassen, dass es die fehlende oder mangelhafte Authentizitäts- und Integritätssicherung erkennt und bei der Bewertung des Beweismittels hinreichend berücksichtigt hat.[91]

Ergänzt werden können die Ausführungen von Rückert im Hinblick auf eine gegebene Lückenhaftigkeit der Argumentation und damit einen Verstoß gegen Denkgesetze, wenn eine Mitteilung über mögliche und nicht mögliche Schluss-

88 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 670 f.
89 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 672 m. w. N.
90 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 669.
91 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 671 f.

folgerungen und Fehlerquellen ausbleibt. Denn so kann eine Plausibilität der einzelnen Untersuchungsschritte nicht durchgeführt und nicht nachvollzogen werden, welche Schlussfolgerungen aus der Befundermittlung gezogen werden können und welche nicht, welches Erfahrungswissen Anwendung findet und mögliche Fehlerquellen und die Auswirkungen auf die Richtigkeitsgewähr blieben unerkannt. Würde der Richter die Sachverständigenaussagen dennoch seiner Urteilsfindung zugrunde legen, kann eine Argumentation für die Schuld oder Unschuld im Bereich der Beweisfrage gar nicht lückenlos sein, denn er hat dabei selbst die Schlussfolgerungen und möglichen Fehlerquellen offenzulegen. Nachdem sich bei einem Verstoß gegen die Grenzen der Sachverständigentätigkeit (s. o. im 3. Teil, B. III. 5. g) mit Verweis auf den 2. Teil, B. VI.) ggf. ein Beweisverbot ergeben kann, hat das u. U. Auswirkungen auf die „erschöpfende" und „lückenlose" Beweiswürdigung, wonach eine Würdigung nur auf solche Tatsachen gestützt werden darf, die ordnungsgemäß in die Hauptverhandlung eingeführt wurden (sog. Inbegriff der Hauptverhandlung). So hat das Tatgericht auch diese Standards in die Beweiswürdigung des IT-Sachverständigenbeweises mit einzubeziehen.

Die Einhaltung der anderen Standards der forensischen Informatik, wie die korrekte Verwendung von wissenschaftlich verifizierten Methoden, die Wiederholbarkeit und Reproduzierbarkeit der Ergebnisse, die Sachkunde des Forensikers und die Dokumentation sind Indizien für die Vermeidung von Fehlern im Rahmen der Denkgesetze und der Verwendung wissenschaftlich gesicherter Erfahrungssätze[92]. Letzteres muss bei der Beurteilung des Verlässlichkeitsgrades der angewendeten Methodik bzw. des angewendeten Erfahrungssatzes zur Bestimmung ihrer Beweiskraft berücksichtigt werden (dazu sogleich).

4. Die objektiven Elemente zur Bestimmung der persönlichen Gewissheit

Das Prinzip der (völlig) freien Beweiswürdigung wurde vom BGH sukzessive dahingehend eingeschränkt,[93] dass die richterliche Überzeugung in Form von persönlicher Gewissheit nicht nur einer rationalen Argumentation standhält, sondern auch auf einer objektiv tragfähigen, verstandesmäßig einsehbaren Tatsachengrundlage beruht.[94] D. h. die gezogenen Schlussfolgerungen müssen ausreichend mit Tatsachen bzw. „objektiven Grundlagen" abgesichert

92 So auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 690.

93 Siehe zur Geschichte der Rspr. etwa *Walter*, Sachverständigenbeweis, S. 87 ff.

94 KK/*Tiemann*, § 261 (9. Auflage) Rn. 5, 62 f.; KMR/*Stuckenberg*, § 261 Rn. 27; *Eisenberg*, Beweisrecht der StPO, Rn. 2, 91 m. w. N.

sein[95], so dass sie nicht nur Annahmen darstellen oder sich als bloße Vermutung erweisen, die letztlich nicht mehr als einen Verdacht zu begründen vermögen.[96] So soll der festgestellte Sachverhalt mit objektiv hoher Wahrscheinlichkeit mit der Wirklichkeit übereinstimmen.[97]

Darauf aufbauend wird also die objektive Stärke der tatrichterlichen Überzeugung von den Schlussfolgerungen, welche aus der Tatsachengrundlage gezogen werden, und der/den Hypothese(n), die aus den Schlussfolgerungen hinsichtlich Tathergang und Tatbeteiligung gewonnen werden sowie der objektiven Wahrscheinlichkeit der Richtigkeit dieser Hypothese bestimmt (vgl. dazu auch die Abb. 1 „Die objektive Stärke der tatrichterlichen Überzeugung i. S. d. § 261 StPO“ im 2. Teil, B. I. 3.).[98] Um die objektive Stärke der tatrichterlichen Überzeugung überprüfen zu können, muss sie intersubjektiv diskutierbar und nachvollziehbar gemacht werden.[99]

Die objektive Wahrscheinlichkeit der Richtigkeit der Hypothese ergibt sich u. a. daraus, wie „gut“ die Qualität der Tatsachengrundlage ist und damit die Ergebnisse des IT-Sachverständigen. Auch wenn die theoretisch denkbaren Möglichkeiten der zur tatrichterlichen Überzeugungsbildung heranzuziehenden Tatsachen nahezu unbegrenzt sind und vom jeweiligen Einzelfall abhängen, lassen sich dennoch allgemeingültige Kriterien zur Bestimmung der Qualität der Tatsachenbasis formulieren. Die Qualität der Tatsachenbasis wird von der „Nähe“ der Tatsachen zum subsumtionsfähigen Sachverhalt sowie der „Zuverlässigkeit“ und „Aussagekraft“ (hier zusammengefasst unter „Beweiswert“) der Tatsachen bestimmt.[100]

a) Die Nähe der Tatsachen zum Sachverhalt

Je unmittelbarer sich danach ein subsumtionsfähiger Sachverhalt aus der Tatsache selbst ergibt, desto weniger (mit Unsicherheiten behaftete) Schlussfolgerungen müssen gezogen werden.[101] Wie bereits angesprochen, lassen sich die im Wege des § 244 Abs. 2 StPO gesammelten Tatsachen in Bezug auf ihre Nähe zum verfahrensgegenständlichen Sachverhalt unterteilen in

---

95 BGH StV 1986, 61.

96 St. Rspr., vgl. BGH StV 2000, 67; wistra 2004, 432; NStZ-RR 2005, 373 m. w. N.

97 BGH StV 1993, 510 (511); vgl. BGH StraFo 2017, 235; vgl. *Detter*, FS BGH, 2000, 679 (684) m. w. N.; BVerfG NJW 2003, 2444 (2445) m. w. N.; KK/*Tiemann*, § 261 (9. Auflage) Rn. 5 f., Rn. 9.

98 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 364 in Bezug auf den Tatverdacht.

99 *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 550 m. w. N.

100 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 366 f., S. 756.

101 Vgl. auch im 2. Teil, B. II. 3. b) cc).

Haupttatsachen, Indizien und Hilfstatsachen; so auch die Beweisthemen des IT-Sachverständigenbeweises (s. o. im 2. Teil, B. I. 2.). In der Gesellschaft herrscht nach wie vor ein Missverständnis, dass Probleme der Wahrheitsermittlung v. a. in den Unsicherheiten der „berühmten Indizienprozesse" liegen würden. Man denke nur an die Unzulässigkeit des Indizienbeweises im gemeinrechtlichen Strafprozess.[102] Wichtig ist in diesem Zusammenhang, dass die Unterscheidung zwischen Haupttatsache und Indizientatsache zwar den Grad der Beweiserheblichkeit, nicht aber die Verlässlichkeit des Beweises betrifft – so kann bspw. ein Indizienbeweis (insb. wenn er mit sachlichen Beweismitteln geführt wird) durchaus verlässlicher sein als ein unmittelbarer Beweis.[103] Der Indizienbeweis ist im Grunde also kein anderer Beweis als der „direkte", sondern allenfalls komplexer, weil er mehr Schlüsse als dieser fordert.[104]

Nachdem es sich bei den von den IT-Sachverständigen zu beantwortenden Beweisfragen häufig um Indizien handelt, die vom Gericht entsprechend gewürdigt werden müssen, soll im Folgenden auch auf die Ermittlung des Beweiswerts von Indizien eingegangen werden.

b) Der Beweiswert des Indizes

Die Übereinstimmung der Definition des Indizes und dem mathematischen Begriff der bedingten Wahrscheinlichkeit, ist der Schlüssel für die forensisch wichtigen Fragen im Rahmen der Beweiswürdigung von Indizientatsachen:

1) Wann erhöht oder vermindert eine Tatsache die Wahrscheinlichkeit der Haupttatsache (Belastungs- oder Entlastungsindiz)?

2) Kann man abschätzen bzw. berechnen, wie stark das Indiz die Wahrscheinlichkeit der Haupttatsache beeinflusst, erhöht oder vermindert (Frage der Beweiskraft des Indizes)?[105]

Um sich den Fragen anschaulich nähern zu können, soll der folgende Beispielfall helfen:[106]

---

102 Vertiefend dazu *Stamp*, Die Wahrheit im Strafverfahren, S. 74 ff.

103 *Eisenberg*, Beweisrecht der StPO, Rn. 8 f.

104 *Stamp*, Die Wahrheit im Strafverfahren, S. 105.

105 *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 565.

106 Fiktiv und angelehnt an den Beispiel-Fall „Alcotest" von *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 566 und des Sachverhalts von AG Reutlingen, Beschl. v. 18.8.2022 – 5 Ds 52 Js 9104/22 jug.

aa) Ein Beispielsfall

Dem Beschuldigtem B wird vorgeworfen, über den Internetdienst Instagram (Accountname: BigRino) eine Nashorn-Datei[107] an drei weitere Nutzer des Internetdienstes Instagram gesendet und diesen durch „hochladen" zur Verfügung gestellt zu haben. Der Beschuldigte streitet die Tat ab. Bei einer (oberflächlichen) „Durchsicht" des iPhones des Beschuldigten wurde kein rinografisches Material aufgefunden. Dafür, dass der Beschuldigte noch weiteres rino- und/oder hippografisches Material besessen hat, gibt es keine hinreichenden Anhaltspunkte. Cloud-Daten oder Backupdaten wurden nicht erhoben. Allerdings konnten auf dem entsprechenden iPhone dreizehn Instagram Accounts, jedoch nicht der, von dem das strafbare Material versendet worden sein soll, in der zugehörigen „App" festgestellt werden.

Die einzigen Tatsachen, die für die Strafbarkeit des B sprechen, sind die mitgeteilten Daten (positive Meldung des Hochladens inkriminierter Dateien mit Zuordnung einer IP-Adresse) der privaten Institution „National Center for Missing an Exploited Rinos" (NCMER) mit Sitz in Bayern.

Das Tatgericht ist also auf das Indiz „positive Meldung der Software von NCMER" beschränkt, von dem auf die Haupttatsache „Besitz und Verbreiten von Rinografie" i. S. d. § 184r StGB geschlossen werden soll.

Eine IT-Sachverständige wurde nun damit beauftragt sich mit der Zuverlässigkeit der Meldung der NCMER auseinanderzusetzen.

Diese stellte daraufhin in verschiedenen Testverfahren[108] fest, dass diese Software nicht hundertprozentig zuverlässig ist. Die Fehlertoleranz, die durch eine mit 100 Probanden (Social-Media-Nutzern) durchgeführte Testserie ermittelt wurde, schlüsselt sich wie folgt auf:

Unter 100 Probanden (1. Gruppe, die „Delinquenten Social-Media-Nutzer"), die rinografisches Material[109] hochgeladen und versendet haben (hier stünde die Haupttatsache „Besitz und Verbreiten von Rinografie" fest), hat die

---

[107] Das nutzt Felix Freiling in seiner Vorlesung als Synonym für kinder- und jugendpornografische Dateien i. S. d. §§ 184b ff. StGB. Der Besitz und das Verbreiten von rino- und hippografischen Schriften ist nach §§ 184r, s StGB strafbar.

[108] Das Tatgericht müsste sich im Rahmen einer umfassenden und erschöpfenden Beweiswürdigung des IT-Sachverständigenbeweises unbedingt auch mit der Zuverlässlichkeit der angewendeten Testserien der IT-Sachverständigen auseinandersetzen und diese nach einer Bestimmung der Methodik als determinsitisch, statistisch oder selbstlernend in die Richtigkeitswahrscheinlichkeitsskala (siehe unter cc) (2)) einordnen, um den Einfluss und die Bindungswirkung der Ergebnisse auf die Überzeugungsbildung zu ermitteln.

[109] Computergeneriert.

Software von NCMER 95-mal zu Recht eine positive Meldung und 5-mal hat sie keine Meldung erstattet.

Diese Testserie hat man auch bei Probanden (2. Gruppe, die „Gesetzestreuen Social-Media-Nutzer") durchgeführt, die kein rinografisches Material hochgeladen und versendet haben. Das wäre die Nicht-Haupttatsache „Kein Besitz und Kein Verbreiten von Rinografie". Die Testserie bei 100 „Gesetzestreuen Social-Media-Nutzern" hat ergeben, dass bei 99 Probanden keine und bei einem Probanden zu Unrecht doch eine positive Meldung erstattet wurde.

Es wird deutlich, dass die Meldung der Software von NCMER (positiv wie ausbleibend) ein Indiz für die Haupttatsache „Besitz und Verbreiten von Rinografie" ist. Denn es hat Einfluss auf das Vorliegen der Haupttatsache.

bb) Die Fragentrias in Bezug auf das Belastungs- oder Entlastungsindiz

Um die erste Frage beantworten zu können, ob ein Indiz belastend oder entlastend ist, sind wiederum drei Fragen (sog. Fragentrias) zu stellen:[110] a) Wie häufig kommt das Indiz bei der Haupttatsache (1) vor? b) Wie häufig kommt das Indiz auch bei der Nicht-Haupttatsache (2) vor? c) Wo kommt das Indiz häufiger vor, bei Gruppe (1) oder Gruppe (2)?

Mithilfe des Beispielfalls soll nun versucht werden, die Fragen in Bezug auf die Be- oder Entlastung zu beantworten. Das Indiz „positive Meldung der Software von NCMER" kommt bei der 1. Gruppe (die mit 95 % Rinografie hochgeladen und verbreitet haben) häufiger vor als bei der 2. Gruppe (den „Gesetzestreuen Social-Media-Nutzern" mit 1 %). Es ist, weil es bei den „Delinquenten Social-Media-Nutzern" 95-mal häufiger vorkommt als bei den „Gesetzestreuen Social-Media-Nutzern", sogar stark belastend. Bei „Delinquenten Social-Media-Nutzern" ist fast immer eine positive Meldung erstattet worden, dafür geradezu typisch. Bei „Gesetzestreuen Social-Media-Nutzern" bleibt fast immer eine positive Meldung aus, dafür also untypisch.

Das Kriterium „typisch" ist allerdings tückisch, denn es verleitet zu Trugschlüssen. „Typisch" soll hier dahingehend verstanden werden, dass das Indiz überwiegend bei der Haupttatsache vorkommt.[111]

Der erste Trugschluss liegt darin, dass man übersieht, dass auch „untypische" Tatsachen ein Belastungsindiz sein können.[112] Beispiel: Dass „Delinquente Social-Media-Nutzer", die Rinographie hochladen und verbreiten

---

110 Das kann man auch mathematisch beweisen, vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 656.

111 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 570.

112 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 571.

(Haupttatsache), auch Software zum endgültigen und forensisch nicht mehr nachvollziehbaren Löschen auf den Rechnern gespeichert haben, wird vllt. eher selten vorkommen. Das Besitzen solcher Software wäre aber gleichwohl ein belastendes Indiz, wenn „Gesetzestreue Social-Media-Nutzer" noch seltener diese Software besitzen würden.

Entscheidend ist also, bei welcher Gruppe das Indiz häufiger vorkommt; das wird als Assymetrie bezeichnet.[113]

Einem zweiten Trugschluss kann man unterliegen, wenn man nur auf das scheinbar für die Haupttatsache „typische" Auftreten eines Indizes blickt und dabei vernachlässigt, dass das Indiz ähnlich häufig zusammen auch mit der Nicht-Haupttatsache vorkommt. Beispiel: Wenn Sachverständige den Nachweis krimineller Aktivitäten im Internet auf Verschlüsselungstechnologien wie den TOR-Browser oder sog. Krypto-Handys stützen; und diesbezüglich ausführen, dass dieses Verhalten ihrer Erfahrung nach deliktstypisch für kriminelle Internetnutzer sei, mithin Belastungsindizien seien. Dass dieses Verhalten bei kriminellen Internetnutzern zu beobachten ist, mag dabei durchaus zutreffen. Hat der Sachverständige seine Erfahrung aber ausschließlich aus der Beobachtung von kriminellen Internetnutzern gewonnen, wird er evtl. übersehen, dass auch vergleichbare Verhaltensweisen ähnlich häufig bei nicht kriminellen Internetnutzern vorkommen könnten – so z. B. wenn Nutzern Datenschutz sehr wichtig ist. Dann liegt jedenfalls keine signifikante Asymmetrie vor.

Der dritte Trugschluss ist am verwirrendsten.[114] Es wird sachverständig vorgetragen, dass höchstens 1 ‰ der Internetnutzer, die rhinografisches Material besitzen und verbreiten („Delinquente Social-Media-Nutzer"), auch selbst Nashörner misshandeln (§ 225r StGB „Misshandlung von Nashörnern"). Da es also selten – mithin nicht typisch für „Delinquente Social-Media-Nutzer" – sei, Nashörner zu misshandeln, sei das Indiz „Delinquenter Social-Media-Nutzer" nicht belastend (für die Haupttatsache „Misshandlung von Nashörnern"). Dabei ist das Indiz „Delinquenter Social-Media-Nutzer" aber gleichwohl belastend, auch wenn nur ein kleiner Teil der „Delinquenten Social-Media-Nutzer" selbst Nashörner misshandelt.[115] Der Trugschluss besteht in der falschen – umgekehrten Fragestellung. Hier wurde gefragt, wie wahrscheinlich es ist, dass die Haupttatsache („Misshandlung von Nashörnern") gegeben ist, wenn das Indiz („Delinquente Social-Media-Nutzer") festgestellt

113 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 572.

114 Vgl. den spektakulären Beispielfall von Alan M. Dershowitz im O. J. Simpson Prozess; vgl. auch *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 574 m. w. N.

115 Vgl. dazu auch *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 574 f. m. w. N.

ist. Die Sachverständigen-Antwort, dafür spreche nur die Wahrscheinlichkeit von 1 ‰, ist zwar richtig. Wenn man aber wissen will, ob „Delinquenter Social-Media-Nutzer" ein Belastungsindiz für die „Misshandlung von Nashörnern" ist, muss man die Frage umdrehen: Wie wahrscheinlich ist es, dass – umgekehrt – das Indiz („Delinquente Social-Media-Nutzer") auftritt, wenn die Haupttatsache („Misshandlung von Nashörnern") gegeben ist? Es kommt auf die Asymmetrie nach der Fragentrias an: 1) Wie viele „Nashorn-Misshandler" (Haupttatsache) haben zuvor Rinografie besessen und verbreitet als „Delinquente Social-Media-Nutzer" (Indiz)? 2) Wie viele Nutzer, die selbst keine Nashörner misshandeln (Nicht-Haupttatsache), sind „Delinquente Social-Media-Nutzer"? 3) Wer ist häufiger „Delinquenter Social-Media-Nutzer"? „Nashorn-Misshandler" oder Nicht-Misshandler von Nashörnern?[116]

Das Indiz „Delinquenter Social-Media-Nutzer" könnte nach dieser Fragentrias also auch belastend sein, je nachdem, ob man entsprechend zugrunde legen muss, dass „Nashorn-Misshandler" (Haupttatsache) häufiger Rhinografie besitzen und verbreiten als „Delinquente Social-Media-Nutzer", die selbst keine Nashörner misshandeln (Nicht-Haupttatsache).

cc) Die Beweiskraft des Indizes

Das Verhältnis, wie viel mal häufiger oder seltener das Indiz bei der Haupttatsache (Gruppe 1) als bei der Nicht-Haupttatsache (Gruppe 2) vorkommt, wird auch als abstrakte Beweiskraft des Indizes verstanden.[117] Mathematisch wird sie als Likelihood-Quotient bezeichnet.[118] Abstrakt deshalb, weil sie noch nichts darüber aussagt, wie wahrscheinlich das Indiz die Haupttatsache im konkreten Fall macht.[119]

Im obigen Beispielfall lässt sich aus der (fiktiven) unterstellten Häufigkeitsverteilung die Beweiskraft sogar quantifizieren. In der forensischen Informatik – wie auch in anderen forensischen Disziplinen, wird das eher selten der Fall sein, vgl. dazu schon die Ausführungen im 3. Teil, B. III. 3. a).

Die „positive Meldung" der Software von NCMER (95 % bei der 1. Gruppe „Delinquenten Social-Media-Nutzer" und nur 1 % bei der 2. Gruppe „Gesetzestreuen Social-Media-Nutzer") kommt bei „Delinquenten Social-Media-

116 I. S. der dritten Frage der Fragentrias: c) Wo kommt das Indiz häufiger vor, bei Gruppe (1) oder Gruppe (2)?

117 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 576.

118 Vgl. dazu auch *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 656.

119 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 577. Dazu, wie wichtig die Angabe von Häufigkeitsverteilungen bzw. Fehlertoleranzen ist und welche Herausforderungen damit einhergehen, vgl. *Dror*, Journal of Forensic Sciences (2020), S. 1 ff.

Nutzer“ 95-mal häufiger vor als bei „Gesetzestreuen Social-Media-Nutzern“.[120] Die positive Meldung hat also eine abstrakte Beweiskraft für den Besitz und die Verbreitung von Rhinografie von 95. Die positive Meldung spricht also für das Vorliegen der Haupttatsache.

Das Ausbleiben der positiven Meldung (99 % bei der 2. Gruppe „Gesetzestreue Social-Media-Nutzer“, aber nur 5 % bei der 1. Gruppe „Delinquente Social-Media-Nutzer“) kommt bei „Gesetzestreuen Social-Media-Nutzern“ 20-mal häufiger vor als bei „Delinquenten Social-Media-Nutzern“.[121] Wird nicht nach dem Besitz und der Verbreitung von Rhinografie gefragt, sondern – umgekehrt – nach dem Nicht-Besitz und der Nicht-Verbreitung von Rhinografie, dann hätte das Ausbleiben der positiven Fehlermeldung eine Beweiskraft von 20 für den Nicht-Besitz und der Nicht-Verbreitung von Rhinografie. Das Ausbleiben der positiven Meldung spricht also für den Nicht-Besitz und die Nicht-Verbreitung von Rhinografie und gegen den Besitz und die Verbreitung davon.

Angeknüpft an den Beispielfall soll das bedeuten, dass für die Würdigung des Indizes „positive Meldung der Software von NCMER“ v. a. die zugrundeliegende Datenverarbeitungsmethode und die ermittelte Fehlertoleranz bzw. Richtigkeitswahrscheinlichkeit von Bedeutung sind. In dem Beispielfall wurde eine genaue fiktive Fehlertoleranz für die Berechnung der Beweiskraft des Indizes angegeben. In der Praxis entstehen solche Meldungen jedoch häufig durch Software, der eine automatische Datenverarbeitung mit unbekannten zugrundeliegenden Annahmen und Heuristiken („Blackbox-Tools“) zugrunde liegt.[122] Hier ist man also weit entfernt von der Angabe von Fehlertoleranzen und der Quantifizierung der Beweiskraft.

(1) Die Zuverlässigkeit der zugrundeliegenden Richtigkeitswahrscheinlichkeit

Bereits im 3. Teil dieser Arbeit wurde darauf hingewiesen, dass die „Quantifizierung“ bzw. Einschätzung der Irrtumswahrscheinlichkeit ein wesentlicher Bestandteil der Assoziation bei der forensischen Rekonstruktion des Tathergangs ist. Denn die Irrtumswahrscheinlichkeit beziffert die „Überzeugungskraft“ der Ergebnisse der Sachverständigentätigkeit.

Für die Bestimmung der Zuverlässigkeit des IT-Sachverständigenbeweises kommt es zunächst auf die Qualität der konkret angewendeten Erfahrungs-

120 95 % geteilt durch 1 % = 95.

121 99 % geteilt durch 5 % = 20.

122 So auch im Beispiel der Rspr. AG Reutlingen, Beschl. v. 18.8.2022 – 5 Ds 52 Js 9104/22 jug.

sätze und verwendeten Datenverarbeitungs- und -analysemethoden an. In diesem Zusammenhang sind die Ausführungen von Rückert von Bedeutung, der die Methodiken der forensischen Informatik zunächst den Kategorien „deterministische, statistische und selbstlernende Methoden“ (siehe oben im 3. Teil, B. III. 2. b)) zuweist, um diese dann in eine Abstufung in Bezug auf deren Zuverlässigkeit einteilen zu können: Als gesicherte wissenschaftliche Erkenntnisse; als wissenschaftliche Erkenntnis mit wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit, oder als (einfache) Erfahrungssätze zur Richtigkeitsbeurteilung bzw. keine Regeln zur Beurteilung der Richtigkeitswahrscheinlichkeit.[123] Wichtig für die Einordnung in die Zuverlässigkeitsskala ist auch, dass Rückert die Methodiken als „nicht standardisiert“ einschätzt.[124] Denn ist eine forensische Methodik standardisiert, reduziert sie damit den notwendigen Detailgrad der Beweiswürdigung des Gerichts bei der Bewertung der Richtigkeitswahrscheinlichkeit und darauf aufbauend die entsprechenden Darstellungsanforderungen im Urteil. In der Regel genügt in solchen Fällen die Angabe der verwendeten Untersuchungsmethode, des Ergebnisses sowie der Richtigkeitswahrscheinlichkeit und ggf. eines Toleranz- bzw. Fehlerbereichs (vgl. auch Fälle im 2. Teil, B. II. 2. a), in denen trotz richterlicher fehlender Sachkunde kein Sachverständiger zu beauftragen ist).

Die Einordnung in diese Zuverlässigkeitsskala soll nicht nur für die Datenverarbeitungs- und analysemethodiken des IT-Sachverständigen gelten, sondern ebenso für die Bestimmung der Beweiskraft der Erfahrungssätze im Sinne der ersten Aussagekategorie des IT-Sachverständigen.

Das Tatgericht hat sich also stets detailliert mit der Untersuchungsmethode und insbesondere den Tatsachen, aus denen sich die Verlässlichkeit und Richtigkeitswahrscheinlichkeit der Methode bzw. des Erfahrungssatzes ergeben, zu befassen und diese entsprechend im Urteil nach § 267 Abs. 1 S. 1 StPO darzustellen.[125] Denn je nach Einordnung bestimmt sich daran anschließend der Einfluss der sachverständigen Ergebnisse und die Bindungswirkung auf die richterliche Überzeugungsbildung. Entscheidend ist hierbei einerseits die

[123] *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 675 ff.
[124] *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 684 f.

Abbildung 11: „Zuverlässigkeitsskala“

[125] Siehe auch vertieft zur Prüfung der Zuverlässigkeit von angewendeter Software bei *Mysegades*, Software als Beweiswerkzeug, S. 45 ff.

Aussagekraft und Bindungswirkung der Sachverständigenergebnisse, aber andererseits auch der Umstand, welche Beweisfunktion das präsentierte Ergebnis in der Sachverhaltsfeststellung einnimmt.[126]

Im Anschluss sollen nun die verschiedenen Stufen der Zuverlässigkeitsskala und ihre jeweiligen Folgen erläutert werden. Weiter soll hervorgehoben werden, dass oft an den zugrundeliegenden Erfahrungssätzen für die Richtigkeitsbeurteilung der Methodik angeknüpft werden muss, da in den seltensten Fällen Richtigkeitswahrscheinlichkeiten der Aussagekategorien bekannt sein werden. Wichtig ist diese Untersuchung v. a. deshalb, weil in deutschen Strafverfahren grds. alle Verlässlichkeitsstufen wissenschaftlicher Methoden und Erfahrungssätze Eingang finden können – anders als im US-amerikanischen Recht[127] – sie müssen „nur" entsprechend gewürdigt werden. Wie auch im US-amerikanischen Recht soll aber auch im deutschen Verfahrensrecht die Einhaltung von Standards der forensischen Informatik bei der Zuordnung der Verlässlichkeitsstufen helfen.[128]

(2) Die Zuverlässigkeitsskala

Mithilfe der Zuverlässigkeits-Abstufung der Methodiken des IT-Sachverständigen kann eine optimierte Beantwortung der Fragen nach Be- oder Entlastungsindiz und der Bestimmung der Beweiskraft erfolgen. Hier wird also die Nähe der Tatsache zum Sachverhalt und die Bedeutung der Beweisfunktion um ihre jeweilige Zuverlässigkeit ergänzt. Das Tatgericht muss in Bezug auf die Methodik (wie verwendete Datenverarbeitungs- und -analysemethoden) und Erfahrungssätze ermitteln, ob es an deren Ergebnisse bzw. an deren Gültigkeit gebunden ist oder ob es weitere Indizien sammeln muss, um den Beweiswert der zu würdigenden Tatsache richtig einschätzen zu können.

Es geht also darum, die angewendete Methodik und Erfahrungssätze des IT-Sachverständigen genau zu bestimmen und der jeweiligen Kategorie i. S. d. Zuverlässigkeitsskala zuzuordnen. Je nach Kategorie kann dann die Zuverläs-

---

126 Vgl. SK-StPO/*Velten*, § 261 Rn. 12; *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 206.

127 Beweisregeln geben verschiedenen präjudizierten „Standards" Regeln für die Berücksichtigung von Beweismitteln vor, die durch (forensik-)wissenschaftliche Methoden gewonnen wurden: Bspw. der sog. Frye-Standard oder der Daubert-Standard; vertiefend dazu siehe *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 674 f.; für einen rechtsvergleichenden Blick in das U.S.-amerikanische Beweisrecht bzgl. Software als Beweiswerkzeug vgl. *Mysegades*, Software als Beweiswerkzeug, S. 185 ff.

128 Siehe dazu auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 674 ff.

sigkeit der ermittelten Ergebnisse und damit die Beweiskraft der (Indizien-) Tatsache bestimmt werden.

(a) Gesicherte wissenschaftliche Erkenntnis

Gesicherten wissenschaftlichen Erkenntnissen muss sich das Tatgericht in seiner Beweiswürdigung anschließen bzw. darf ihnen nicht widersprechen.[129] An gesicherte wissenschaftliche Erkenntnisse sind Tatrichterinnen v. a. deshalb gebunden, weil diese zwingend überprüfbar und falsifizierbar sind und sich im wissenschaftlichen Diskurs ständig bewähren müssen (vgl. dazu auch im 3. Teil, A. I.). Insoweit übernimmt der wissenschaftliche Diskurs eine Kontrolle ihrer Richtigkeit, die das Tatgericht prozessökonomisch nicht leisten könnte. So müssen Richterinnen jedenfalls eine anerkannte und nicht falsifizierte wissenschaftliche Methodik als „objektive Beweiswürdigungsgrenze" berücksichtigen.[130] Als wissenschaftlich gesichert gilt eine Erkenntnis dabei nur, wenn die Erkenntnis nach dem aktuellen Stand der Wissenschaft unangefochten ist und ihr daher eine jeden Gegenbeweis ausschließende Beweiskraft zukommt.[131] Die Bindungswirkung für das Tatgericht besteht dabei auch unabhängig davon, ob das Gericht die Erkenntnisse selbst nachprüfen bzw. nachvollziehen kann,[132] was v. a. bei komplexen wissenschaftlichen Zusammenhängen von Bedeutung ist. Bei bestehenden wissenschaftlichen Meinungsstreitigkeiten über die „Gesichertheit" der Erkenntnisse muss das Tatgericht – i. d. R. gestützt auf Auskünfte von Sachverständigen – entscheiden, welcher Auffassung es sich anschließt, und das entsprechend begründen.[133] Soweit der BGH (vermeintlich) ein Abweichen des Tatgerichts von gesicherten wissenschaftlichen Erkenntnissen im Einzelfall zugelassen hat, verlangt er eine ausführliche Begründung des Abweichens, die sich auf überzeugende und sorgfältige Studien, die das Gegenteil der vermeintlich gesicherten Erkenntnis belegen, und/oder sich auf anerkannte Autoritäten im jeweiligen Fachgebiet stützt.[134] Existieren solche überzeugenden Gegenstudien und abweichende Meinungen aner-

[129] BGHSt 21, 157 (159); 29, 18 (21); 37, 89 (91 f.); SSW/*Schluckebier*, § 261 Rn. 20; MüKo-StPO/*Miebach*, § 261 Rn. 70; KMR/*Stuckenberg*, § 261 Rn. 34; Löwe/Rosenberg/*Sander*, § 261 Rn. 68 jeweils m. w. N.

[130] Vgl. dazu auch *Mysegades*, Software als Beweiswerkzeug, S. 63 m. w. N.

[131] BGHSt 21, 157 (159); 29, 18 (21); 37, 89 (91 f.); SSW/*Schluckebier*, § 261 Rn. 20; MüKo-StPO/*Miebach*, § 261 Rn. 70; KMR/*Stuckenberg*, § 261 Rn. 34; Löwe/Rosenberg/*Sander*, § 261 Rn. 68 jeweils m. w. N.

[132] BGHSt 21, 157 (159); Löwe/Rosenberg/*Sander*, § 261 Rn. 69.

[133] BGH bei *Dallinger*, MDR 1952, 274 (275); KMR/*Stuckenberg*, § 261 Rn. 34; Löwe/Rosenberg/*Sander*, § 261 Rn. 68 jeweils m. w. N.

[134] BGH bei *Dallinger*, MDR 1952, 274 (275); KMR/*Stuckenberg*, § 261 Rn. 34; Löwe/Rosenberg/*Sander*, § 261 Rn. 68 jeweils m. w. N.

kannter Experten im jeweiligen Fall, kann jedoch bereits nicht mehr von gesicherten wissenschaftlichen Erkenntnissen gesprochen werden, es liegt vielmehr ein Meinungsstreit vor, sodass diese Rspr. im Ergebnis keine Ausnahme von den Grundsätzen begründet. Bei alldem muss natürlich berücksichtigt werden, dass es absolut sichere Erkenntnisse nicht gibt (siehe oben im 3. Teil, A. I.). Wissenschaftliche Erkenntnisse können zwar falsifiziert, niemals jedoch endgültig verifiziert werden. Deshalb dürfen Tatgerichte bei der Bewertung, ob eine Erkenntnis wissenschaftlich als gesichert anzusehen ist, keine überhöhten, bereits aus wissenschafts- und erkenntnistheoretischen Gründen nicht erfüllbaren Anforderungen stellen. Dementsprechend genügt stets eine „an Sicherheit grenzende Wahrscheinlichkeit", dass die Erkenntnisse richtig sind.[135]

Hierunter zu fassen sind Rückert folgend Datenverarbeitungsprogramme und Datenanalysemethoden mit deterministischen Methoden.[136] Wurde durch eine solche Methode bspw. gezeigt, dass eine bestimmte Datei (z. B. ein kinderpornografisches Bild) auf einem Datenträger vorhanden ist, kann das Tatgericht in seiner Würdigung nicht einer gegenteiligen Einlassung des Angeklagten folgen (soweit es um das tatsächliche Vorhandensein der Datei geht, wobei die Vorsatzfrage und der strafrelevante Inhalt davon natürlich unabhängig zu bewerten sind) und muss vom tatsächlichen Vorhandensein der Datei auf dem Datenträger im Moment der Untersuchung ausgehen. Diese Bindungswirkung gilt z. B. auch in Bezug auf die Vornahme einer Kryptowährungstransaktion von einer bestimmten Adresse an eine andere bestimmte Adresse in einer bestimmten Höhe zu einem bestimmten Zeitpunkt, wenn die Transaktion durch eines der o. g. deterministischen Analyseverfahren festgestellt wurde. Ebenso kann das über die Feststellung gesagt werden, dass ein bestimmter PGP-Schlüssel in einem bestimmten Darknet-Forum von einem bestimmten Account gepostet wurde.[137] Soweit es sich also bei den angewendeten Verfahren nach dem Stand der Forschung in der forensischen Informatik um deterministische Methoden handelt, ist das Tatgericht regelmäßig an die Ergebnisse der Untersuchung gebunden.

Auch können hierunter wohl einige der Erfahrungssätze aus der Datenträgerforensik gefasst werden, z. B. in Bezug auf die oben dargestellten Eigenschaften von digitalen Spuren (Dritter Teil, B. II.) oder die verschiedenen Abstraktionsebenen von Datenträgern (Dritter Teil, B. III. 1. b)).

---

135 Zum Ganzen BGHSt 21, 157 (161) und MüKo-StPO/*Miebach*, § 261 Rn. 71 m. w. N.

136 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 678 ff. Vgl. auch Einordnung und Ausführungen von *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 152 ff.

137 Vgl. die Beispiele aus *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 679.

(b) Standardisierte Verfahren

Dogmatisch hergeleitet werden auch die standardisierten Verfahren im Strafprozess über die Erfahrungssätze.[138] Ähnlich der Würdigung von gesicherten wissenschaftlichen Erkenntnissen kürzen auch „standardisierte Verfahren" die Beweiswürdigung ab (siehe bereits oben Zweiter Teil, B. II. 2. a) und Dritter Teil, B. III. 5.).

In der Rspr. zu daktyloskopischen Gutachten[139], der Messung der BAK[140], dem Blutgruppenvergleich[141], chemisch-toxischen Untersuchungen des Wirkstoffgehalts von Betäubungsmitteln[142] sowie insbesondere bei DNA-Analysen[143] und automatischen Geschwindigkeitsmesssystemen (im Bußgeldverfahren)[144] hat der BGH eine Differenzierung zwischen standardisierten und nicht standardisierten Methoden vorgenommen.[145] Der BGH gibt jedoch keine Abgrenzung dazu vor, welche Art von Verfahren Tatgerichte als standardisiert betrachten können. So sollen im Gegensatz zu den eben genannten forensischen Disziplinen bspw. Glaubhaftigkeitsgutachten nicht standardisierte Ver-

---

138 Zur dogmatischen Herleitung vgl. auch *Mysegades*, Software als Beweiswerkzeug, S. 233 ff.

139 BGH, Urteil v. 29.09.1992 – 1 StR 494/92 = NStZ 1993, 95, zit. n. juris, Rn. 4; BGH, Beschluss v. 15.09.2010 – 5 StR 345/10 = NStZ 2011, 171, zit. n. juris, Rn. 9 m. w. N.

140 Standardisiert laut BGH, Beschluss v. 20.12.1978 – 4 StR 460/78 = BGHSt 28, 235, zit. n. juris, Rn. 8; BGH, Beschluss v. 15.09.2010 – 5 StR 345/10 = NStZ 2011, 171, zit. n. juris, Rn. 9. Näheres zu den verwendeten Verfahren zur BAK-Bestimmung findet sich bei *Lundt/Jahn*, Gutachten des Bundesgesundheitsamtes, S. 12 ff.

141 Standardisiert laut BGH, Urt. v. 18.12.1958 – 4 StR 399/58 = BGHSt 12, 311 = NJW 1959, 780 (781); BGH, Beschluss v. 15.09.2010 – 5 StR 345/10 = NStZ 2011, 171, zit. n. juris, Rn. 9.

142 Standardisiert laut BGH, Urt. v. 16.10.2014 – 3 StR 268/14 = NStZ-RR 2015, Rn. 10.

143 Mittlerweile bezeichnet der BGH den Gesamtprozess der DNA-Identifikation, der aus zahlreichen und arbeitsteiligen Einzelschritten sowohl technischer als auch statistischer Art besteht, als standardisiertes Verfahren, vgl. nur BGH, Beschl. v. 28.08.2018 – 5 StR 50/17 = BGHSt 63, 187, Rn. 9. Dabei besteht er eigentlich aus mehreren Einzelverfahren. Der BGH geht wohl davon aus, dass auch kompliziertere Verfahren, die mehrere Personen ausführen werden und die der ausführende Sachverständige nicht bis ins letzte Detail verstehen kann, als standardisiert angesehen werden können, vgl. *Mysegades*, CR 2018, 225 (225 f.) m. w. N. und vertiefend zur DNA-Identifikation *Mysegades*, Software als Beweiswerkzeug, S. 249 ff.; *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 685 f.

144 Vgl. vertiefend *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 686 f.; *Mysegades*, Software als Beweiswerkzeug, S. 283 ff.

145 Siehe dazu auch *Miebach*, NStZ 2021, 403 (409); *Mysegades*, Software als Beweiswerkzeug, S. 232 ff.

fahren sein, weil sie „höhere Anforderungen stellen […]".[146] Vermutlich meint der BGH damit, dass bei diesen Glaubhaftigkeitsgutachten trotz bestehender Mindeststandards[147] die individuelle Herangehensweise und Bewertung des Sachverständigen wichtiger sei, als ein einheitliches Verfahren.[148] Das entspricht jedenfalls dem vom BGH festgestellten Unterschied zwischen Blutgruppenvergleichen und „erbkundlichen" Vergleichen:[149] Bei letzterem stellt der BGH auf die Wertungsabhängigkeit des erbkundlichen Vergleichs ab und entwickelt daraus, dass die methodischen Grundlagen und Anknüpfungstatsachen besonders zu prüfen seien.[150] Auch für morphologische Gutachten kam der BGH zu dem Ergebnis, dass sie aufgrund der rein graduellen Unterschiede zwischen einzelnen äußeren Merkmalen und fehlender statistischer Daten von einer subjektiven Wertung des Sachverständigen abhängig wären. Es seien unterschiedliche Ergebnisse bei unterschiedlichen Sachverständigen zu erwarten, sodass sie nicht als standardisierte Verfahren angesehen werden könnten.[151] Gleiches scheint für Vergleichsgutachten bzgl. Werkzeugspuren zu gelten.[152]

Die Differenzierung zwischen standardisiert und nicht standardisiert betrifft zwar vordergründig die Darstellung der verwendeten Methoden und deren Weg zum gefundenen Ergebnis zum Zweck der Nachprüfbarkeit durch Rechtsmittelgerichte (vgl. § 267 StPO). Als der Darstellung vorgelagertem Schritt geht es dabei aber auch um die Verlässlichkeitsprüfung im Rahmen der Beweiswürdigung beim Einsatz standardisierter und nicht standardisierter Verfahren.[153]

Grundlegend lässt es der BGH bei standardisierten Methoden genügen, wenn das Tatgericht das Ergebnis solcher Untersuchungen als richtig anerkennt und sich die Darstellung der Überzeugungsbildung im Urteil auf die Mitteilung des Ergebnisses der Untersuchung beschränkt. Einer Erörterung der Zuverlässigkeit der Untersuchungsmethode bedarf es in solchen Fällen dagegen nicht.[154] Ist das Tatgericht von der Zuverlässigkeit des jeweiligen

---

146 BGH, Urt. v. 25.01.2011 – 5 StR 418/10, Rn. 22.

147 BGH, Urt. v. 30.07.1999 – 1 StR 618/98 = BGHSt 45, 164, Rn. 11 ff.

148 *Mysegades*, Software als Beweiswerkzeug, S. 239 m. w. N.

149 So auch *Mysegades*, Software als Beweiswerkzeug, S. 240.

150 BGH, Urteil v. 16.06.1953 – 1 StR 809/52 = BGHSt 5, 34 = NJW 1954, 83 (83 f.).

151 BGH, Urteil v. 15.02.2005 – 1 StR 91/04 = NStZ 2005, 458, zit. n. juris, Rn. 16 m. w. N.

152 BGH, Beschluss v. 15.09.2010 – 5 StR 345/10 = NStZ 2011, 171, zit. n. juris, Rn. 9.

153 Vertiefter zu den genauen Rechtsfolgen von standardisierten Verahren vgl. auch *Mysegades*, Software als Beweiswerkzeug, S. 240 f.

154 BGH, Beschl. v. 15.09.2010 – 5 StR 345/10 = NStZ 2011, 171, Rn. 9; BGH, Beschl. v. 28.08.2018 – 5 StR 50/17 = BGHSt 63, 187, Rn. 8; BGH, Beschl. v. 20.11.2019 – 4 StR 318/19 = NJW 2020, 350, Rn. 4 m. w. N. Die erste ersichtliche

standardisierten Verfahrens generell überzeugt, kann es diese generelle Überzeugung auf den Einzelfall übertragen, wenn die verfahrensgegenständliche Auswertung die Voraussetzungen des standardisierten Verfahrens erfüllt. Der Erfahrungssatz der Vergleichbarkeit aller nach dem standardisierten Verfahren durchgeführten Auswertungen spricht für die generelle Zuverlässigkeit des Verfahrens.[155] Die Rspr. geht zudem davon aus, dass sich das Tatgericht durch die Standardisierung des Verfahrens auch von der generellen Zuverlässigkeit selbst überzeugen kann mithilfe „alltäglicher Heuristiken"[156]. Das Tatgericht muss nicht jeder Prämisse seiner Überzeugung grenzenlos auf den Grund gehen, sondern darf sich auch für die Zuverlässigkeit dieser Verfahren mit einem „nach der Lebenserfahrung ausreichende[n] Maß an Sicherheit, das vernünftige Zweifel nicht aufkommen lässt", begnügen.[157]

In allen anderen Fällen muss sich das Tatgericht mit der Verlässlichkeit der verwendeten Untersuchungsmethode im Allgemeinen und ihrer Anwendung im Einzelfall auseinandersetzen.

Ohne dass der BGH es ausdrücklich sagt, entspringt die Verringerung der Darstellungspflichten praktischen und prozessökonomischen Überlegungen. Durch die Beschleunigung des Verfahrens können diese auch dem Beschuldigten zugutekommen. Wo Verfahren eingesetzt werden, die alle Sachverständigen im relevanten Bereich einheitlich befolgen und die den Tatgerichten, Verfolgungsbehörden und spezialisierten Verteidigern durch mehrfache Beschäftigung bekannt sind,[158] wäre es ein unnötiger und zeitaufwendiger Formalismus, in jedem Fall wieder die Zuverlässigkeit des Verfahrens im Einzelnen detailliert zu prüfen. Das potentielle Minus an wissenschaftlich-empiri-

---

Entscheidung des BGH, Urt. v. 18.12.1958 – 4 StR 399/58 = BGHSt 12, 311 = NJW 1959, 780 (781) hierzu spricht in einem obiter dictum von „allgemein anerkannte[n], häufig angewandte[n] Untersuchungsweisen".

155 So auch die Formulierung des BGH, Urteil v. 16.10.2014 – 3 StR 268/14 = NStZ-RR 2015, 14, Rn. 10. nach der kein standardisiertes Verfahren anzunehmen ist, wenn Anhaltspunkte für Fehler oder Abweichen vom Verfahren vorliegen.

156 Vgl. auch *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 579, Rn. 581, die diese Schlüsse bei Indizien als „Alltagstheorien" bezeichnen. Zu Risiken bei der Anwendung von Alltagsheuristiken siehe *Nink*, Justiz und Algorithmen, S. 33 f. m. w. N.; kritisch auch etwa *Keller*, GA 1999, S. 255 (258, 264), der darauf hinweist, dass die Ergebnisse von Alltagsheuristiken wissenschaftlich gesehen nicht besser sind als die für unzulässig gehaltenen Polygraphen; *Puppe*, JZ 1996, S. 318 (320): „alltagstheoretische Scheingewißheiten".

157 St. Rspr. des BGH, Urteil v. 12.07.2016 – 1 StR 595/15, zit. n. juris, Rn. 33 m. w. N.; vgl. BGH, Urteil v. 06.11.1998 – 2 StR 636/97 = NStZ-RR, 301, zit. n. juris, Rn. 11 m. w. N.; BeckOK-StPO/*Eschelbach*, 36. Aufl. 2020, § 261 Rn. 45; KK/*Ott*, 8. Aufl. 2019, § 261 Rn. 215; *Mysegades*, Software als Beweiswerkzeug, S. 237 f.

158 So BGH, Urteil v. 26.05.2009 – 1 StR 597/08 = BGHSt 54, 15, zit. n. juris, Rn. 20.

scher Richtigkeit in jedem Einzelfall kann der Rechtsstaat bei dieser Standardisierung zur effizienten Behandlung von sich häufig wiederholenden Fallgestaltungen hinnehmen.[159]

Wann aber handelt es sich um ein „standardisiertes Verfahren"?[160]

Standardisierung im beweisrechtlichen Sinne erfordert zunächst, dass in der tatsächlichen täglichen Praxis der IT-forensischen Untersuchungen bei allen relevanten Akteuren (polizei- und staatsanwaltschafts-interne IT-Sachverständige, private IT-Sachverständige, die im Auftrag der Gerichte und Staatsanwaltschaften tätig werden, etc.) dieselben Standards eingehalten werden. Hierfür nicht ausreichend ist insbesondere, dass solche Standards in der forensischen Literatur als einzuhaltende Qualitätsstandards anerkannt sind und empfohlen werden. Mindestanforderung muss ebenfalls sein, dass verschiedene Sachverständige bei der Anwendung des Verfahrens auch mit unterschiedlichen Detailmethoden zum gleichen Ergebnis kommen würden.[161] Zu Beginn seiner Rechtsprechung zum standardisierten Verfahren forderte der BGH zudem, dass die zuständigen Sachverständigeninstitutionen eine gleichbleibende Zuverlässigkeit durch „interne Präzisionskontrollen und Richtigkeitskontrollen" sowie durch Ringversuche sicherstellen.[162] Gerade das Erfordernis von Ringversuchen hat der BGH zwar seitdem nicht mehr konstant wiederholt, ihr Vorhandensein oder die Durchführung interner Qualitätskontrollen kann jedoch indiziell für die Beurteilung als standardisiertes Verfahren wirken.[163]

Die Standardisierung muss außerdem auch zu den Rechtsmittelgerichten vorgedrungen sein (v. a. zum BGH, aber auch zu den OLG für ihre jeweiligen Bezirke) und von diesen als Standardisierung im beweisrechtlichen Sinn anerkannt werden. Andernfalls könnten die Rechtsmittelgerichte nicht überprüfen, ob die Standardisierung soweit fortgeschritten ist, dass sie eine Reduzierung

---

159 *Keller*, GA 1999, S. 255 (264) m. w. N.

160 Vgl. dazu auch *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 211 f.

161 BGH, Beschluss v. 28.08.2018 – 5 StR 50/17 = BGHSt 63, 187, zit. n. juris, Rn. 11; *Müller/Eisenberg*, JR 2019, 46 (47), die darauf hinweisen, dass der BGH dieses Erfordernis selbst nicht hinreichend genau prüft. Eine Standardisierung sollte tatsächlich bereits erreicht und nicht nur wünschenswert oder angestrebt sein.

162 BGH, Beschluss v. 20.12.1978 – 4 StR 460/78 = BGHSt 28, 235, zit. n. juris, Rn. 6. Erhebliche Kritik an den Ringversuchen im Bereich DNA findet sich bei *Neuhaus/Artkämper*, Kriminaltechnik und Beweisführung im Strafverfahren, S. 114 f. m. w. N. Die die Fehlerquoten der Ringversuche seien sehr hoch. Jedenfalls bei forensisch-toxikologischen Untersuchungen von Betäubungsmittel-Gehalten sind interne und externe Qualitätskontrollen in den Richtlinien zwingend vorgesehen, vgl. etwa *Bork/Stein/El-Khadra-Klut et al.*, Toxichem Krimtech 87, 35 (42 f.).

163 *Mysegades*, Software als Beweiswerkzeug, S. 238.

der Anforderungen an die Beweiswürdigung und die Darlegung durch die Tatgerichte rechtfertigt.[164]

Schließlich dürfen keine konkreten Anhaltspunkte für Fehler oder atypische Fälle vorliegen.[165]

Auch für die forensische Informatik wäre es attraktiv Standardisierungen zu schaffen, um die hohen Anforderungen an die Detailprüfung in jedem Einzelfall zu minimieren und die Verfahren zu beschleunigen (i. S. d. Art. 6 Abs. 1 S. 1 EMRK).[166].

Allerdings lassen sich die Methoden und Erfahrungssätze der forensischen Informatik nach dem jetzigen Stand der Wissenschaft und Rechtsprechung als nicht einheitlich standardisiert bewerten.[167] Damit müssen sich die Tatgerichte mit der Verlässlichkeit und der Richtigkeitswahrscheinlichkeit der Methoden und Erfahrungssätze im Einzelfall intensiv auseinandersetzen.[168]

Begründet wird die Bewertung der Untersuchungsmethoden und Erfahrungssätze der forensischen Informatik als „nicht standardisiert" v. a. damit, dass – selbst wenn sich in einigen Bereichen in der Praxis der forensischen Informatik Standards etabliert haben – diese noch in die Rspr. der Tat- und Rechtsmittelgerichte vordringen muss, bevor eine Absenkung der Beweiswürdigungs- und Darstellungsanforderungen gerechtfertigt wäre. So zeichnet sich zwar eine positive Entwicklung in diese Richtung ab, indem sich die Tatgerichte immer vertiefter mit den einzelnen Schritten der IT-forensischen Untersuchung und der Einhaltung der Standards beschäftigen (siehe oben im 2. Teil, B. IV. 3.) und auch die Nichteinhaltung forensischer Mindeststandards in Einzelfällen gerügt wird. Prognostisch scheint eine vollständige Etablierung von Standards, wie sie in anderen forensischen Bereichen stattgefunden hat, für viele Bereiche der forensischen Informatik und Datenanalyse aber eher

---

164 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 684 ff.

165 Vgl. BGH, Urt. v. 16.10.2014 – 3 StR 268/14 = NStZ-RR 2015, 14, Rn. 10.

166 Zu Grundlage und Ausformung des Beschleunigungsgrundsatzes MüKo-StPO/*Kudlich*, Einl. Rn. 155 ff. m. w. N.

167 So auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 688.

168 Wie wenig standardisiert die aktuellen IT-Sachverständigen Gutachten sind, belegt auch eine Studie aus 2022 in Norwegen, „Reliability assessment of digital forensic investigations in the Norwegian police" von *Stoykova/Andersen/Franke/Axelsson*, Forensic Science International Digital Investigation (2022), S. 301351, die ergab, dass 21 (der 124) untersuchten Gutachten unzureichend dokumentiert waren, um die Zuverlässigkeit der digitalen Beweise zu beurteilen. Es war nicht möglich, die an den einzelnen Objekten durchgeführten digitalen kriminaltechnischen Maßnahmen nachzuvollziehen oder die digitalen Beweismittel mit ihrer Quelle in Verbindung zu bringen. In keinem der Fälle wurde nachgewiesen, dass die digitale forensische Methodik eingehalten wurde, die verwendeten Methoden und Werkzeuge gerechtfertigt waren, oder die Ergebnisse und Fehlerquoten der Tools validiert werden konnten.

unwahrscheinlich. Gründe dafür sind die Besonderheit der Technologie (Abgekoppeltheit von der physischen Welt und Universalität) und die dadurch bedingte Vielseitigkeit von Fallgestaltungen sowie die sich daraus ergebende schnelle technologische Entwicklung im Bereich der Computer- und Internettechnik.[169] Was überhaupt praktisch und technisch in einer Standardisierung festgelegt werden könnte, obliegt außerdem auch nicht den juristischen Verfahrensbeteiligten oder der Rechtswissenschaft, sondern technischen Normungsgremien oder der relevanten Branche. Denkbar wären etwa standardisierte Trainingsdatensätze für Systeme maschinellen Lernens, feste Protokollierungsschritte oder feste Qualitätsmanagementvorgaben.[170] Neben der Standardisierung der eingesetzten Datenverarbeitungs- und -analysemethoden selbst ist auch eine Standardisierung von Prüfungsverfahren durch IT-Sachverständige für die praktische Anwendung von Software zu Beweiszwecken interessant. Denn steht die Zuverlässigkeit einer Softwareauswertung in Frage, liegt aber eine sachverständige Bestätigung der Zuverlässigkeit vor, ermöglicht eine standardisierte Prüfung dem Gericht, die Qualität dieser Prüfung besser einschätzen zu können.[171]

Im Ergebnis muss sich das Tatgericht also mit der Verlässlichkeit der verwendeten Untersuchungsmethoden und Erfahrungssätze des IT-Sachverständigen im Allgemeinen und ihrer Anwendung im Einzelfall auseinandersetzen. Konkret kann das bedeuten, dass die Tatrichterinnen die Grundlagen der Erfahrungssätze und der Datenverarbeitungs- und -analysemethoden würdigen müssen; bspw. ob die Prämissen, Modelle und Implementierung tatsächlich auf wissenschaftlichem Konsens beruhen, ob es eine unabhängige Validierung in anerkannten Zeitschriften mit Peer Review gibt oder ob in den „Laboren" interne und externe Qualitätskontrollen durchgeführt wurden.[172]

Kann das Tatgericht die Einzelheiten der Methodik nicht durch Befragung des IT-Sachverständigen aufklären, muss es ihre Zuverlässigkeit auf anderem Weg klären, bspw. durch Vernehmung der verantwortlichen Software-Entwicklerinnen oder die Einholung eines weiteren Sachverständigengutachtens. Steht keiner dieser Wege zur Verfügung muss das Tatgericht den Beweiswert entsprechend niedrig bewerten.[173]

---

169 So auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 687 f. und *Mysegades*, Software als Beweiswerkzeug, S. 276 für die Verwendung von Software durch den IT-Sachverständigen.

170 *Mysegades*, Software als Beweiswerkzeug, S. 537.

171 *Mysegades*, Software als Beweiswerkzeug, S. 538. Für die IT-Forensik vgl. *Heinson*, IT-Forensik, 2015, S. 408; vgl. auch *Knopp*, GI-Jahrestagung 2009, S. 1552 (1560).

172 *Mysegades*, Software als Beweiswerkzeug, S. 276.

173 *Mysegades*, Software als Beweiswerkzeug, S. 277.

(c) Neue wissenschaftliche Erkenntnisse und Untersuchungsmethoden

V. a. für die forensische Informatik relevant ist, dass neue wissenschaftliche Erkenntnisse und Untersuchungsmethoden,[174] die (noch) nicht nach den o. g. Maßstäben als gesichert gelten können, vom Tatgericht ebenfalls zu berücksichtigen sind. Die Sachaufklärungspflicht des § 244 Abs. 2 StPO gebietet es auch, dass sich das Gericht über solche neuartigen Erkenntnisquellen unterrichtet, die für den jeweiligen Fall relevant sind und diese in seine Beweiswürdigung mit einbezieht.[175] Mit der Neuheit können geringere generelle Erprobung, geringere Anpassung auf den konkreten Nutzungsbereich sowie eine geringere kritische Kontrolle im wissenschaftlichen Feld und daraus resultierend höhere Fehleranfälligkeit zusammenfallen. Zu diesen Punkten sollte sich daher zunächst der beauftragte IT-Sachverständige in seinem Gutachten äußern, um Gericht und Prozessbeteiligten eine kritische Prüfung der Stärken und Schwächen der Methode zu ermöglichen, und schließlich das Tatgericht in seiner Beweiswürdigung. Dabei muss es v. a. die für und gegen die Validität der neuen Erkenntnisse und Methoden sprechenden Gesichtspunkte eruieren und gegeneinander abwägen.[176]

(d) Wissenschaftliche Erkenntnis mit wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit

Unterhalb der nach diesen Maßstäben gesicherten wissenschaftlichen Erkenntnisse rangieren solche wissenschaftlichen Erkenntnisse, bei denen nur eine gewisse (hohe) Richtigkeitswahrscheinlichkeit unter Anwendung wissenschaftlicher Methoden angegeben werden kann. Solche Erkenntnisse sind für das Tatgericht nicht bindend, es muss aber die Wahrscheinlichkeitsaussage in seine Beweiswürdigung einbeziehen und die Richtigkeit der Aussage im jeweiligen Einzelfall anhand weiterer Indizien bestätigen oder widerlegen.[177] Eine fehlerhaft angegebene oder berechnete Wahrscheinlichkeit kann dabei als Rechenfehler einen Verstoß gegen Denkgesetze und damit einen Fehler bei der Beweiswürdigung darstellen.[178]

---

174 Vgl. dazu auch *Mysegades*, Software als Beweiswerkzeug, S. 165 ff.

175 BGHSt 41, 206 (215).

176 *Mysegades*, Software als Beweiswerkzeug, S. 166; BGHSt 41, 206 (215); BGH StV 1994, 227; KMR/*Stuckenberg*, § 261 Rn. 36.

177 BGH NJW 1973, 1411; BeckOK StPO/*Eschelbach*, § 261 Rn. 41; *Eisenberg*, Beweisrecht der StPO, Rn. 103; siehe auch BGHSt 37, 157.

178 BGHSt 38, 320.

Hierunter sind die statistischen Methoden von Datenanalyseprogrammen zu fassen, aber nur, wenn die zugrundeliegenden Annahmen verlässlich sind.[179] Denn bei statistischen Datenanalysemethoden sind die gewonnenen Informationen nicht unzweifelhaft in den analysierten Daten enthalten. Die Informationen lassen sich aus den analysierten Daten nur mit einer gewissen Wahrscheinlichkeit entnehmen. Diese Methoden verwenden dafür Algorithmen (präzise Verarbeitungsvorschriften für ein elektronisch arbeitendes Gerät;[180] z. B. „wenn-dann-Bedingung"), die auf Annahmen (Heuristiken) basieren. Diese Annahmen wiederum basieren auf statistischen Auswertungen anderer Datensätze (sog. Ground Truth) oder auch „nur" auf Erfahrungssätzen oder kriminalistischer Erfahrung.[181]

Basieren die Grundlagen der Annahme ihrerseits auf mit wissenschaftlichen Methoden erlangten Erkenntnissen und lassen sich auf dieser Grundlage berechnete Richtigkeitswahrscheinlichkeiten angeben, kann die auf dieser Annahme basierende Methode als Erfahrungssatz mit wissenschaftlich fundierter Wahrscheinlichkeitsangabe behandelt werden. In anderen Fällen, in denen – z. B. mangels Verfügbarkeit von Ground Truth Daten – eine solche Angabe nicht möglich ist oder nicht auf wissenschaftlich fundierte Methoden gestützt werden kann, sind die Ergebnisse eines statistischen Datenverarbeitungsvorgangs lediglich wie „sonstige" Erfahrungssätze zu behandeln.[182] Die wissenschaftliche Fundierung von Annahmen und die Angabe einer darauf basierenden Richtigkeitswahrscheinlichkeit ist Gegenstand aktueller Forschung im Bereich der forensischen Informatik, bspw. für den Bereich der praxisrelevanten Kryptowährungsanalysen. Hier wird versucht, die Verlässlichkeit der vielfach in kommerziellen wie nicht-kommerziellen Tools verwendeten „Multi-Input-Heuristik" zu berechnen. Daneben werden Taxonomien für verschiedene Formen der Annahmen entwickelt, welche sich nach unterschiedlicher Verlässlichkeit ordnen lassen.[183] Können für die zugrundeliegenden Annahmen keine verlässlichen Richtigkeitswahrscheinlichkeiten berechnet werden, weil die Annahmen auf unberechenbaren Vorgängen basieren (z. B. bei Annahmen hinsichtlich des Verhaltens von Nutzern bestimmter Internetdienstleistungen), kommt für eine wissenschaftlich fundierte Berechnung der Richtigkeitswahrscheinlichkeit auch die Durchführung wissenschaftlicher Testreihen mit dem Werkzeug in Betracht, bei denen das auf der Annahme basierende Werkzeug auf bekannte Datensätze angewendet wird und die Anteile der – je

179 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 680.

180 *Nink*, Justiz und Algorithmen, S. 143.

181 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 680.

182 Vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 681 m. w. N.

183 *Deuber/Ronge/Rückert*, Proceedings on Privacy Enhancing Technologies (2022), Vol. 3, S. 670 ff.

nach der Funktion des Tools – „richtigen" Ergebnisse dokumentiert werden (z. B. im Fall von Klassifizierungen: die richtig-positiven, richtig-negativen, falsch-positiven und falsch-negativen Ergebnisse).

In diesen Fällen ist das Tatgericht zwar nicht an das Ergebnis gebunden und muss die bloße Wahrscheinlichkeit der Richtigkeit mit anderen Indizien abgleichen und sich in seiner Beweiswürdigung damit auseinandersetzen. Ist jedoch die Höhe der Richtigkeitswahrscheinlichkeit ihrerseits wissenschaftlich unumstritten, muss das Tatgericht jedenfalls diese Höhe zugrunde legen.[184]

Bei annahmebasierten Datenanalysemethoden sind weiterhin jedoch die Einflussfaktoren auf diese Richtigkeitswahrscheinlichkeit vom Tatgericht bei seiner Beweiswürdigung zu beachten. So führt Rückert[185] überzeugend aus, dass sich die Richtigkeitswahrscheinlichkeit der zugrundeliegenden Annahmen im Zeitverlauf oder durch bestimmte Ereignisse (wie Änderungen in den Protokollen der analysierten Systeme, z. B. der Blockchain-Systeme von Kryptowährungen) verändern können, was ggf. Einfluss auf die Höhe der Richtigkeitswahrscheinlichkeit der Annahme haben kann. Dadurch können bislang als Erfahrungssätze mit fundierter wissenschaftlicher Richtigkeitswahrscheinlichkeit behandelte Methoden in den Bereich sonstiger Erfahrungssätze verschoben werden. Ebenso müssen etwaige (ggf. neu auftretende) Fehlerquellen, welche die zugrundeliegende Annahme betreffen, vom Tatgericht identifiziert werden. Ein praxisrelevantes Beispiel für eine solche Fehlerquelle ist etwa die zunehmende Vornahme sog. CoinJoin-Transaktionen in Kryptowährungssystemen, bei denen zu Anonymisierungszwecken mehrere Transaktionen mehrerer Nutzer in einer großen Transaktion an die verschiedenen Empfänger zusammengefasst werden.[186] Werden solche Transaktionen von einem Analysetool auf Basis der o. g. Multi-Input-Heuristik analysiert, wird es zu falsch-positiven Treffern kommen, weil das Programm die Adressen der CoinJoin-Transaktion demselben Cluster zuordnet, obwohl es sich tatsächlich um verschiedene Nutzer handelt.[187]

(e) Sonstige Erfahrungssätze

Auf unterster Stufe der Verlässlichkeitsskala stehen die sonstigen bzw. „einfachen" Erfahrungssätze; also diejenigen, die nicht auf wissenschaftlich gesicherten Erkenntnissen beruhen, nicht zu den neuartigen, umstrittenen wis-

184 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 682.

185 Digitale Daten als Beweismittel im Strafverfahren, S. 682 f.

186 *Möser/Böhme*, Join Me on a Market for Anonymity, WEIS 2016; *Fröwis et al.*, Forensic Science International: Digital Investigation (2020) Vol. 33, 200902, S. 2 f.

187 *Fröwis et al.*, Forensic Science International: Digital Investigation (2020) Vol. 33, 200902, S. 2 f.

senschaftlichen Methoden und Erkenntnissen gehören und bei denen auch keine auf wissenschaftlichen Methoden basierende Wahrscheinlichkeitsangabe hinsichtlich der Richtigkeit möglich ist. Diese Erfahrungssätze können aus verschiedenen Berufs- oder Lebensbereichen herrühren, und insbesondere auch kriminalistische Erfahrungsregeln sein. Mangels wissenschaftlich „messbarer" bzw. berechenbarer Wahrscheinlichkeit kommt diesen Erfahrungssätzen bloße Indizwirkung zu, welche in die Beweiswürdigung des Gerichts gemeinsam mit anderen Indizien einfließt.[188] Hier spielt v. a. die Einhaltung der oben beschriebenen Standards der forensischen Informatik eine Rolle (siehe im 3. Teil, B. III. 5.). Auch kann die Qualität der Input-Daten dazu gehören.[189] Eine Beweiswürdigung ist insbesondere dann fehlerhaft, wenn das Ergebnis solchen Erfahrungssätzen widerspricht und das Tatgericht sich hierzu nicht geäußert hat.[190]

Technische Regelwerke wie Normen der DIN oder VDI sind selbst keine Erfahrungssätze, können solche aber enthalten. Das hat das Gericht im Einzelfall festzustellen.[191]

In der forensischen Praxis – v. a. in der forensischen Informatik – sieht man sich oft vor dem Problem, dass es nur selten verlässliche Informationen über die Häufigkeitsverteilung von Indizien und über die Anfangswahrscheinlichkeit gibt.[192] Im Rahmen der Würdigung und der objektiven Bestimmung der persönlichen Gewissheit müssen die Verfahrensbeteiligten also stets Überlegungen zu einer „gedachten" bzw. „geschätzten" Häufigkeitsverteilung anstrengen, wenn sie die Beweisbedeutung eines durch den IT-Sachverständigen ermittelten Indizes im konkreten Fall beurteilen möchten (auch wenn das nicht explizit zum Ausdruck gebracht bzw. gar quantifiziert wird).[193] Ausschlaggebend dabei ist stets, wie gut diese Alltagstheorien wissenschaftlich geprüft sind. Bei diesen Fragen – ob es den Erfahrungssatz überhaupt gibt und ob das Indiz bei der Haupttatsache häufiger bzw. seltener bei der Nicht-Haupttatsache vorkommt – sind oft nur Überlegungen auf einem Plausibilitätsniveau möglich (vgl. dazu bei B. II. 1.).[194] So bedarf es dann zur Bestim-

---

188 Hierzu: BGH NStZ-RR 1998, 267; BeckOK-StPO/*Eschelbach*, § 261 Rn. 41; KMR/*Stuckenberg*, § 261 Rn. 36.

189 Siehe zum sog. Garbage-in-Garbage-out-Problem, *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 695 f.

190 BGH NStZ-RR 2010, 182 (183).

191 *Mysegades*, Software als Beweiswerkzeug, S. 64 m. w. N.

192 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 629.

193 Vgl. vertiefend dazu *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 580.

194 Vgl. vertiefend dazu *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 581.

mung der Richtigkeitswahrscheinlichkeit der Methodik eines Erfahrungssatzes (einer „gedachten Häufigkeit"), um die Beweiskraft der Tatsachengrundlage erörtern und hinterfragen zu können, auf welcher Basis der Schluss (z. B. die Hypothese zum Tathergang) erfolgte.[195] Schätzungen von Anfangswahrscheinlichkeiten sind großzügig anzulegen, um den Kreis der möglichen Alternativen bzw. Tatverdächtigen nicht zu früh einzuengen. Dabei helfen konkrete Randbedingungen.[196]

In diesem Zusammenhang soll auch auf die Dringlichkeit hingewiesen werden, in der Wissenschaft der forensischen Informatik die Studienlage, die Tests und damit auch die kriminalistischen Erfahrungswerte auszuweiten und zu vertiefen.

Es ist allerdings darauf zu achten, dass es bei dem Schluss vom Indiz auf die Haupttatsache nicht auf die bloße Möglichkeit ankommt (bspw. dass das Indiz zusammen mit der Haupttatsache vorkommt), sondern auf die Asymmetrie (dass das belastende Indiz häufiger bei der Haupttatsache als bei der Nicht-Haupttatsache vorkommt).[197] Das widerspricht insoweit auch nicht der sachlich-rechtlichen Überprüfung der tatrichterlichen Beweiswürdigung, wonach die Schlüsse des Tatrichters von einem Indiz auf eine Haupttatsache nur möglich sein müssen. Das betrifft lediglich die Grenzen der revisionsgerichtlichen Überprüfung der tatrichterlichen Beweiswürdigung. So gilt es, die zwei Ebenen der Beweiswürdigung durch den Tatrichter und die revisionsgerichtliche Überprüfung der tatrichterlichen Beweiswürdigung auseinander zu halten.[198] Für den Tatrichter gilt also, wenn er ein Indiz für belastend halten will, dass dieses die Wahrscheinlichkeit der Beweistatsache erhöhen muss. Die Schlüsse, auf die es ankommt, sind die Antworten auf die Fragentrias.[199]

Weil der Gesetzgeber der freien Beweiswürdigung und der Einschätzung des Beweiswerts durch das Tatsachengericht vertraut, soll zunächst grundsätzlich kein Beweismittel von der Beweiswürdigung ausgeschlossen sein. Eine enge Ausnahme bildet aber die Ungeeignetheit eines Beweismittels, wenn feststeht, dass „jede Möglichkeit ausgeschlossen ist," dass das Beweismittel Sachdienliches ergeben kann und es „völlig wertlos" ist.[200] Wenn nach Mysegades[201] in Frage steht, ob eine Software eine klare und wiederholbare Metho-

---

195 *Dewald/Freiling*, Forensische Informatik, S. 49 f.; vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 578.

196 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 633.

197 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 635.

198 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 636.

199 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 637.

200 Löwe/Rosenberg/*Sander*, § 261, Rn. 90b; Vgl. auch *Mysegades*, Software als Beweiswerkzeug, S. 69 m. w. N.

201 Software als Beweiswerkzeug, S. 70.

dik verfolgt, ob sie auf Grundlage einer gesicherten und geeigneten Datengrundlage arbeitet, ob sie manipulationssicher ist oder ob hinreichende empirische Belege für die Zuverlässigkeit der Ergebnisse (Validierung) vorliegen, komme eine völlige Ungeeignetheit i. S. d. § 244 Abs. 3 S. 3 Nr. 4 StPO zumindest in Betracht. Hieran reiht sich auch die Frage, der sich Rückert[202] angenommen hat, wie das Tatgericht im Rahmen der Beweiswürdigung, insbesondere mit den Ergebnissen von sog. Blackbox-Tools, umgehen muss.[203]

(f) Die Folgen von Blackbox-Tools[204] für die Beweiswürdigung

Die Frage nach der Einschätzung des Beweiswerts im Rahmen der Beweiswürdigung bzw. der Ungeeignetheit des Beweismittels betrifft sowohl die Konstellation, in der bei einem kommerziellen Blackbox-Tool die Aufklärung der Funktionalität scheitert, als auch solche, bei denen Blackbox-Tools unter einem grundlegenden Nachvollziehbarkeitsmangel leiden. Das ist insbesondere beim Einsatz von selbstlernenden Datenanalysemethoden (maschinelles Lernen, künstliche Intelligenz) der Fall. Der Nachvollziehbarkeitsmangel liegt darin begründet, dass Programme des maschinellen Lernens ihre Algorithmen und die den Algorithmen zugrundeliegenden Heuristiken aus Trainingsdaten selbst entwickeln und fortwährend anpassen.[205] Häufig können nicht einmal mehr die Entwickler selbst genau erklären, wie das Programm zu einem gefundenen Ergebnis gelangt.[206] Selbst wenn das prinzipiell möglich ist (so nimmt das Forschungsfeld der „selbsterklärenden" und „erklärbaren" KI immer weiter zu), besteht für die Beteiligten im Strafverfahren regelmäßig das Problem, dass sie keinen Zugang zu den Trainingsdaten haben (bspw. wegen des Geschäftsgeheimnisses bei kommerziellen Programmen)[207]. Auch die Überprüfung selbstlernender Programme durch IT-Sachverständige mit Hilfe sog. Interpretations-Tools[208] ist derzeit nur eingeschränkt möglich und

202 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 688 ff.

203 Vgl. *Valerius*, ZStW 133 (2021), S. 152 (163), der den Einsatz von Blackbox-Tools generell mit dem Grundsatz der freien richterlichen Beweiswürdigung für nicht vereinbar hält.

204 Die Probleme ergeben sich auch für andere forensische Disziplinen, denn die Technologie und ihre Vor- und Nachteile kommen auch dort zur Wirkung, vgl. nur *Jackson/McAreavey*, Retskraft – Copenhagen Journal of Legal Studies (2019) Vol. 3, Nr. 1.

205 Für Details zu verschiedenen Lern-Modellen, siehe *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 306; *Alpaydin*, Maschinelles Lernen, S. 2.

206 Siehe hierzu etwa *Gless*, Georgetown Journal of International Law 2020, Vol. 51, No. 2, S. 195 (S. 211 ff.); *Coglianese/Lehr*, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 Geo. L.J. 1147 (2017).

207 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 689.

208 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 696.

führt häufig nicht zur vollständigen Nachvollziehbarkeit der Vorgänge innerhalb des selbstlernenden Systems.[209]

Für die eigentliche Beweiswürdigung der Ergebnisse des Blackbox-Tools kommt es anschließend darauf an, inwieweit eine Richtigkeitswahrscheinlichkeit ermittelt werden konnte und ob diese Richtigkeitswahrscheinlichkeit einer solchen mit wissenschaftlicher Fundierung entspricht.[210]

Existieren im Zeitpunkt der Entscheidung bereits Interpretations-Tools und Testmöglichkeiten für das jeweilige Blackbox-Programm, die eine breite wissenschaftliche Anerkennung erfahren haben und die eine nach wissenschaftlichen Methoden mit an Sicherheit grenzender Wahrscheinlichkeit zutreffende Aussage über die Richtigkeitswahrscheinlichkeit der Methodik treffen können, finden die o. g. Grundsätze über Erfahrungssätze mit wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit Anwendung: Die Angabe der Richtigkeitswahrscheinlichkeit ist in die tatrichterliche Beweiswürdigung mit einzubeziehen und das Ergebnis mit anderen verfügbaren Indizien abzugleichen, um es zu bestätigen oder zu widerlegen[211]. Diese Situation dürfte derzeit allerdings für die wenigsten Blackbox-Tools gelten. Rückert[212] sieht einen solchen künftigen Anwendungsbereich hauptsächlich für Blackbox-Tools, die einen engen, klar definierten Anwendungsbereich hätten (z. B. Klassifizierungssysteme für Bild- und Videomaterial, das bestimmte Eigenschaften aufweist, bspw. Erkennung von Kinderpornographie oder Erkennung von KFZ-Kennzeichen, Gesichtserkennung, Text-Erkennung und Stimm-Identifikation).[213] Gleiches würde für die Überwachung von Vermögenstransaktionen gelten.[214]

Für Blackbox-Tools, bei denen sich keine derart wissenschaftlich fundierte Aussage über die Richtigkeitswahrscheinlichkeit treffen lässt, fordert Rückert bei der Einordnung als sonstiger Erfahrungssatz als „Erfahrungssatz für eine ‚geschätzte' Richtigkeitswahrscheinlichkeit" zumindest, dass das Tool sich in (wenn auch nicht wissenschaftlich fundierten) Testreihen und ggf. beim Einsatz in der Realwelt als „zuverlässig" erwiesen hat und somit zumindest eine geschätzte Aussage über die Richtigkeitswahrscheinlichkeit möglich ist.[215]

---

209 *Kaur et al.*, Interpreting interpretability: Understanding data scientists' use of interpretability tools for machine learning, CHI 2020, Paper 92.

210 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 696.

211 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 689.

212 Digitale Daten als Beweismittel im Strafverfahren, S. 689.

213 Vgl. Interpol, Towards Responsible AI Innovation – Second Interpol-Unicri Report on Artificial Intelligence in Law Enforcement, S. 12 ff., abrufbar unter https://unicri.it/towards-responsible-artificial-intelligence-innovation [26.6.2023].

214 *Salditt*, in: Fischer/Hoven (Hrsg.), Verdacht, S. 199 (S. 201 ff.).

215 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 696 f.

Das ist derzeit der Fall bei Programmen zur Auswertung von komplexen, von vielen Variablen abhängigen und daher i. d. R. sich häufig untereinander unterscheidenden Sachverhalten (wie Verhaltensanalysen, z. B. die Suche nach „verdächtigem Verhalten" auf Videos oder die Analyse sozialer Netzwerke).[216]

Schließlich kann nach Rückert[217] für den Umgang mit solchen Blackbox-Tools, bei denen sich das Gericht mit sachverständiger Hilfe unter Einbezug des Standes der Forschung nicht von der Zuverlässigkeit überzeugen kann (insb. keine Aussage zur Richtigkeitswahrscheinlichkeit möglich ist), auf die Rspr. des BGH zum Polygraphen als ungeeignetes Beweismittel zurückgegriffen werden.[218] Nach den dort entwickelten und später bestätigten Grundsätzen fehlt es einem Beweismittel an der Beweiseignung und damit an jedem – auch indiziellen – Beweiswert, wenn die Zuverlässigkeit der Untersuchungsmethode und die Richtigkeitswahrscheinlichkeit des Ergebnisses nach dem Stand der Forschung nicht bestimmt werden kann und auch kaum Kriterien für die Bestimmung der Zuverlässigkeit vorhanden sind.[219] Die Würdigung eines solchen Beweismittels ist dem Tatgericht nicht möglich, weil es keine Aussage über die Zuverlässigkeit und den Beweiswert des Beweismittels innerhalb der vorzunehmenden Gesamtbetrachtung mit anderen Indizien treffen kann. Das Beweismittel kann andere Indizien weder bestätigen noch widerlegen. Das Gericht kann auch nicht bemessen, wie gewichtig das Indiz aus dem ungeeigneten Beweismittel ist und damit, ob die Gesamtschau der Indizien unter Einbeziehung des ungeeigneten Beweismittels ausreicht, um zu einer subjektiven Gewissheit i. S. v. § 261 StPO zu gelangen. Bei der Betrachtung von Blackbox-Tools gilt danach, dass wenn nach dem Stand der Forschung

---

216 *Kakadiya et al.*, AI Based Automatic Robbery/Theft Detection using Smart Surveillance in Banks 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), S. 201; *Nurek/Michalski*, Appl. Sci. 2020, Vol. 10 No. 5, 1699.

217 Digitale Daten als Beweismittel im Strafverfahren, S. 385, 696 f.

218 Vgl. dazu die grundlegende Entscheidung des BGH, Urteil v. 17.12.1998 – 1 StR 156/98 = BGHSt 44, 308, zit. n. juris, Rn. 28 f., 48 f., 52 f., 55 ff., 71 f.: Hier wird davon ausgegangen, dass die Methode aufgrund unsicherer oder zweifelhafter Datenlage hinsichtlich der gezogenen Rückschlüsse, mangelnder Standardisierbarkeit der Durchführung und eines kaum abschätzbaren Manipulationsrisikos nicht als hinreichend wissenschaftlich valide anzusehen ist, vgl. *Mysegades*, Software als Beweiswerkzeug, S. 265 f.; siehe auch *Momsen*, KriPoZ 2018, 142 (144 ff.). In diesem Zusammenhang sind auch die Ausführungen von *Neuhaus*, in: FS Beulke, S. 911 (921 ff.) interessant, der sich ausführlich mit dem forensischen – nicht computergestützten – Profiling als polizeilicher Ermittlungsmethode auseinandergesetzt hat und es aufgrund einer mangelnden klaren Methodik und fehlender empirischer Belege für seine Ergebnisse für ein völlig ungeeignetes Beweismittel hält.

219 Grundlegend BGHSt 44, 308; bestätigt durch BGH NStZ 2011, 474; zur Parallelproblematik beim Einsatz von KI zur Lügenerkennung: *Rodenbeck*, StV 2020, 479.

keine auf rationalen Erwägungen fußende Aussage zur Richtigkeitswahrscheinlichkeit getroffen werden kann und es an sachlichen Kriterien zur Bestimmung der Richtigkeitswahrscheinlichkeit fehlt, das Ergebnis des Datenanalysevorgangs keinen Beweiswert hat und nicht in die Beweiswürdigung einbezogen werden darf.[220]

(3) Fazit und Ideen zur Verbesserung

Wie oben bereits dargestellt, muss das Tatgericht in Bezug auf die sachverständige Methodik, und damit auch die angwandten Datenverarbeitungs- und -analysemethoden, ermitteln, ob es an deren Auswertung wegen wissenschaftlicher Erkenntnisse oder Erfahrungssätze gebunden ist. Ist die Auswertung nachweisbar eine Repräsentation gesicherter wissenschaftlicher Erkenntnisse und kann sich das Gericht hiervon etwa durch eine alternative Berechnung überzeugen, ist es an die Auswertungsergebnisse insoweit gebunden. Gibt es dagegen keinen Nachweis dafür, dass die sachverständige Analyse wissenschaftliche Methoden verfolgt oder wissenschaftliche Standards einhält, muss das Tatgericht sie genauso behandeln wie jede andere bloße Behauptung. Es muss sich dann über andere Indizien eine volle Überzeugung von der Richtigkeit der Behauptung in Form der Ergebnisse der Datenauswertung bilden.[221] Je nachdem wie sicher die präsentierten Sachverständigenergebnisse den Schluss auf die entscheidungserhebliche Beweisfrage vorgeben, desto umfangreicher ist auch die Funktion dieses Ergebnisses für die Sachverhaltsfeststellung. Während ein als weniger sicher bzw. wahrscheinlich präsentiertes Ergebnis nur mit mehreren weiteren Indizien in der Gesamtwürdigung auf die entscheidungserhebliche Tatsache hinweisen kann, vermag ein ausreichend sicheres Ergebnis unter Umständen auch allein den Schluss auf eine entscheidungserhebliche Tatsache begründen, womit keine weiteren Beweismittel für die Überzeugungsbildung erforderlich wären. Für die forensische Informatik wird häufig gelten, dass das präsentierte Sachverständigenergebnis mit weiteren Indizien in die Gesamtwürdigung eingestellt werden muss, denn sie werden i. d. R. nur gewisse Wahrscheinlichkeitsurteile liefern und das Gericht kann diese nur mit einer entsprechenden Wahrscheinlichkeitsquote in seine Gesamtindizienwürdigung einstellen.[222]

Im Anschluss an die vorweggenommenen Ausführungen bei der (eingeschränkten) Weisungsfreiheit des IT-Sachverständigen, soll an dieser Stelle als Fazit noch einmal darauf hingewiesen werden, dass – Rückert folgend –

220 So ähnlich auch die Ausführungen von Mysegades zur Ungeeignetheit von Beweismitteln, siehe *Mysegades*, Software als Beweiswerkzeug, S. 68 f. m. w. N.

221 So auch *Mysegades*, Software als Beweiswerkzeug, S. 65.

222 *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 206 f.

unter den Gesichtspunkten der Aufklärungspflicht nach § 244 Abs. 2 StPO und der Pflicht zur erschöpfenden Beweiswürdigung nach § 261 StPO unter Heranziehung der bestmöglichen und sachnächsten Beweise ein Vorrang der Verwendung von nachvollziehbaren IT-forensischen Erfahrungssätzen sowie Untersuchungs- und Datenanalysemethoden mit hoher Richtigkeitswahrscheinlichkeit besteht, wenn eine gleiche Eignung vorliegt. Das hat der Auftraggeber bereits im Rahmen seiner Leitungsbefugnis nach § 78 StPO sicherzustellen, vgl. dazu Zweiter Teil, B. VII.

Weiter sollen Beispiele dargestellt werden, die evtl. geeignet sein könnten, die Qualität der forensischen Ergebnisse für die juristische Praxis zu verbessern: Zunächst könnte am Ende des Verfahrens (nach Urteilsspruch bzw. Rechtshängigkeit) gemeinsam mit einer zuständigen Person eine Einzelevaluation der IT-forensischen Analyse durchgeführt werden. Dabei könnte bspw. anhand eines nach der Analyse erfolgten Geständnisses bzw. Zeugenaussagen o. ä. überprüft werden, inwieweit die Ergebnisse der Analyse mit den weiteren Ermittlungsergebnissen und Erkenntnissen aus der Hauptverhandlung übereinstimmen. Dabei wird die prozentuale Richtigkeit der Analyseergebnisse ausgewertet. Danach werden die richtigen/falschen Aussagen dahingehend überprüft, wie stark sie übereinstimmen bzw. abweichen.[223] So könnte eine Art Trefferquote für die Tathergangskonstruktion bzw. das Täterprofil erstellt und bewertet werden.[224]

Als Vorbild könnten weiter die Regelungen zu BAK-Messungen dienen. Diese sind zum einen stets mit zwei voneinander unabhängigen, technisch unterschiedlichen Messverfahren durchzuführen. Zum anderen sehen Richtlinien interne und externe Qualitätskontrollen der Labore vor.[225] In diesem Zusammenhang könnte das „Blind-Testing" der Forensiker als Beispiel herangezogen werden, wie es in den USA bei anderen forensischen Gebieten praktiziert wird. Für den Bereich der forensischen Informatik könnte die Schwierigkeit der Image-Erstellung bspw. durch eine Zusammenarbeit mit dem Masterstudiengang der forensischen Informatik überwunden werden, indem man die Studierenden ein Image im Rahmen einer praktischen Übung erstellen lassen könnte.

In Bezug auf die Prüfung der Zuverlässigkeit der von IT-Sachverständigen angewendeten Software kann auf die Ausführungen von Mysegades[226] und Rückert[227] verwiesen werden. Danach stehen Entwicklerinnen und Testerin-

223 Vgl. *Stinshoff*, Operative Fallanalyse, S. 45 f.

224 Vgl. auch *Stinshoff*, Operative Fallanalyse, S. 34.

225 *Mysegades*, Software als Beweiswerkzeug, S. 248 m. w. N.

226 Software als Beweiswerkzeug, S. 45 ff. m. w. N.

227 Interpretations-Tools und Testverfahren in Bezug auf Blackbox-Tools, vgl. *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 694 f.

nen die Kontrolle des vorhandenen Quellcodes und die dynamische Kontrolle ohne Kenntnis (Blackbox-Test) oder mit Kenntnis des Quellcodes (Whitebox-Test) durch die Untersuchung von Input- und Output-Daten bei laufendem Programm zur Auswahl. Weiter können sich Gerichte und Tool-Anwenderinnen auf externe Indizien stützen, um die Zuverlässigkeit der Software zu prüfen, wie bspw. empirische Beobachtungen der Realität oder Zeugenaussagen, die mit den Ergebnissen der Software übereinstimmen oder etwa die jahrelange fehlerfreie Anwendung.[228] Darüberhinaus könnten auch Validierungsstudien in Zeitschriften mit Peer Review, Zertifizierungen oder Konformitätsbewertungen der angewendeten Software[229] sowie eine Dokumentation der einzelnen Berechnungsschritte dabei helfen, um eine Nachvollziehbarkeit greifbarer zu machen.[230]

dd) Die Belastungswahrscheinlichkeit

Zurück bei der Prüfung der Beweiskraft ist allerdings die prozessentscheidende Frage vielmehr, wie wahrscheinlich die Haupttatsache geworden ist, nachdem das Indiz festgestellt ist, die „Belastungswahrscheinlichkeit".[231]

In diesem Zusammenhang begegnet man häufig dem Trugschluss, der als „inverse fallacy" (auch „Vertauschungsfehler") bezeichnet wird.[232] Dabei werden die Vorgaben aus der Fragentrias umgedreht. Es wird fälschlicherweise danach gefragt, wie wahrscheinlich es ist, dass das Indiz vorliegt, wenn die Haupttatsache feststeht (vgl. dazu auch das oben angeführte Beispiel). Dieser Vertauschungsfehler kann sich auch bei der Bewertung der Beweisbedeutung des Lügendetektors[233] auswirken. Die (scheinbar hohen) Trefferquoten des Polygraphen entsprechen den bedingten Wahrscheinlichkeiten des hier gebrachten Beispielfalls. Sie besagen nur, wie häufig die „positive Meldung der Software von NCMER" erstattet wird bzw. ausbleibt, wenn man einen Social-Media-Nutzer testet, der Rinografie hochlädt und verbreitet („Delinquenten Social-Media-Nutzer") oder einen Social-Media-Nutzer testet, der keine Rinografie hochlädt und verbreitet („Gesetzestreuen Social-Media-Nutzer"). Im Fall des Polygraphen: Wie häufig ist das Testergebnis positiv bzw. negativ, wenn man einen wirklichen Lügner bzw. einen wirklichen Nicht-

228 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 47 ff. mit weiteren Fallbeispielen.

229 *Mysegades*, Software als Beweiswerkzeug, S. 527 ff.

230 *Mysegades*, Software als Beweiswerkzeug, S. 255 f. m. w. N.

231 Vgl. vertiefend dazu *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 585.

232 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 587.

233 Vgl. BGH NJW 1999, 657.

Lügner testet. Diese Wahrscheinlichkeiten dürfen nicht umgedreht werden, wenn es um die prozessrelevante Frage geht, wie wahrscheinlich es ist, dass man nach positivem Testergebnis auch tatsächlich einen Lügner entlarvt hat.[234]

Für die Abschätzung der Belastungswahrscheinlichkeit wird eine „Anfangswahrscheinlichkeit" („apriori) vorausgesetzt. Wenn man diese vernachlässigt, bezeichnet man diesen Trugschluss auch als „base rate neglect" oder „Trugschluss des Staatsanwalts" (bzw. „Verteilungsfehler").[235]

Der Beispielfall könnte also dahingehend fortgeführt werden, dass einer von 1.000 Social-Media-Nutzern in Deutschland auf Instagram Rinografie hochlädt und verbreitet. Werden nun alle 1.000 Social-Media-Nutzer von der Software von NCMER getestet, wird der eine „Delinquente Social-Media-Nutzer" positiv gemeldet; aber auch 1 %, also 10, der „Gesetzestreuen Social-Media-Nutzer" werden von der Software gemeldet. Von den insg. 11 gemeldeten Social-Media-Nutzern hat jedoch nur einer tatsächlich Rinografie hochgeladen und verbreitet. Die Belastungswahrscheinlichkeit – also die Wahrscheinlichkeit, dass sich nach dem Test unter den gemeldeten auch tatsächlich ein „Delinquenter Social-Media-Nutzer" befindet – beträgt also 1/11, mithin nur 9 %.

Die Beweiskraft der Meldung der Software ist jedoch nach wie vor hoch signifikant, denn die Wahrscheinlichkeit hat sich von ursprünglich 0,1 % auf ca. 9 % (also um das 90-fache) erhöht.

Das Beispiel könnte jetzt beliebig geändert werden: So könnte man den Test nicht auf Social-Media-Nutzer von Instagram, sondern auf Internetnutzer von „Elysium" oder „Deutschland im Deep Web"[236] übertragen; dann wäre die Anfangswahrscheinlichkeit wohl viel höher. Oder der Test würde sich auf ein Chatforum „Rechts- und IT-Professorinnen im Austausch über Kochrezepte und Gartentipps" beziehen; dann wäre die Anfangswahrscheinlichkeit vermutlich niedriger.

In den verschiedenen Fallkonstellationen wäre die abstrakte Beweiskraft des Indizes jeweils gleich (95 zu 1). Die konkrete Beweiskraft hängt viel mehr von der jeweiligen Anfangswahrscheinlichkeit ab.

---

234 Wie häufig die „gefühlsmäßige Einschätzung" der Belastungswahrscheinlichkeit falsch sein kann, zeigt der Test von Schweizer, vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 586.

235 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 589; zur Berücksichtigung der a priori-Wahrscheinlichkeit vgl. auch *Mysegades*, Software als Beweiswerkzeug, S. 143 f.

236 Vgl. https://www.deutschlandfunk.de/strafverfolgung-im-darknet-wie-der-staat-im-netz-nach-100.html [29.6.2023].

Die Überlegung, die den Beispielfall trägt, ist das Theorem von Bayes.[237] Damit lässt sich errechnen, wie sich die Anfangswahrscheinlichkeit nach Berücksichtigung von neuen Informationen erhöht hat.[238]

Bezüglich der Anfangswahrscheinlichkeit ergeben sich die gleichen Herausforderungen für die Verfahrensbeteiligten wie zu der Häufigkeitsverteilung von Indizien: Die fehlende Studienlage und Quantifizierbarkeit der Richtigkeitswahrscheinlichkeit.

c) Zwischenergebnis

Bei der Bestimmung der objektiven Stärke der freien tatrichterlichen Überzeugung nach § 261 StPO ist im Rahmen der Würdigung der Tatsachengrundlage auf die „Überzeugungskraft" der Ergebnisse der Sachverständigentätigkeit einzugehen.

Die Gerichte müssen dafür die Grundlagen, die Schlussfolgerungen und Hypothesen offenlegen sowie die objektive Wahrscheinlichkeit der Richtigkeit dieser Hypothese bestimmen.

Für die Bestimmung der Zuverlässigkeit der zugrundeliegenden Richtigkeitswahrscheinlichkeit kommt es beim IT-Sachverständigenbeweis auf die konkret angewendeten Erfahrungssätze und verwendeten Datenverarbeitungs- und analysemethoden an, wobei diese dann, entsprechend ihrer Kategorien (deterministische, statistische und selbstlernende Methoden), in eine Zuverlässigkeitsskala eingeordnet werden können.[239] Nicht zuletzt bedarf es dafür einer intersubjektiven Diskutierbarkeit und Nachvollziehbarkeit der Zuverlässigkeit der zugrundeliegenden sachverständigen forensischen Methoden, da es sich bei den verschiedenen IT-Sachverständigenaussagen (auch der zugrundeliegenden Datenverarbeitungs- und -analysemethoden) um „nicht standardisierte" Methoden handelt.

Im Bereich der forensischen Informatik wird selten eine Richtigkeitswahrscheinlichkeit oder Häufigkeitsverteilung quantifizierbar angegeben werden können, weshalb sich die Tatgerichte regelmäßig mit Erfahrungssätzen („gedachten Häufigkeiten") zur Einschätzung der Richtigkeitswahrscheinlichkeit der Methodik auseinandersetzen müss(t)en; so auch im oben angeführten Kemptener Bitcoin-Fall[240] oder in dem „echten" Fall, an dem der Beispielfall

---

237 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 593, 643 ff.

238 Vgl. *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 647.

239 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 651 ff.

240 Zum Verfahrensgang: LG Kempten, 29.10.2014 – 6 KLs 223 Js 7897/13; BGH, 21.07.2015 – 1 StR 16/15; LG Kempten, 13.4.2016 – 13 Ss 360/16; BGH, 27.7.2017 – 1 StR 412/16.

(siehe A. III. 4. b) aa)) angelehnt wurde. Hier wurde die Meldung durch eine „automatisierte Blackbox-Software" aus den USA generiert und es konnten weder Angaben bzgl. der zugrundeliegenden Annahmen gemacht noch die Einhaltung der Standards der forensischen Informatik geprüft werden. Auch gibt es (noch) keine Erfahrungssätze für die Beurteilung der Richtigkeitswahrscheinlichkeit (wie Tests in der Realität). So kam das Gericht hier richtigerweise zu dem Ergebnis, dass auf dieser Grundlage keine Urteilsfindung stattfinden kann.[241]

5. Darstellung in den Urteilsgründen, § 267 StPO

Eine weitere Sicherung gegen eine willkürliche Urteilsfindung ist die Anforderung an das Gericht, das Ergebnis der Würdigung zu begründen und die als Grundlage festgestellten Tatsachen in den Urteilsgründen zu dokumentieren. § 267 StPO dient der Überprüfung des Urteils durch das Rechtsmittelgericht.[242] Dieses prüft dabei nicht die „Wahrhaftigkeit" der Aussagen, sondern die Rationalität und Stimmigkeit ihrer Wiedergabe und der Begründung ihrer Bewertung.[243] Dem Revisionsgericht muss i. d. S. jedenfalls eine Überprüfung nach den Maßstäben rationaler Argumentation möglich sein.[244] Der Umfang der Darstellung richtet sich auf der einen Seite nach der Bedeutung des Sachverständigengutachtens für die Sachentscheidung[245] und auf der anderen Seite danach, was das Revisionsgericht benötigt, um die Einhaltung der objektiven Grenzen der freien richterlichen Beweiswürdigung zu prüfen.[246] Mindestens erkennbar muss sein, worauf die tatsachengerichtliche Wertung beruht. Bei fraglicher wissenschaftlicher Zuverlässigkeit sachverständiger Methodik stellt die Rechtsprechung besonders hohe Anforderungen an die Darstellungen des Tatsachengerichts. So hat der BGH festgestellt, dass Tatgerichte bei den nicht standardisierbaren morphologischen Gutachten[247] sowie bei umstrittenen

---

241 AG Reutlingen, Beschl. v. 18.8.2022 – 5 Ds 52 Js 9104/22 jug.

242 Siehe zur Darstellungspflicht im Zusammenhang mit der revisionsgerichtlichen Überprüfung der Zuverlässigkeit von Software als Beweiswerkzeug bei *Mysegades*, Software als Beweiswerkzeug, S. 66 ff.

243 https://www.zeit.de/gesellschaft/zeitgeschehen/2015-09/strafprozessrecht-beweisueberzeugung/seite-3 [26.6.2023].

244 BGH NStZ-RR 2007, 86; *Sander*, StV 2000, 45 m. w. N.

245 BGH, Beschluss v. 25.04.2019 – 1 StR 427/18 = NStZ 2020, 294, zit. n. juris, Rn. 27 m. w. N.; BGH, Beschl. v. 24.01.2019 – 1 StR 564/18, Rn. 7; *Miebach*, NStZ 2020, 72 (78).

246 St. Rspr., siehe nur BGH, Beschl. v. 22.05.2019 – 1 StR 79/19 = NStZ-RR 2019, 253, Rn. 5 m. w. N.; *Miebach*, NStZ 2020, 72 (77 f.).

247 BGH, Urt. v. 27.10.1999 – 3 StR 241/99 = NStZ 2000, 106, Rn. 2 f., 6. Zu deren erheblichen Fehlerpotential siehe nur *Gabriel/Huckenbeck/Kürpiers*, NZV 2014, 346 ff. m. w. N.

„Jeansfaltengutachten“ in besonderem Maße die Grundlagen und Fehleranfälligkeiten darstellen müssten.[248] Bei besonders schwierigen Materien, die das Tatgericht im Einzelnen nicht verstehen kann, dürfe es sich auf die Darstellung beschränken, ob der Sachverständige selbst zuverlässig und erprobt ist.[249] Praktisch ist das eine bloße Reputationsprüfung,[250] die zu einer faktischen Richtigkeitsvermutung für das konkrete Gutachten auf Grundlage des Rufs des Sachverständigen führt. Überzeugen kann das nicht, denn die bloße Reputationsprüfung kann schon deswegen nie genügen, weil sie nichts über das konkrete Gutachten aussagt. Noch dazu besteht im Zusammenhang mit den IT-Sachverständigen die Schwierigkeit der Nachvollziehbarkeit der Reputation, aufgrund der uneinheitlichen und wenig verständlichen Qualifikationshinweisen (vgl. dazu Zweiter Teil, B. II. 2. c) aa)). Der Sachverständige muss zumindest ein Mindestmaß an intersubjektiver Vermittlung der Grundlagen des Gutachtens gegenüber dem Tatgericht leisten. Das Tatgericht wiederum muss dann zumindest auf der Metaebene prüfen, ob es das konkrete Gutachten für vertrauenswürdig hält, also insbesondere, ob der Sachverständige objektiv und präzise den konkreten Sachverhalt begutachtet hat.[251]

In Bezug auf die obenstehenden Ausführungen kann berichtet werden, dass sich in der Praxis Überlegungen der Tatrichter zur Zuverlässigkeit der IT-Sachverständigenaussage – und damit auch zu einer Richtigkeitswahrscheinlichkeit der angewendeten Methode bzw. zu den konkreten Randbedingungen – dem tatrichterlichen Urteil meist nicht entnehmen lassen. V. a. wenn es sich aber um (noch) nicht-standardisierte Methoden handelt, die das Gericht zu würdigen hat, muss die intersubjektive Diskutierbarkeit und Nachvollziehbarkeit in einer Tiefe geschehen, so dass auch eine revisionsrechtliche Überprüfbarkeit stattfinden kann. Nicht zuletzt um so künftig sicherstellen zu können, dass sich auch die höchstrichterliche Rechtsprechung mit den Standards der forensischen Informatik und den Erfahrungssätzen und angewendeten Methodiken auseinandersetzen (müssen).

---

248 BGH, Beschl. v. 15.04.1998 – 3 StR 129/98 = NStZ 1998, 528, Rn. 15 f.; BGH, Urt. v. 27.10.1999 – 3 StR 241/99 = NStZ 2000, 106, Rn. 7, 10; *Neuhaus/Artkämper*, Kriminaltechnik und Beweisführung im Strafverfahren, Rn. 433; *Mysegades*, Software als Beweiswerkzeug, S. 148.

249 Siehe nur BGH, Urt. v. 08.03.1955 – 5 StR 49/55 = BGHSt 7, 238 = NJW 1955, 840 (841); BGH, Urt. v. 18.12.1958 – 4 StR 399/58 = BGHSt 12, 311 = NJW 1959, 780 (781); *Deppenkemper*, Beweiswürdigung, S. 314; *Müller*, Der Sachverständige, Rn. 691a; SK-StPO/*Rogall*, Vor § 72 Rn. 119, 123 m. w. N. Vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 322.

250 SK-StPO/*Rogall*, Vor § 72 Rn. 119.

251 Vgl. auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 240 ff. m. w. N.; *Mysegades*, Software als Beweiswerkzeug, S. 149.

In diesem Zusammenhang führt Mysegades aus, dass, wenn die gerichtliche Entscheidung (auch) auf einer nicht nachvollziehbaren Datenverarbeitungs- und -analysemethode („opake Softwareauswertung“) beruht, das Tatgericht bei der Darstellung der Beweiswürdigung einbeziehen muss, warum das Gericht von der Richtigkeit der konkreten Softwareauswertung überzeugt ist. Hierfür kommen je nach Fallgestaltung verschiedene Indizien wie z. B. eine Zweitprüfung mit einer anderen Software oder stützende, externe Beobachtungen in der Wirklichkeit in Frage (vgl. auch A. III. 4. b) cc) (3)). Typischerweise wird das Tatgericht darlegen müssen, warum es eine Software für generell zuverlässig hält – etwa wegen einer unabhängigen Validierung – und ob dies Rückschlüsse auf die konkrete Auswertung ermöglicht. Das Tatgericht kann sich in seiner Darstellung auf die Indizien beschränken, die seine Überzeugung leiten, und muss keine komplette Historie der Softwareentwicklung darlegen. Mit Indizien, die gegen die Zuverlässigkeit sprechen, muss es sich dabei aber auch auseinandersetzen.[252]

IV. Zusammenfassung „Grundlagen tatrichterlicher Überzeugung“

Im Rahmen der freien Überzeugung von IT-Sachverständigengutachten nach § 261 StPO haben die Richter ihre subjektive Gewissheit den Verfahrensbeteiligten, den Rechtsmittelgerichten und der Öffentlichkeit objektiv zugänglich zu machen – mit den Regeln der praktischen Rationalität. Denn wie oben dargestellt, wird Wahrheit – anders als im Modell einer materiellen bzw. objektiven Wahrheit – nicht schlicht gefunden, sondern im Wege der Beweisaufnahme hergestellt. Dass Wahrheit ein Produkt dieses Herstellungsprozesses ist, bedeutet, dass für die richterliche Überzeugung „keine subjektive, sondern eine in der Untersuchung validierte Überzeugung“ genügt (B. I.). Um vor der Rechtsordnung Bestand zu haben, muss die Würdigung daher vollständig sein, die allgemeinen Regeln schlussfolgernden Denkens müssen befolgt werden (wobei insb. die Einhaltung der Standards der forensischen Informatik Berücksichtigung finden soll) und die objektiven Elemente zur Bestimmung der persönlichen Gewissheit müssen intersubjektiv diskutierbar und nachvollziehbar gemacht werden. Bei der Bestimmung der objektiven Stärke der tatrichterlichen Überzeugung muss die Zuverlässigkeit der Tatsachengrundlage erörtert werden. Das gilt, weil es sich bei den Erfahrungssätzen und Methodiken der forensischen Informatik um nicht „gesicherte Standards“ handelt. D. h. auf Ebene der IT-Sachverständigen müssen sowohl die Tatsachengrundlage (wie die Anknüpfungstatsachen, die Anfangswahrscheinlichkeiten, die Grundannahmen), als auch die daraus gezogenen Schlussfolgerungen und die

252 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 68.

darauf aufbauenden Hypothesen (in Bezug auf die Beantwortung der Beweisfragen) erörtert sowie die objektive Wahrscheinlichkeit der Richtigkeit dieser Hypothese bestimmt werden. Nur so kann die „Überzeugungskraft" der Ergebnisse der Sachverständigentätigkeit gewürdigt werden.

Dabei kommt es also auf Richtigkeitswahrscheinlichkeit der konkret angewendeten Erfahrungssätze und verwendeten Datenverarbeitungsmethoden an. Diese müssen zunächst genau benannt und entsprechend der jeweiligen Kategorie (deterministische, statistische und selbstlernende Methoden) durch die Verfahrensbeteiligten in eine Zuverlässigkeitsskala eingeordnet werden: Als gesicherte wissenschaftliche Erkenntnisse; als wissenschaftliche Erkenntnis mit wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit, oder als (einfache) Erfahrungssätze zur Richtigkeitsbeurteilung; keine Regeln zur Beurteilung der Richtigkeitswahrscheinlichkeit.[253] Je nachdem muss das Gericht den Sachverständigenaussagen folgen oder die Erkenntnisse sind für das Tatgericht eben nicht bindend, wobei es die Wahrscheinlichkeitsaussage in seine Beweiswürdigung einbeziehen und die Richtigkeit der Aussage im jeweiligen Einzelfall anhand weiterer Indizien bestätigen oder widerlegen muss. In Fällen von Blackbox-Tools kann es auch sein, dass das Ergebnis des Datenbearbeitungs- oder -analysevorgangs keinen Beweiswert hat und nicht in die Beweiswürdigung einbezogen werden darf.

Dabei zu berücksichtigen ist stets der gern überschätzte Aussagegehalt eines digitalen Beweismittels.[254]

B. Die Würdigung von IT-Sachverständigenaussagen

Zu der Herausforderung der Bestimmung des Beweiswerts von IT-Sachverständigengutachten (regelmäßig als Indizientatsachen) kommt hinzu, dass die besondere Schwierigkeit der Beweiswürdigung beim Sachverständigenbeweis darin besteht, dass das Vorhandensein der Sachverständigen die Kette von Indizien noch einmal verlängert, die vom durch die Richterinnen wahrnehmbaren Material zum Beweisthema führt. So ermöglicht bzw. erleichtert der Sachverständige zwar erst die Beweiswürdigung, da ein Indiz in der Kette nur vom Sachverständigen geschaffen wird oder nur er die erforderliche Sachkunde besitzt, um die Bedeutung des vorhandenen Indizes für das Beweisthema zu erfassen. Allerdings kommen auch die mit einem persönlichen

253 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, S. 675.

254 Eine ausgedruckte WhatsApp-Nachricht, die im Urkundenbeweis verlesen wird, besagt noch nichts über den Urheber. Der Mitschnitt einer TKÜ besagt für sich genommen noch nicht, welche Personen miteinander gesprochen haben. Auch das Auffinden eines USB-Sticks mit kinderpornografischen Bilddateien in einer Wohnung belegt noch nicht, dass es der Wohnungsinhaber war, der diese Bilder vorsätzlich besitzt.

Beweismittel verbundenen Probleme hinzu, die die Richter berücksichtigen müssen. Es haben also zwei hintereinander geschaltete Beweiswürdigungen zu erfolgen: 1) Das dem Sachverständigen zur Verfügung stehende Beweismaterial, wobei die Beurteilung des Sachverständigen zur Hilfe kommt und 2) ob die Person des Sachverständigen vertrauenswürdig ist.[255]

Es empfiehlt sich, entsprechend den drei Strukturteilen von Argumentationen[256] folgende Fragen im Rahmen der Würdigung der Sachverständigenaussage zu beantworten:[257]

1) Welche Tatsachenbehauptung lässt sich dem Beweisthema entnehmen?

2) Welche Anknüpfungstatsachen (Befund- und Zusatztatsachen) wurden zugrunde gelegt, und durften sie zugrunde gelegt werden?

3) Mit welchen Werkzeugen wurden die selbst zu ermittelnden Befund- und Zusatztatsachen generiert? Wie zuverlässig sind die Werkzeuge und Ergebnisse?

4) In welchen Schritten gelangt das Gutachten zur Stellungnahme zum Beweisthema?

4a) Welche Folgerungen sind nötig, um in Zwischenschritten von den Anknüpfungstatsachen zur Tatsachenbehauptung des Beweisthemas bzw. dessen Verneinung zu gelangen?

4b) Welche Erfahrungssätze stützen diese Folgerungen, und sind sie genügend bestätigt, um die Folgerungen in den Zwischenschritten und in der abschließenden Stellungnahme zum Beweisthema zu rechtfertigen? Wie zuverlässig sind sie?

Das IT-Sachverständigengutachten soll schließlich auf seine Aussagemöglichkeit, Aussagekraft und Genauigkeit gewürdigt werden. Dabei ist die Darlegung der wissenschaftlichen Methodik (einschließlich ihrer Kritik) erforderlich, womit wieder die oben stehenden Ausführungen relevant werden.

Angefangen mit der Feststellung, ob das Gutachten von einem unbefangenen Sachverständigen in zuverlässiger und vertrauenswürdiger Weise erstattet ist (siehe im 2. Teil, B. II. 2. c) dd) sowie B. V. 2. c) und B. VI.)[258], weiter mit der Überprüfung des vom Sachverständigen beschrittenen Weges (etwa seiner Methodik, der angewandten Mittel und Erfahrungssätze, der Art der Tatsachengewinnung einschließlich der dabei vorgenommenen Beurteilungen)[259],

---

255 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 169 f.

256 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 104 ff.

257 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 393.

258 Vgl. auch *Mayer*, in: FS-Mezger, S. 475; *Mösl*, DRiZ 1970, 112.

259 *Peters*, Strafprozess, S. 364.

bis hin zur kritischen Untersuchung aller Einzelheiten der Ausführungen des Gutachtens hat der Richter sich eine selbständige Meinung über die Beantwortung der Beweisfrage zu bilden und entsprechend zu verwerten.[260] Daher muss der Richter, wenn er sich der sachverständigen Meinung anschließt, im Urteil kenntlich machen, dass das aufgrund eigener Überzeugung geschehen ist.[261] Um zu einem Schuldspruch zu kommen, muss er voll überzeugt sein (vgl. A. I. und II.). Dazu kann er gelangen, auch wenn das Gutachten diesen Grad an Überzeugung eigentlich nicht rechtfertigen würde. Denn der Richter führt die Prüfung des Sachverständigengutachtens unter Auswertung der gesamten Beweisaufnahme durch, verwertet also auch Umstände, die der Beurteilung des Sachverständigen durch die Begrenzung des Beweisthemas (siehe Formulierung des Beweisthemas im 2. Teil, B. II. 3. c) und zu den Grenzen der Sachverständigentätigkeit im 2. Teil B. VI.) entzogen sind.[262]

Der Richter kann auch entgegen den Sachverständigenausführungen, der aufgrund ihm bekannter ähnlicher Fälle und den dabei bestätigten Erfahrungssätzen Folgerungen i. S. der Annahme eines Kausalzusammenhangs gezogen hat, aus den besonderen Umständen des Einzelfalls Zweifel an dieser Annahme haben und eine andere Schlussfolgerung ziehen.[263] Unter Zugrundelegung, dass die Tatsachenfeststellung prinzipiell wissenschaftliche Forschungstätigkeit ist,[264] kann er für das Abweichen an den sachverständigen Ausführungen andere eigene wissenschaftliche Gründe setzen.[265] Diese Gründe muss

---

260 Vgl. BGHSt 8, 113 = LM StPO § 244 Abs. 3 Nr. 13 mit Anm. von Kohlhaas = NJW 1955, 1642: Der Tatrichter sei „zu einem eigenen Urteil auch in schwierigen Fachfragen verpflichtet", er habe „die Entscheidung auch über diese Frage selbst zu erarbeiten, ihre Begründung selbst zu durchdenken", er dürfe „sich dabei von Sachverständigen nur helfen lassen". Im Anschluss daran formulieren *Gschwind/Peterson/Rautenberg*, Die Beurteilung psychiatrischer Gutachten im Strafprozess, S. 15: „Im Idealfall ist der Richter damit also der Zwerg auf dem Kopf des Riesen, der mehr sieht als dieser"; *Kühne*, Strafprozesslehre, Rn. 517 mit Fn. 109 formuliert in Bezug auf die Entscheidung des BGH, dass dieser in eine sachlich unvertretbare Schwärmerei über ein nicht existentes Richterbild geraten sei.

261 BGHSt 12, 311 = LM StPO § 267 Abs. 1 Nr. 22 mit Anm. von Krumme = NJW 1959, 780 = MDR 1959, 412 (im Anschluss an BGHSt 7, 238 = JZ 1955, 456; 8, 113, 118 = LM StPO § 244 Abs. 3 Nr. 13 mit Anm. von Kohlhaas = NJW 1955, 1642); BGH StV 1982, 210; OLG Celle VRS 25, 55 = MDR 1963, 334; OLG Hamm NJW 1963, 405; *Albrecht*, NStZ 1983, 486 (491); Löwe/Rosenberg/*Gollwitzer*, § 261 Rn. 99; *Jessnitzer*, StV 1982, 180 f.

262 Vgl. auch *Peters*, Psychologischer Sachverständiger, S. 781; *Marmann*, GA 1953, 144 f.

263 Vgl. dazu auch *Marmann*, GA 1953; G. Walter, S. 281.

264 Vgl. dazu im 2. Teil, B. I. 1.; sowie *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 25 f.

265 Vgl. auch *Bockelmann*, GA 1955, 329, der dem Richter in diesen Fällen die Rolle eines Lernenden, der zum Kritiker seines Lehrers werden kann, zuspricht; *Blau*,

er aber erkennbar machen.[266] Dabei droht dem Tatrichter stets, dass sein Urteil aufgrund „angemaßter Eigensachkunde“ aufgehoben werden kann, wenn er eine vom Gutachten abweichende Überzeugung gewonnen hat. Auch besteht ein Revisionsgrund bei „kritikloser Übernahme des Gutachtens“, weil er in die wissenschaftliche Begründung des Gutachtens nach Meinung des Revisionsgerichts nicht genügend eingedrungen ist.[267]

I. Die Würdigung trotz mangelnder Sachkunde des Richters

Auch aus anderen forensischen Gebieten kennt man das Problem, dass der Richter eben hinsichtlich der Beweisfrage, die er nun zu würdigen hat, wenig Wissen hat, weshalb er überhaupt das Gutachten in Auftrag gegeben hat. Damit einher geht auch der gefühlte Kontrollverlust. Problematisch sind die Fälle, in denen dem Richter mangels fehlenden Fachwissens die Überprüfbarkeit der Richtigkeit des Gutachtens nur schwer möglich ist.[268] Zumal es sich dabei um sehr komplexe und hoch spezialisierte Wissenschaften bzw. Sachgebiete handeln kann, verbunden mit einer für Laien schwer verständlichen

---

ZStW 78 (1966), S. 153 ff.; Mehr zur Befugnis des Richters, sich erlernbare fachwissenschaftliche Kenntnisse anzueignen und sogleich zu benutzen vgl. auch BGHSt 12, 18 (19 f.) = NJW 1958, 1596 = MDR 1958, 938 = JZ 1959, 130 mit Anm. von Eb. Schmidt; BGH MDR 1978, 42; Alsberg/Nüse/Meyer-*Dallmeyer*, Der Beweisantrag im Strafprozess, S. 695, S. 698; *Falck*, JR 1955, 286; *Hepner*, Richter und Sachverständiger, S. 41, 50, 109; *Jessnitzer*, Handbuch, S. 116; *Nikisch*, Zivilprozessrecht, S. 356; *Schäfer*, Die Praxis des Strafverfahrens, S. 309; KK/*Herdegen*, § 244 (Aufl.) Rn. 30 ist dagegen zurückhaltender und sieht eine Abweichung nur in Bezug für „gesicherte, einfach strukturierte und bei Anwendung im Einzelfall leicht zu handhabende Erfahrungssätze“ zulässig.

266 *Dilcher*, Der Beweis durch Sachverständige, S. 40; Löwe/Rosenberg/*Gollwitzer*, § 261 Rn. 66, 98; *Mösl*, DRiZ 1970, 113; *Sarstedt/Hamm*, Revision, Rn. 404. Beispiel einer solchen begründeten Abweichung BGHSt 21, 62 = LM StPO § 244 Abs. 2 Nr. 43 mit Anm. Kohlhaas = MDR 1966, 699; *Henke*, NStZ 2023, 13 (17).

267 Beispiele: *Dallinger*, MDR 1972, 570; BGH GA 1977, 275; *Holtz*, MDR 1977, 284; 1980, 274; OLG Hamm NJW 1967, 691; VRS 41, 276; OLG Köln VRS 47, 281; OLG Koblenz DAR 1974, 134; VRS 51, 116; OLG Stuttgart Justiz 1971, 312; kritisch dazu KK/*Herdegen*, § 244 Rn. 30; *Roxin*, Strafverfahrensrecht, S. 257; OLG Hamm NJW 1978, 1210 = MDR 1978, 593: der Richter könne sich außerhalb der Hauptverhandlung von einem Sachverständigen beraten lassen; jedenfalls nicht einen Sicherheitsabschlag von der Sachverständigenausführung (Kemptener-Bitcoin-Fall).

268 Zu diesem Problem vgl. BGHSt 7, 238, 239; BGH StV 1989, 331, 332 mit Anm. Wasserburg; SK-StPO/*Rogall*, Vor § 72 Rn. 119; *Müller*, Der Sachverständige im gerichtlichen Verfahren, Rn. 691 f.; *Mayer*, in: FS-Mezger, S. 455, 476; *Detter*, NStZ 1998, 60; *Alsberg/Nüse/Meyer*, Der Beweisantrag im Strafprozess, S. 727; *Plewig*, Funktion und Rolle des Sachverständigen, S. 76; kritisch dazu *Erb*, ZStW 121 (2009), 882 ff., 884, 887 ff.

Fachsprache, die es den Richtern nahezu unmöglich macht, die Gutachtenerstattung nachzuvollziehen.[269]

Die Praxis zeigt aber, dass das Problem der Gefahr der Einschränkung der Freiheit in der Entscheidungsfindung durch den Sachverständigenbeweis regelmäßig nicht in einem Spannungsverhältnis zu § 261 StPO begründet liegt, sondern sich die Gerichte nicht hinreichend mit den Gutachten auseinandersetzen.[270] Ein Mangel an Zeit ist als Grund für eine fehlende Auseinandersetzung mit dem Gutachten nicht hinnehmbar. Einer der bekanntesten Fälle in diesem Zusammenhang ist wohl der Fall „Mollath".[271] Das Bundesverfassungsgericht hob die Vorinstanzen auf und verwies den Fall zur erneuten Entscheidung u. a. deshalb zurück, weil sich die Gerichte mit den Gutachten nicht hinreichend beschäftigt hatten.[272] Dem Mangel an Wissen kann durch explizites Nachfragen und Nachvollziehen des Gutachtens entgegengewirkt werden.[273] Denn es ist Aufgabe des Sachverständigen, das Gericht auf ein so gesichertes „Wissensfundament" zu stellen, dass es ein eigenständiges Urteil bilden kann. Die Beurteilung des Beweisthemas ist jedoch ureigenste Aufgabe des Gerichts.[274] Daher dürfen trotz der großen Arbeitsbelastung der Gerichte Zeit und Mühen nicht gescheut werden.[275]

Auch hier wird noch einmal mehr deutlich, wie wichtig die Aneignung von elementaren Grundlagen im Bereich der forensischen Informatik ist, um den Sachverständigen wissenschaftstheoretisch einordnen und seine Ausführungen entsprechend abgestuft bewerten zu können.[276]

So ist eine „Kompetenzüberschreitung" oder „Entscheidungsanmaßung" des Sachverständigen immer nur über eine mangelhafte Erfüllung der Lei-

---

269 Vgl. auch *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 32 f.; *Mysegades*, Software als Beweiswerkzeug, S. 122.

270 Vgl. *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 32 f.; *Plewig*, Funktion und Rolle des Sachverständigen, S. 29 ff., der von „Kompetenzunterschreitung" spricht.

271 Vgl. *Hauer*, ZRP 2013, 209 f.

272 BVerfG, Beschl. v. 26.8.2013, Az. 2 BvR 371/12.

273 So auch bei *Stinshoff*, Operative Fallanalyse, S. 169.

274 *Erb*, ZStW 121 (2009), 882, 884.

275 So fordert auch SK-StPO/*Rogall*, Vor § 72 Rn. 134, dass sich Richter eine „gesunde Skepsis und ein gesundes Misstrauen gegenüber Gutachtenleistungen bewahren sollten und *Mysegades*, Software als Beweiswerkzeug, S. 123 m. w. N. führt als Gegenbeispiel die Rechtsgeschichte von „junk science" in den USA an mit zahlreichen Gerichtsentscheidungen, die auf „wissenschaftlichen" Methoden beruhten, die später als unhaltbar entlarvt wurden.

276 So auch in *Walter*, Sachverständigenbeweis, S. 120.

tungsaufgabe i. S. d. § 78 StPO oder auch „Kompetenzunterschreitung“ i. S. d. § 261 StPO des Richters möglich.[277]

II. Die Würdigung des untersuchten Sachverhalts des Sachverständigen (1. Schritt)

Hilfreich bei der Würdigung ist, wenn der Sachverständige seine vorgebildete Überzeugung (zur Beantwortung der im Auftrag genannten Frage) in einer ähnlichen Struktur aufbaut (und formuliert) wie die der richterlichen Überzeugung, damit sie von der Gerichtsperson entsprechend verstanden und gewürdigt werden kann („syllogistische Struktur“, siehe oben im 3. Teil, B. III. 4.).[278]

Der Sachverständige erlangt im Verlauf seiner Tätigkeit im Rahmen des Auftrags eine (u. U. große) Menge an Informationen, v. a. im Bereich der forensischen Informatik (Stichwort „big data“), die von unterschiedlichem Gewicht bzw. Wert für die Beantwortung der Auftragsfrage sein können (vgl. dazu auch im 2. Teil, B. VII. 1.). Im Sinne eines vollständigen Inkenntnissetzens des Gerichts wurde bereits erörtert, dass – insb. bei IT-Sachverständigengutachten, die Tatsachengrundlage (wie die Anknüpfungs-, Befund- und Hilfstatsachen, die angewendeten Werkzeuge und Erfahrungssätze, deren Richtigkeitswahrscheinlichkeit und Unsicherheiten sowie die Anfangswahrscheinlichkeiten und Grundannahmen), als auch die daraus gezogenen Schlussfolgerungen und die darauf aufbauenden Hypothesen (in Bezug auf die Beantwortung der Beweisfragen) sowie deren Wahrscheinlichkeit im Gutachten bzw. in den dazugehörigen Arbeitsunterlagen angegeben und offengelegt werden müssen. Das sind alles Faktoren, die den Wert des Ergebnisses bestimmen (siehe hierzu A. III. 4. b)).

Bei der Differenzierung können zudem verschiedene Besonderheiten auftreten, je nachdem welchem der drei verschiedenen Aussagekategorien das Beweisthema angehört und ob es sich auf sog. innere oder äußere Tatsachen bezieht.[279] Äußere Tatsachen sind dadurch charakterisiert, dass sie grds. der Wahrnehmung zugänglich sind. Innere Tatsachen[280] hingegen sind psychische Vorgänge und Zustände anderer Menschen (das Innehaben von Gefühlen, das

277 Vgl. *Walter*, Sachverständigenbeweis, S. 149 m. w. N.

278 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 170.

279 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 171.

280 Hier kann noch nach eigen- und fremdpsychischen Tatsachen differenziert werden; vgl. dazu *Mezger*, AcP 117 (1918), Beilageheft, S. 1 (S. 35 ff.). Allerdings hauptsächlich relevant für den psychiatrischen bzw. psychologischen Sachverständigen und wohl eher nicht für den IT-Sachverständigenbeweis.

Akzeptieren oder Präferieren), die für Dritte nicht unmittelbar wahrnehmbar sind.[281]

1. Erste Kategorie (Erfahrungssätze)

Wie oben ausgeführt (siehe im 2. Teil, B. II. 3. d) aa)), sind die mitgeteilten Erfahrungssätze (bzw. deren Anwendung) des Sachverständigen Aussagen über das Bestehen eines Zusammenhangs (sog. Schlussregeln) zwischen Ereignistypen. Der Erfahrungssatz stellt die Verknüpfung zwischen den Ereignistypen als Konditionalsatz dar. Als Hintergrundannahme stützt der Erfahrungssatz die Schlussregel, die den Richter nach Rationalisierungsregeln befugt, mit Hilfe der ihm zur Verfügung stehenden Daten eine für die Sachverhaltsfeststellung (die prozessuale Tat) relevante Schlussfolgerung zu ziehen.

Der Wert des Erfahrungssatzes in einer bestimmten Argumentation ist davon abhängig, wie genau die darin genannten Ereignistypen in den Daten des Falls wiedergefunden werden können, denn die Erfahrungssätze umschreiben nur „vertypte" Situationen (siehe dazu bei A. III. 4. zur Qualität der Tatsachenbasis). Daher zählt es zu den wichtigsten Aufgaben des Sachverständigen, über die verknüpften Ereignistypen möglichst genau zu berichten.[282] Um eine Anwendung der Erfahrungssätze zu ermöglichen, ist es auch notwendig, auf häufig auftretende Abweichungen von den vorausgesetzten Erfahrungssätzen hinzuweisen. Diesbezüglich sollen noch einmal die Ausführungen unter A. III. 4. b) cc) (2) hervorgehoben werden.

Daneben muss der Sachverständige auch die Art der Verknüpfung herausarbeiten, um den Gerichtspersonen verständlich zu machen, inwieweit das Auftreten eines Ereignistyps das eines anderen bedingt („Bedingungszusammenhang"). Wenn der im Erfahrungssatz enthaltene Bedingungszusammenhang zwischen den Ereignistypen (Ursache und Erfolg) nur „schwach positive Relevanz" besitzt, kommt der Sachverständige zum Einsatz. In diesem Fall hat er den Erfahrungssatz selbst anzuwenden und Vorschläge zur Schlussfolgerung in der zu beurteilenden Situation zu unterbreiten.

a) Ungeprüfte Übernahme der Bedingungsverhältnisse und Wahrscheinlichkeitsrelationen?

In diesen Konstellationen ergibt sich die Frage, ob die Gerichte kausale Bedingungsverhältnisse und Wahrscheinlichkeitsrelationen aus den entsprechenden Wissenschaftszweigen ungeprüft übernehmen müssen bzw. dürfen,

---

281 *Mezger*, AcP 117 (1918), Beilageheft, S. 1 (35 f.).

282 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 175.

so wie der Sachverständige sie mitteilt. Das bietet sich nicht nur aus Zweckmäßigkeitsüberlegungen (und dem Beschleunigungsgrundsatz folgend) an, sondern es erscheint in einer immer komplexer und spezialisierter werdenden Welt der Experte in diesem Gebiet vertrauenswürdiger als der nicht in dieser Wissenschaft ausgebildete Richter.[283]

Wie bereits dargestellt darf das Tatgericht nach § 261 StPO ein (mündlich) erstattetes Sachverständigengutachten jedoch nicht ohne eigene Stellungnahme in das Urteil einfließen lassen. Auch bei kausalen Bedingungsverhältnissen und Wahrscheinlichkeitsrelationen ist es nicht selbstverständlich, dass das Gericht die Mitteilung des Erfahrungssatzes ungeprüft übernehmen kann. Denn aus den Ausführungen oben wird deutlich, dass es sich bei den Sachverständigenaussagen der ersten Kategorie nicht nur um gesicherte Erfahrungssätze handelt, sondern v. a. Erfahrungssätze mit „schwach positiver Relevanz" mitgeteilt werden, das gilt v. a. auch für die forensische Informatik (vgl. A. III. 4. b) cc) (2)).

So ist in einem ersten Schritt festzustellen, um welchen konkreten Erfahrungssatz es sich handelt, auf dem die Hintergrundannahme oder Schlussfolgerung fußt und welche Art Tatsache (Haupttatsache oder Indiz) damit bewiesen werden soll. In einem zweiten Schritt kann mithilfe der Einordnung des entsprechenden mitgeteilten Erfahrungssatzes in die Zuverlässigkeitsskala (oben) ermittelt werden, inwieweit die freie richterliche Beweiswürdigung ggf. einschränkt (gesicherte wissenschaftliche Erkenntnis oder standardisiertes Verfahren) bzw. auszuweiten ist (weitere Indizien sammeln, die die Tatsachen stützen). Im dritten Schritt ist die Antwort in der Frage des Selbstvertrauens als ein Akt „subjektiven Fürwahrhaltens" zu finden.[284]

Die Herausdifferenzierung einzelner wissenschaftlicher Erfahrungssätze stellt einen Prozess fortschreitender Arbeitsteilung dar. Bis in die Sprache hinein erstreckt sich dieser Vorgang.[285] Es ist zweckmäßig, sich die vorhandenen Spezialisierungen zunutze zu machen und insoweit mehr den Fachleuten zu vertrauen als der eigenen Beurteilung. Allerdings bedeutet Zweckmäßigkeit noch keinen zwingenden Grund, sich auf die Ansicht anderer zu verlassen. Immerhin lebt der wissenschaftliche Fortschritt davon, dass Menschen anerkannte Erfahrungssätze in Zweifel ziehen und so zu neuen Erkenntnissen vorstoßen. Bei fehlender eigener Sachkunde muss den Richtern ein Vertrauen (bis zu einem gewissen Grad, jedenfalls nicht blind) auf Erfahrungssätze wohl

283 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 173.

284 Dazu auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 179.

285 So werden die Bezeichnungen für Fachausdrücke z. B. Medizinern und Physikern überlassen; vgl. zu dieser „Linguistic Division of Labour" auch *Lehrer*, Self-Trust, S. 144; *Putnam*, Representation and Reality, S. 22 ff.

zugestanden werden.[286] Auch die Rspr. deutet das an, wenn sie verlangt, dass der Tatrichter gesicherte wissenschaftliche Erkenntnisse hinnehmen muss, auch wenn er die Richtigkeit der Ergebnisse selbst nicht nachprüfen kann (siehe dazu in A. III. 2.). V. a. mithilfe der oben beschriebenen Fragentrias kann die Sachverständigenargumentation in Bezug auf die Beweiskraft von Indizientatsachen in zweifacher Hinsicht verbessern und sie intersubjektiv diskutierbar machen: Dissens wird transparent und es müssen Randbedingungen beachtet werden.[287]

b) Tiefenstruktur des Erfahrungssatzes

Weiter ergibt sich die Frage, wie detailliert die Tiefenstruktur der Erklärung der Kausalbeziehung vom Sachverständigen offengelegt werden muss, um diese entsprechend zu würdigen.[288] Nach der Rspr. soll bspw. für den Nachweis der Ursächlichkeit nicht erforderlich sein, dass der naturwissenschaftliche Wirkungsmechanismus im Einzelnen bekannt ist. Die Literatur kritisierte das jedoch und verlangt vielmehr, dass das Kausalgesetz, welches im Einzelfall die Beziehung zwischen Ursache und Erfolg erklärt, namhaft gemacht werden muss.[289] Die Generalisierungen der Oberprämisse einer Kausalerklärung darf nicht „flach" sein, d. h. nicht nur das Vokabular der Unterprämisse und des Explanandums/Ereignistyps wiederholen.[290] Wenn aber Tiefenstruktur für das Vokabular bei Formulierungen eines Kausalgesetzes gefordert wird, dann erhebt sich sofort die Frage, wie detailliert der Spezifizierungsvorgang fortgesetzt werden muss. Mackie[291] hat eine Formulierung wissenschaftlicher Generalisierungen, die ein Maximum an erklärendem Gehalt aufweisen, als minimal vollständige Kausalerklärung bezeichnet. Eine solche minimal vollständige Kausalerklärung könnte jedoch kaum je in den Naturwissenschaften und erst recht nicht vor Gericht erreicht werden. Es geht also darum, einen „Mittelweg" zwischen dem Gebrauch vollständig erklärender Termini und einer groben alltagssprachlichen Umschreibung der relevanten Faktoren zu finden.[292]

---

286 *Toepel* spricht noch von einer Pflicht zu Vertrauen, vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 173 ff.

287 Vgl. vertiefend dazu *Bender/Nack/Treuer*, Tatsachenfeststellung vor Gericht, Rn. 581 f.

288 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 174, S. 186 ff. m. w. N.

289 Dieses Phänomen wurde bezüglich des Kausalitätserfordernisses in den sog. strafrechtlichen Produkthaftungsfällen diskutiert; siehe LG Aachen JZ 1971, 507 („Contergan"); BGHSt 37, 106 („Lederspray"); 41, 206 („Holzschutzmittel").

290 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 188 f. m. w. N.

291 *Macki*, Truth, Probability and Paradox, S. 261 f.

292 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 174, 186 ff.

2. Zweite Kategorie (Befundbewertung)

Wird der Sachverständige damit beauftragt, im Einzelfall Schlussfolgerungen zu ziehen mit Hilfe der Anwendung seines Erfahrungswissens, ergeben sich v. a. zwei Fehlerquellen, auf die das Tatgericht besonders zu achten hat: 1) Der Sachverständige könnte den Erfahrungssatz falsch eingeschätzt haben (drei denkbare Möglichkeiten, siehe dazu sogleich) oder 2) falsche Daten zugrunde gelegt haben (siehe dazu dann unter II. 3.).[293]

a) Falsche Einschätzungen des Erfahrungssatzes

Der Erfahrungssatz wird falsch eingeschätzt, wenn er einerseits nicht erlaubt, von den zugrunde gelegten Daten auf die gezogene Schlussfolgerung überzugehen (fehlender Anknüpfungspunkt). Das kann darauf zurückzuführen sein, dass der Erfahrungssatz nicht an den zugrunde gelegten Daten anknüpft, sondern an anderen, die den zugrunde gelegten Daten ähnlich sind.[294] Andererseits ist es auch möglich, dass der Erfahrungssatz zwar an den zugrunde gelegten Daten anknüpft, dass er jedoch noch eine ganz andere Schlussfolgerung als die vom Sachverständigen gezogene zulässt. Dieser Fehler tritt bei Unkenntnis des Inhalts des Erfahrungssatzes auf.[295] Letztlich ist es auch denkbar, dass der Erfahrungssatz zwar eine Verbindung zwischen den Daten und der Schlussfolgerung herstellt, allerdings das Gewicht unter- oder überschätzt wird, welches der Erfahrungssatz der Relation zwischen Daten und Schlussfolgerung beimisst. Dieser Fehler tritt insb. im Zusammenhang mit statistischen Erfahrungssätzen auf, wenn es der Sachverständige unterlässt, durch eine entsprechende Quantifizierung zu kennzeichnen, dass die Schlussfolgerung nur mehr oder minder wahrscheinlich[296] ist (vgl. hierzu A. III. 4. b) cc) (1) und im Ditten Teil, B. III. 3. a) und d)). Der Erfahrungssatz könnte vage sein dahingehend, dass er statt einer bestimmten Schlussfolgerung eine Auswahl mehrerer Möglichkeiten zulässt. Wenn hier die Möglichkeiten vom Sachverständigen nicht aufgezeigt würden, ergäbe sich ein unvollständiges und damit verfälschendes Bild.[297]

---

293 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 212.

294 So kann bspw. die Verfärbung der Haut bei bestimmten Giften geringfügig differieren. Wenn der Erfahrungssatz nur besagt, dass bei Beibringung eines Giftes A sich die Haut mit einer bestimmten Blauschattierung verfärbt, während bei Beibringung des Giftes B eine geringfügig andere Blauschattierung auftritt, so liegt die Gefahr eines fehlerhaften Schlusses auf das Gift A nahe, falls eine in Wirklichkeit durch B hervorgerufene Blauschattierung vorliegt.

295 Wenn z. B. ein medizinischer Sachverständiger aus dem korrekt genannten Sektionsbefund auf einen falschen Todeszeitpunkt schließt.

296 Oder „seltener" ist, wenn er sich vorsichtig ausdrücken möchte.

Die mit dem Ziehen von Schlussfolgerungen verbundenen Schwierigkeiten werden also erst bei Offenlegung der Argumentationsstruktur deutlich, aus der das Ergebnis abgeleitet wird.[298] Das Gericht darf daher nicht kritiklos die Folgerung des Sachverständigen übernehmen, sondern muss sie nachvollziehen und durch die Darstellung im Urteil (§ 267 StPO) den übrigen Beteiligten ebenfalls dieses Nachvollziehen ermöglichen.[299] Das Akzeptieren der Tatsachenbehauptung gründet sich nicht unmittelbar auf das Vertrauen in die Person des Sachverständigen, sondern darauf, wie die Schlussfolgerungen aus dem Zusammenspiel von Daten und Erfahrungssätzen hervorgehen (Rationalitätsregeln, siehe bei A. III.). Der Sachverständige soll durch sein größeres Wissen und seine größere Erfahrung bei der Anwendung des Wissens dem Gericht ermöglichen, eine überzeugend begründete Schlussfolgerung darzustellen. Aber das Ergebnis muss unabhängig von seiner Person überzeugen.[300]

Zeigt der Sachverständige einen Weg, wie die Schlussfolgerung bewiesen werden kann, so gibt er ein Beispiel für eine Überzeugungsbildung in der Weise, dass sie der Richter in seine Überzeugung aufzunehmen in der Lage ist. Die vom Sachverständigen vorgebildete Überzeugung sollte daher eine parallele Struktur zur nachfolgenden richterlichen Überzeugung besitzen (vgl. die Ausführungen im 2. Teil, B. II. 3. c) aa)). So besteht bei der vom Sachverständigen angebotenen Lösung, genau wie bei der Überzeugungsbildung des Tatgerichts, die Notwendigkeit, rivalisierende Hypothesen abzuwägen (i. S. d. „gerechtfertigten Akzeptierens“).

---

297 Ergebnisse von DNA-Analysen werden oft überschätzt, vgl. bspw. die Fälle von BGHSt 38, 320 (323 f.) und BGH NStZ 1994, 554. Im erstgenannten Fall errechnete der Sachverständige eine Belastungswahrscheinlichkeit von 99,986 %. Der BGH betont, dass die DNA-Analyse nur ein Indiz darstellt. Genau genommen handelt es sich nicht unbedingt um ein Indiz für die Täterschaft, sondern um ein Indiz für die Anwesenheit des Beschuldigten am Tatort. Auf die Täterschaft kann erst im Zusammenhang mit einer Gesamtwürdigung aller Umstände geschlossen werden. Insb. der genaue Fundort kann eine Rolle spielen. Spermaspuren am Opfer ergeben etwa eine hohe Signifikanz für die Täterschaft bei einem Sexualdelikt erst dann, wenn ausgeschlossen ist, dass sich das Opfer mit dem Täter freiwillig eingelassen hat oder dass die Spuren nicht zu einem früheren Zeitpunkt verursacht wurden, zu dem das Opfer noch einem Geschlechtsverkehr zugestimmt hatte. Vgl. dazu vertiefend auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 183 f., 212 f.

298 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 211.

299 Das verlangt auch die st. Rspr., vgl. BGHSt 7, 238 (240); 12, 311 (314); BGH NJW 1982, 1882 m. Anm. Peters, JR 1983, 164; BGH NStZ 1982, 342; BGH bei Pfeiffer/Miebach NStZ 1984, 17; BGH VRS 31, 107; OLG Köln NJW 1982, 249; OLG Bremen VRS 48, 272; OLG Celle VRS 42, 41; OLG Düsseldorf VRS 78, 125; 64, 208; OLG Hamm VRS 40, 197; OLG Koblenz VRS 51, 115; umfangreichere Nachweise aus der unveröffentlichten Rspr. des BGH bei KK/*Engelhardt*, § 261, StPO Rdnr. 32.

300 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 211 f.

An dieser Stelle wird v. a. die Gewichtung von Hypothesen und deren Irrtumswahrscheinlichkeiten wichtig.

In Bezug auf diesen Vorgang lässt sich eine stark persönliche Komponente nicht eliminieren (irreduzible Vagheiten). Beim Richter, als demjenigen, der eine vom Gesetz vorgesehene Autoritätsposition innehat, ist die Ausnutzung des dadurch gegebenen Spielraums tolerierbar (siehe oben bei A. II. zur unvermeidbaren Rest-Subjektivität). Enthalten jedoch die Rationalitätsregeln selbst diese Vagheiten, ist es Aufgabe des Sachverständigen, das Gericht darüber zu informieren, wo solche unbestimmten Bereiche vorhanden sind.[301] Das Gericht ist nach der Konzeption des Gesetzes dafür zuständig, diese Vagheiten durch konstitutive Entscheidung aufzulösen (§ 1 GVG und v. a. aus § 261 StPO).[302] In der Praxis ist es jedoch nicht üblich, dass Sachverständige von sich aus über solche Vagheiten informieren.[303] Deshalb muss das Gericht aktiv danach fragen, ob und wo der Sachverständige Gewichtungen vorgenommen hat, die von seiner persönlichen Einschätzung beeinflusst sein könnten.[304]

Auch ist es an dieser Stelle noch einmal von Bedeutung auf den Sprachgebrauch des Sachverständigen bei der Darstellung bzw. Präsentation des Beweisthemas einzugehen: Der Sachverständige beschreibt die Erfahrungssätze und artikuliert insoweit die kognitiven Erwartungen der wissenschaftlichen Gemeinschaft. Er bewertet den Sachverhalt aufgrund der wissenschaftlichen Erfahrungssätze und bedient sich insoweit des evaluativen oder kritischen Sprachgebrauchs. Aber anders als dem Gericht steht ihm niemals der konstitutive Sprachgebrauch zu, durch den ein Sachverhalt bindend für andere Personen festgestellt wird. Der Sachverständige soll insoweit nur evaluativ mögliche Überzeugungen zeigen. Daraus wählt dann das Gericht konstitutiv seine Überzeugung aus.[305] In der Praxis wird der Sachverständige jedoch dazu tendieren, sein Ergebnis als zwingend darzustellen.[306] Mangels genauer Kenntnis ist es denkbar, dass die Verfahrensbeteiligten das Verschweigen von (subjektiven) Bewertungen gar nicht bemerken. Wird jedoch festgestellt, dass der Sachverständige auf Beurteilungsspielräume dieser Art

---

301 Das lässt sich auch aus der Formulierung des Sachverständigeneides ableiten. Gem. § 79 Abs. 2 StPO hat der Sachverständige das Gutachten unparteiisch und nach bestem Wissen und Gewissen zu erstatten, (siehe oben im 2. Teil, B. II. und III. 2. d)).

302 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 211 f. m. w. N.

303 Vgl. *Barton*, Der psychowissenschaftliche Sachverständige, S. 32 ff.

304 Hier könnten z. B. die critical questions bei argumentation schemes helfen vgl. *Deuber et al.*, Argumentation Schemes for Blockchain Deanonymization (vorgestelltes Paper bei JURISIN 2022), https://doi.org/10.48550/arXiv.2305.16883 [26.6.2023].

305 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 215.

306 Vgl. insb. medizinische Sachverständige, die es gewohnt sind, möglichst eindeutige Diagnosen zu stellen.

nicht hingewiesen hat, dann ist ggf. sogar ein Revisionsgrund nach § 337 StPO gegeben.[307]

Aufgrund der Vagheit der zur Verfügung stehenden Erfahrungssätze, ist es besonders schwierig, auf fremdpsychische Tatsachen zu schließen. So führt eine Anwendung von vagen Erfahrungssätzen zu noch vageren Schlussfolgerungen. Dieses Problem spitzt sich zu, wenn die Schlussfolgerung auf den rechtlichen Begriff gezogen werden sollen (bspw. die Vorsatzfrage in Bezug auf die §§ 184b ff. StGB). So vermag der ungeschulte Richter im Bereich der forensischen Informatik nicht zu erkennen, welche Beweiskraft sich aus den vom IT-Sachverständigen ermittelten Daten und deren Beschaffenheit bzw. ihrem Fundort ableiten lässt; und ebenso kennt der rechtsunkundige Sachverständige die juristischen Begriffe und ihre Auslegung nicht (wie Vorsatz nach §§ 15, 16 StG) bzgl. derer er dem Gericht entgegenkommen soll. Im Bereich der Vorsatzfeststellung lassen Strafverfolgungsorgane den Sachverständigen meistens nur im Rahmen seines Fachgebiets (wie über die Herabsetzung der Wahrnehmungsfähigkeit infolge Alkoholgenusses) ein Gutachten erstatten. Das Gericht selbst zieht dann die Schlussfolgerung, ob der Angeklagte vorsätzlich gehandelt hat.[308]

b) Trennung zwischen Rechts- und sonstigen Tatsachen

In Bezug auf die Trennung zwischen Tatsachen- und Rechtsfragen überkommt den Richter als Auftraggeber die Herausforderung, dass, wenn im Untersuchungsauftrag nach Rechtsfragen gefragt wurde (siehe dazu oben im 2. Teil, B. II. 3. b) bb)), jetzt letztlich doch er selbst entscheiden muss – trotz des komplizierten Sachverhalts. Dabei wird von ihm verlangt, dass er zumindest versucht, die einzelnen Schritte nachzuvollziehen, auf denen der Sachverständige seine Beurteilung aufbaut. Das muss sich auch aus der Darstellung im Urteil ergeben.[309] V. a., wenn sich die Tatsachen- und Rechtsfragen nicht klar trennen lassen, ergeben sich dabei Probleme. In Bezug auf die Schuldfähigkeit hat sich z. B. die Gewohnheit herausgebildet, den Sachverständigen als Gehilfen bei Bewertungen heranzuziehen, die sich schon auf die Interpre-

---

307 Denn es wird sich nicht ausschließen lassen, dass die vorenthaltene Information das Gericht bei seiner Entscheidung beeinflusst hätte; vgl. auch *Mezger*, AcP 117 (1918), Beilageheft, S. 1 (170 f.); *Stein*, Privates Wissen, S. 118 f.

308 Beispielsweise, ob die Wahrnehmungsfähigkeit aufgrund des Alkoholgenusses derart herabgesetzt war, dass es möglich erscheint, der Angeklagte habe das Kind am Straßenrand nicht bemerkt, um dann selbst zu entscheiden, ob der Angeklagte das Kind nicht bemerkt hat; zur Schuldfähigkeit und psychiatrischen Gutachtern vgl. *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 218.

309 Dazu BGH StV 1998, 470; BGH NJW 2000, 1350 in Bezug auf ein Jeansfaltengutachten.

tation des Gesetzes erstrecken (siehe oben zum Problem bei Haupttatsachen im 2. Teil, B. II. 3. b) cc)). Hier verlassen die Sachverständigen ihre Expertise und übernehmen Schlussfolgerungen, die eigentlich dem Gericht obliegen. Würde das Gericht einfach nur nach dem Ergebnis der Sachverständigenbeurteilung fragen und sich den Ausführungen des Sachverständigen ohne nachvollziehbare Argumentation im Urteil anschließen, entzöge es sich seiner Verantwortung, sodass ein revisibler Verstoß gegen das Gebot einer umfassenden Beweiswürdigung i. S. d. § 261 StPO vorläge.[310] Um beim obigen Beispiel zu bleiben, sollte der IT-Sachverständige deshalb auch nie Vorsatz in Bezug auf §§ 184 b ff. StGB „feststellen", sondern nur, dass technisch bedingte Umstände vorliegen, die darauf hindeuten.

Diese Vermengung der „Aufgabenbereiche" bringt dabei die folgenden Gefahren mit sich: So ergibt sich eine mögliche Suggestivwirkung der Sachverständigenausführungen insb. auf Schöffen.[311] Hier sind die Berufsrichter in der Pflicht, über die eingeschränkte Bedeutung der Stellungnahme aufzuklären. Dass eine etwaige verbleibende Beeinflussung der Regelung in der StPO nicht widerspricht, lässt sich daraus ableiten, dass die Berufsrichter auch sonst die Laienrichter in ähnlicher Weise beeinflussen wie die Sachverständigen. Denn die Laien besitzen auch auf dem Gebiet der rechtlichen Beurteilung nicht die erforderliche Sachkunde, so dass die Richter ihnen die notwendigen juristischen Zusammenhänge vermitteln (wie Sachverständige über Rechtsfragen), vgl. Nr. 126 Abs. 2 RiStBV. Bleibt die erforderliche Beratung durch die Berufsrichter allerdings aus, stellt das keinen revisiblen Verstoß dar (v. a. wenn man bedenkt, dass diese Erklärung sowieso während der „Geheimen Beratung" stattfindet). So wird auch mangelnde Aufklärung der Schöffen in Bezug auf die Tragweite der Sachverständigengutachten als nicht revisibel gesehen werden.

Positiv kann man allerdings sehen, dass evtl. die zusätzlichen Informationen und eine breiter angelegte Äußerung des Sachverständigen die forensische Gesprächsbasis ausdehnt und die Gefahr verringert, dass da, wo weitere Aufklärungen möglich wären, die (normative) Entscheidung schon zu früh eingreift. Weiter kann sie der Urteilsbildung des Richters auch insofern dienlich sein, als er feststellen kann, ob der Sachverständige von grundsätzlich richtigen rechtlichen Voraussetzungen ausgegangen ist.[312]

In der Praxis sollten – zumindest in „einfacher" gelagerten Fällen – Formulierungen wie „Datei X enthält kinderpornografische Inhalte" vermieden werden. Die letztendliche Einstufung einer Datei als Kinderpornografie i. S. d.

310 *Dahs/Dahs*, Revision, Rn. 422; Löwe/Rosenberg/*Gollwitzer*, § 261 Rn. 92 m. w. N.
311 SK-StGB/*Rudolphi*, § 20, Rdnr. 90.
312 Vgl. BGHSt. 7, 283.

§ 184b StGB obliegt den juristischen Entscheidern. Eine bessere Formulierung wäre bspw.: „Bei Datei X handelt es sich – aus technischer Sicht – vermutlich um eine inkriminierte Datei mit kinderpornografisch verdächtigem Inhalt“ (Erklärung/Darstellung folgt).

3. Dritte Kategorie (Befundgewinnung/Ergebnisse von Datenverarbeitungsvorgängen)

Zunächst ist innerhalb dieser Kategorie eine Abgrenzung zwischen Befund- und Zusatztatsachen vorzunehmen, denn über letztere darf der IT-Experte nur als Zeuge und nicht als IT-Sachverständiger vernommen und die Aussage auch entsprechend gewürdigt werden.[313]

Singuläre Prämissen, die in einer Argumentation für eine innere oder äußere rechtlich erhebliche Tatsache von Bedeutung sind und die nicht nur ihrerseits durch eine Argumentation erschlossen werden, sind durch ein Akzeptieren aufgrund von Wahrnehmungen gekennzeichnet. Solche singulären Prämissen können nur äußere Tatsachen aussagen. Innere Tatsachen sind nie unmittelbar beobachtbar. Sie können nur aus äußeren Tatsachen, dem Verhalten von Menschen bzw. deren Aussage geschlossen werden (für den Bereich der forensischen Informatik ist das wohl eher irrelevant).

Wie oben dargestellt, können sich bei der Würdigung von Schlussfolgerungen u. a. auch daraus Fehler ergeben, dass falsche Daten zugrunde gelegt werden (siehe zweite Fehlerquelle unter B. II. 2.). Hier lassen sich die auftretenden Beweiswürdigungsprobleme als ein Ausschnitt derjenigen der ersten Aussagekategorie erkennen: Die singuläre Prämisse kann in Zweifel gezogen werden, wenn das Instrument fehlerhaft arbeitet, dessen sich die IT-Sachverständige bedient, wie etwa Datenverarbeitungs- und -analyseprogramme, oder, wenn die Sinnesorgane der Sachverständigen versagt haben. Beide Arten von Fehlern werden nur mit Hilfe von Kriterien erkannt, die wie alles Wissen generell formuliert werden müssen, um in einer Argumentation für das Vorliegen eines Fehlers Relevanz in Bezug auf die Schlussregel zu besitzen.[314] In Bezug auf die Würdigung der zugrundeliegenden Methoden und Erfahrungssätze kann auf die Ausführungen oben bei A. III. 4. b) cc) (2) verwiesen werden.

Für eine ausführliche Plausibilitätskontrolle bzgl. des verwendeten Werkzeugs, wie die angewendete Software, könnte das Tatgericht darüber hinaus bspw. folgende Fargen stellen: Hat die Software die richtigen Daten berück-

313 Vgl. dazu im 2. Teil, B. II. 3. b) und d); sowie *Hess*, Digitale Technologien und freie Beweiswürdigung, S. 200 m. w. N.

314 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 235.

sichtigt? Ist eine datengetriebene Software anhand überzeugender, effektiver Modelle auf Grundlage einer repräsentativen, diskriminierungsfreien Trainingsdatenmenge trainiert worden? Haben die Entwicklerinnen die Software dafür vorgesehen, in der konkreten Fallkonstellation eingesetzt zu werden? Ist die Software handwerklich richtig programmiert?[315]

Wahrnehmungswissen[316] bedeutet zum Teil Kohärenz mit dem Evaluierungssystem und der Vertrauenswürdigkeit der wahrnehmenden Person.[317] Die wahrnehmende Person ist der IT-Sachverständige. Weiter erstreckt sich die Beweiswürdigung damit auch auf die Erörterung, ob der Sachverständige vertrauenswürdig ist.

III. Die Würdigung der Person des Sachverständigen (2. Schritt)

Die Richter verwenden als Mittel zum Beweis der entscheidungserheblichen Tatsachen Aussagen des Sachverständigen, die sie nicht mittels eigener Sinneswahrnehmung/Sachkunde überprüfen können. Sie übernehmen die Sicht von Tatsachen, so wie sich diese dem IT-Sachverständigen präsentieren. Das Gericht besitzt nur eine sehr beschränkte Kontrollmöglichkeit.[318] Zudem ergibt sich eine zu beobachtende Selbstüberschätzung forensischer Experten, die richtig eingeschätzt und auf ihren wahren Aussagehalt hin bewertet werden muss. So wird spekuliert, dass die Selbstüberschätzung von forensischen Experten vermutlich teilweise auf den Anfängen der Kriminalliteratur basiere, die viele Fortschritte bei den polizeilichen Ermittlungsmethoden begeistert aufnahm und dramaturgisch überhöhte. Das berühmteste Beispiel ist der geniale Spurenleser und Detektiv Sherlock Holmes, der im London des späten 19. und frühen 20. Jahrhunderts Straftäter mit Scharfsinnigkeit und einem Vergrößerungsglas überführt.[319] Das setzt sich auch heute noch fort in der Literatur (wo sogar Fachleute „ihre“ tolle Arbeit beschreiben, wie Benecke[320]) und in Filmen wie „Bones, die Knochenjägerin“. Aber auch in der Praxis konnte die Verfasserin i. R. v. Workshops beobachten, dass sich vereinzelte IT-Sachverständigenbüros weit mehr juristische Expertise zusprechen als den zur Entscheidung berufenen Tatrichtern.

---

315 *Mysegades*, Software als Beweiswerkzeug, S. 7.

316 Als zum Teil theoriengeprägt und damit geprägt durch systematisierte Argumentation.

317 Zum anderen Teil als sensorisches Element verstanden. Vgl. dazu auch *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 237.

318 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 55.

319 *Dewald/Freiling*, Forensische Informatik, S. 27.

320 https://home.benecke.com/ [29.6.2023].

1. Kriterien für die Vertrauenswürdigkeit von Aussagepersonen (Die Drei Faktoren)

Die Würdigung der Person des Sachverständigen setzt geeignete Kriterien für die Vertrauenswürdigkeit von Aussagepersonen voraus. Insoweit unterscheidet sich die Problematik also nicht von der Beurteilung eines Zeugen. Das Vertrauen eines Beurteilenden in die Aussage anderer Personen beruht auf drei Faktoren, die für persönliche Beweismittel charakteristisch sind:[321] Wahrhaftigkeit[322], Objektivität[323] und Sensitivität[324] der Beweispersonen.[325] Schum[326] und Toepel[327] haben Indizien für diese drei Faktoren systematisiert und die Beurteilung der Vertrauenswürdigkeit des Sachverständigen dargestellt.[328]

---

321 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 55, 239 ff.; *Schum*, Evidential Foundations, S. 100 ff.

322 Wenn eine Person Tatsachen behauptet, glaubt sie diese Tatsachenbehauptungen. Diese Voraussetzung wird in der Rspr. als „Glaubwürdigkeit" bezeichnet. Dabei wird eine „spezielle" von der „allgemeinen" unterschieden. Erstere betrifft die Beurteilung der Glaubhaftigkeit der Aussage zum jeweiligen Verfahrensgegenstand, vgl. auch BGHSt 29, 162 (163); BGH StV 1994, 64. Die allgemeine betrifft dagegen die Frage (insb. des Charakters), ob man der Aussageperson hinsichtlich sonstiger Angelegenheiten, unabhängig vom Verfahren, grundsätzlich Vertrauen schenken kann, vgl. dazu BGHSt 11, 97 (98 ff.). Nach *Eisenberg*, Beweisrecht der StPO, Rn. 1426 ist die allgemeine Glaubwürdigkeit nur ein Indiz bzgl. der speziellen Glaubwürdigkeit der Aussage. Es könnte aber auch sein, dass diese Charaktereigenschaften Relevanz für die anderen beiden Faktoren (bzw. die „Aussagefähigkeit") gewinnen: Wer bspw. einen sehr nachlässigen Charakter hat, beschreibt möglicherweise seine Sinneseindrücke sehr unpräzise, so dass auch Zweifel an der Objektivität aufkommen können.

323 Wenn eine Person Tatsachen behauptet und daran glaubt, hat sie Sinnesdaten erhalten, die diese Tatsachenbehauptung rechtfertigen.

324 Wenn eine Person behauptet, daran glaubt und entsprechende Sinnesdaten erhalten hat, dann handelt es sich um eine korrekte Aussage; auch „Präzession".

325 *Eisenberg*, Beweisrecht der StPO, Rn. 1362 ff., fasst 2. und 3. unter dem Begriff „Aussagefähigkeit" zusammen. Darunter wird die Fähigkeit einer zu vernehmenden Person verstanden, einen (konkreten) Sachverhalt zutreffend wiederzugeben, sofern diese Person willens ist, eine korrekte und vollständige Aussage zu machen, vgl. auch BGHSt 36, 217 (219); 41, 107 (109).

326 *Schum*, Evidential Foundations, S. 100 ff.

327 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 244 f.

328 Beachtet werden sollte dabei, dass Wahrhaftigkeit als Verständlichkeitsbedingung jeder Kommunikation vorausgesetzt wird. Relevant wird sie daher erst, wenn sie aufgrund gewisser Lügensymptome in Frage gestellt werden muss. Die Bedeutung der Lügensymptome kann durch positive Charaktereigenschaften wieder an Relevanz verlieren.

Wahrhaftigkeit ist eine Verständlichkeitsbedingung für jede Art von Kommunikation (siehe oben im 2. Teil, B. II. 3. c) aa)). Positiv kann die generelle Annahme von Wahrhaftigkeit nicht nachgewiesen werden. Andersherum, wenn das Verhalten der Aussageperson darauf hinweist, dass diese Annahme vorliegend nicht gerechtfertigt ist, ist die Aufstellung einer Skala von Lügensymptomen denkbar.[329] Weiter bedeutet die mangelnde positive Nachweisbarkeit der Wahrhaftigkeit in Bezug auf eine Aussage nicht, dass ausschließlich negative Eigenschaften der Aussageperson in diesem Zusammenhang vorgebracht werden können. So ist bspw. ein moralisch einwandfreier, unbestechlicher Charakter geeignet, die Relevanz gegenteiliger Indizien zu mindern.

Der Grad der Beherrschung durch die Aussageperson unterscheidet die Wahrhaftigkeit von der Objektivität und der Sensitivität. Fehler entstehen hier unbewusst aufgrund von Interessen der Aussageperson (Beeinflussung der Objektivität, vgl. hierzu im 2. Teil, B. II. 2. c) dd) und ee)) oder der die Aufnahmekapazität der Sinnesorgane übersteigendenden Differenziertheit des Sachverhalts bzw. einer Beeinflussung der Aufnahmekapazität durch Krankheiten oder Rauschmittel (Mängel hinreichender Sensitivität).[330] Von einer Aussageperson, deren Objektivität und Sensitivität besonders gut entwickelt sind, ist zu erwarten, dass sie in höherem Maß erkennt, wann ihre Fähigkeiten zu einer objektiven und sensiblen Beobachtung zur Zeit der Wahrnehmung ausnahmsweise eingeschränkt waren. Hat die Person tatsächlich die Einschränkungen ihrer Wahrnehmungsfähigkeit wahrgenommen, so ist von ihr im Rahmen der Wahrhaftigkeit zu erwarten, dass sie auf etwaige Einschränkungen hinweist. Andernfalls könnte von Täuschung gesprochen werden. Auf diese Weise wachsen die Erwartungen gegenüber der Wahrhaftigkeit der Aussageperson, je objektiver und sensibler sie ist. Bei einem Sachverständigen werden daher auf dem Gebiet seiner besonderen Sachkunde meist höhere Erwartungen an seine Wahrhaftigkeit bestehen als bei einem Zeugen.[331]

2. Qualifikation des IT-Sachverständigen

Die Problematik der Würdigung des Sachverständigen besteht darin, aussagekräftige positive oder negative Indizien zu finden, die das Gericht der Beur-

---

329 Vgl. dazu *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 244 f. m. w. N.

330 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 242.

331 So hat das Gesetz beim Zeugen im Regelfall die Vereidigung vorgesehen, § 59 StPO, während die Vereidigung des Sachverständigen gemäß § 79 Abs. 1 StPO grds. im Ermessen des Gerichts steht.

teilung zugrunde legen kann. Das Gericht ist i. d. R. nicht in der Lage, die Sachkunde der zum Sachverständigen bestellten Personen zu testen, sondern muss sich auf grobe standardisierte Kriterien verlassen. So z. B. im Hinblick auf die Ausbildung des Sachverständigen wie Hochschulqualifikationen, Fortbildungen, oder die langjährige Tätigkeit auf einem bestimmten Gebiet. Das kann für eine gewisse Erfahrung garantieren,[332] das kann aber auch hemmen, indem zu viel Routine und vordefinierte Wege und Denkweisen verfestigt wurden (Klischees und Vorurteile), die den Einzelfall nicht mehr berücksichtigen (vgl. dazu auch im 2. Teil, B. II. 2. c) ee)). Weiter spricht die Einhaltung der forensischen Mindeststandards im Sinne des 3. Teils, B. III. 5. für die Eignung der Person als gewissenhaftes und zuverlässiges Sachverständigenbeweismittel. Im Übrigen wird auf den 2. Teil, B. II. 2. c) cc) verwiesen.

In diesem Zusammenhang ist auch nochmal hervorzuheben, wie wichtig es ist – auch für die Würdigung der Person des IT-Sachverständigen –, dass sich die Verfahrensbeteiligten fundierte Kenntnisse im Bereich der forensischen Informatik aneignen.

Auch für den umgekehrten Fall – dass Forensiker ihr Grundfachwissen in Bezug auf verfahrens- und strafrechtliche Vorschriften ausweiten – wird häufig eine „Ausbildung zum Sachverständigen" gefordert.[333] Entscheidend soll zwar nach wie vor das Fachwissen und der Sachverstand des Fachvertreters sein, hilfreich sind daneben aber sicherlich auch verfahrensrechtliche und gewisse materiellrechtliche Grundkenntnisse, nicht zuletzt um eine gemeinsame Gesprächsbasis mit den juristischen Verfahrensbeteiligten, insb. dem Auftraggeber, zu finden (siehe dazu im 2. Teil, B. II. 3. c)). Hierfür bieten sich Masterstudiengänge der forensischen Informatik (mit interdisiplinären Bezügen zum Strafrecht), Workshops, Fortbildungen, o. ä. an, aber auch die Erfahrung, die sich im Laufe der Jahre zu einem guten Rechtsempfinden verdichtet. Von einem guten Sachverständigen wird in diesem Zusammenhang echtes Verständnis gefordert, das auf dem Wissen um die dogmatische Notwendigkeit der strafrichterlichen Tätigkeit basiert. Der Strafjurist ist auf eine bestimmte Argumentationsstruktur festgelegt, die durch die Trennung von Tatbestand und Rechtsfolge gekennzeichnet ist und die richterliche Begründung von einem sozial erheblichen Sachverhalt aus auf einen sich daraus ergebenden Lö-

---

332 *Toepel*, Grundstrukturen des Sachverständigenbeweises, S. 246.

333 Z. B. *Wetterich*, NJW 68, S. 114. *Walter*, Sachverständigenbeweis, S. 126 f. dagegen hegt Zweifel daran, ob es nötig ist, für Gerichtszwecke einen bestimmten Typ von Fachmann – nämlich „den Sachverständigen" – herauszubilden. Überspitzt formuliert er es, wenn er behauptet, genau das Gegenteil sei der Fall: Entscheidend seien das Fachwissen und der Sachverstand des Fachvertreters. Außerdem würde es die Unabhängigkeit des Sachverständigen im Umgang und in der Ausübung seines Fachgebiets beeinflussen.

sungsvorschlag hin ausrichtet.[334] Diese notwendige Argumentationsstruktur sollte der IT-Sachverständige schon in seinem vorbereitenden schriftlichen Gutachten anbieten und dabei die verschiedenen Tatsachen- und Aussagekategorien, angewendete Methodiken, Grundannahmen, Anfangswahrscheinlichkeiten und Richtigkeitswahrscheinlichkeiten bzw. Unsicherheiten ausweisen.

3. Fazit

Dreh- und Angelpunkt für die Würdigung der Person des IT-Sachverständigen dürfte bereits die Leitungspflicht aus § 78 StPO und die Formulierung des Beweisthemas sein: Je genauer die Ausgestaltung der Auftragserteilung und der Leitung sowie deren Dokumentation in den Akten, desto besser ist die Überprüfbarkeit der Objektivität des Gutachtens und damit die des IT-Sachverständigen. Finden sich bspw. Informationen in dem Gutachten, die in den dem Sachverständigen überlassenen Aktenteilen nicht vorhanden waren und die auch nicht im Rahmen des Auftrags zur Ermittlung beauftragt waren, deutet das darauf hin, dass der Sachverständige die Anknüpfungstatsache bzw. den Auftrag, diese zu erforschen, (unzulässigerweise) auf „ermittelndem" Wege erlangt hat. Demnach dient die ordnungsmäße Leitung des Sachverständigen auch dazu, die Objektivität des Gutachtens zu gewährleisten.[335] Weitere Vorschläge zur Wahrung der Objektivität werden im Kapitel „bias" (Zweiter Teil, B. II. 2. c) ee)) dargestellt.

C. Vagheiten in der Person des Richters

Nicht nur in der Person des Sachverständigen liegt eine Herausforderung im Rahmen der Würdigung des Sachverständigenbeweises, sondern auch in der Person der Richterinnen. In der öffentlichen Wahrnehmung dominiert das Bild des Homo iuridicus – also der Juristin, die streng formal nach Recht und Gesetz entscheidet. Neutral und vorurteilsfrei gegen jedermann, unter Ausblendung aller irrelevanten Tatsachen und Motive. Diesen Homo iuridicus gibt es nicht, er ist ein Trugbild. Tatsächlich tappen Juristinnen in die gleichen Entscheidungsfallen wie jeder Mensch.[336]

Das gilt sowohl für den fehlerhaften Prozess der Überzeugungsbildung (dazu sogleich) als auch für Defizite, die in der Person der Urteilsfindenden liegen: In der persönlichen Entscheidung wirkt sich alles aus, was die Richte-

---

334 Vgl. etwa *Krauß*, Die strafrechtliche Problematik kriminologischer Ziele und Methoden, S. 35 ff., der den Ablauf der Rechtsfindung wie folgt darstellt: aufklären – entscheiden – vollziehen.

335 Vgl. auch *Stinshoff*, Operative Fallanalyse, S. 147.

336 Vertiefend dazu *Risse*, NJW 2018, 2848.

rin geformt und gestaltet hat.[337] Wie oben bereits erwähnt, ist die Überzeugungsbildung ein schöpferischer Akt und Tatsachen feststellen heißt, sie erkennen und deuten unter erheblicher Einbeziehung des Rechtsgefühls und Einflüssen von (unterbewussten) Werten, Erwartungen und Annahmen (siehe dazu auch im 2. Teil, B. II. 2. c) ee)).[338] Auch Logik und Erfahrung spielen bei diesem vielschichtigen Prozess eine wichtige Rolle.[339] Für die Nachvollziehbarkeit dieses Prozesses muss beachtet werden, dass jeder tatsächlichen Folgerung ein schwer erfassbarer und beschreibbarer Wahrnehmungsprozess vorausgeht. Der Vorgang ist für niemanden sichtbar und findet keine unmittelbare Verschriftlichung, weshalb sich kriminalistische Fehler oder unrichtige Haltungen schwer finden bzw. erkennen lassen.[340] So können sich bspw. schwankende Grundhaltung mit empfindlichen Reaktionsverhalten vs. großzügiges Beachten fremder Wertvorstellungen und sich daraus ergebende Verhaltensmuster gegenüberstehen und zu unterschiedlichen Urteilsfindungen führen.[341] Allzu großes Selbstbewusstsein und zum Teil akademische Hybris können vernünftige Einwände unberücksichtigt lassen.[342] Daher muss eben ein umso größeres Augenmerk auf den bereits oben beschriebenen Regeln der praktischen Rationalität (A. III.) und insbesondere der Überprüfbarkeit mithilfe des § 267 StPO (A. III. 5.) liegen.

I. Fehler im Vorgang der Beweisbewertung

Die Hauptfehlerquelle bei der richterlichen Überzeugungsbildung ist die unrichtige Bewertung der erhobenen Beweise.[343] Dabei zieht der Tatrichter seine Folgerungen nicht lediglich erst aus dem am Schluss der Beweisaufnahme vorliegenden Material, sondern der Prozess der Überzeugungsbildung verläuft schon parallel zur Beweisaufnahme[344] und bestimmt die inhaltliche

337 *Peters*, Fehlerquellen, S. 107.

338 Vgl. auch *Alsberg*, JW 1929, 859 (863), der das emotionale Element bei der Überzeugung noch stärker betont. Eine umfassende Analyse findet sich bei *Bohne*, Zur Psychologie der richterlichen Überzeugungsbildung, S. 59 ff. Auch dazu *Schneider*, JuS 1970, 273; *Peters*, Fehlerquellen, S. 239; *Frielinghaus*, Vorgänge (1971) Vol. 5, S. 163.

339 Vgl. *Kuchinke*, Grenzen der Nachprüfbarkeit, 1964, S. 174 ff.; *Schwinge*, Revision, S. 186 ff.; *Engisch*, Logische Studien, S. 43, 94 f.

340 *Walter*, Sachverständigenbeweis, S. 96.

341 *Walter*, Sachverständigenbeweis, S. 91.

342 *Walter*, Sachverständigenbeweis, S. 91.

343 *Peters*, Strafprozess, S. 232.

344 Obgleich diese i. e. S. nicht zur Überzeugungsbildung als solcher zu rechnen ist. Beweisaufnahme und Überzeugungsbildung stehen doch in einem konditionalen Verhältnis, siehe dazu oben im 2. Teil, A.

Gestaltung der Beweisaufnahme je nachdem, ob der Tatrichter zu einem früheren oder späteren Zeitpunkt der Beweisaufnahme sein Meinungsbild verfestigt hat. Hier berühren sich die persönlichen Dispositionen des Tatrichters mit der Würdigung der schon erhobenen Beweise und der weiteren Gestaltung der Beweisaufnahme.[345] Hier können Fehler in der Person des Richters, bzw. in seinem Denken, das mit seiner emotionalen Befindlichkeit und seinen Assoziationen von emotionalen und kognitiven Erfahrungen und Erinnerungen verknüpft ist, zu mangelhafter und unvollständiger Beweisaufnahme führen. Die Würdigung eines Teils der Beweismittel stellt dann meist gleichzeitig einen Fehler in der Vollständigkeit der zu erhebenden Beweise dar.[346] Ein Fehler bei der Bewertung der erhobenen Beweise kann sich damit unmittelbar auf die weitere Beweisaufnahme auswirken, so dass eine falsche Beweiswürdigung gleichsam eine doppelte Fehlerhaftigkeit im gesamten Erkenntnisprozess hervorrufen kann. An dieser Stelle kommt der Verletzung anerkannter Regeln schlussfolgernden Denkens und der Zuverlässigkeitsskala eine besondere Bedeutung zu, denn auch eine freie Beweiswürdigung ist ohne die Logik dieser allgemeinen Regeln nicht denkbar (siehe dazu bei A. III. 2.). Sie setzen fest, welche tatsächlichen Feststellungen sich ergeben, wenn gewisse Beweisergebnisse vorliegen.[347]

Ursache einer falschen Bewertung der Beweisaufnahme kann auch das Außerachtlassen forensischer und auf Lebenserkenntnis beruhender Erfahrungen sein,[348] und zwar solcher, die selbst nicht den Grad zwingender Erfahrungssätze erreichen, dennoch aber häufig Indiz für die Verknüpfung zweier Gegebenheiten sein können, ohne eben das heuristische Prinzip (der strengen Beweisregeln) zu erfüllen (siehe dazu bei A. III. 4. b) cc) (2) (e)).[349]

Fehler können auch beim Umgang mit mehreren zur Verfügung stehenden Beweismitteln unterlaufen. Eine Hypothese eines Gutachtens gewinnt u. U. durch Indizien einen höheren Beweisgrad als es dem Gutachten, aber auch allein den Indizien, entspräche.[350] Zwei ungenügende Beweisketten können so für den Richter zur Grundlage seiner Gewissheit werden, ohne dass er die Tragfähigkeit der Einzelbeweise hinreichend untersucht hat. Dann ergibt sich aus zwei Eventualitäten die eine letztlich überzeugungsbildende Realität.

---

345 *Walter*, Sachverständigenbeweis, S. 92.

346 Ähnlich *Fezer*, Möglichkeiten, S. 60.

347 *Walter*, Sachverständigenbeweis, S. 93; *Dahs/Dahs*, Revision, Rn. 57; *Eb. Schmidt*, Lehrkomm. § 337, Rn. 30.

348 *Peters*, Fehlerquellen, S. 233 nennt diese Gedanken „Vorsichtsregeln" und die sich für den Richter daraus ergebenden besonderen Aufgaben „Kontrollaufgaben".

349 *Walter*, Sachverständigenbeweis, S. 93 f.; *Käßer*, Wahrheitsforschung, S. 35.

350 Vgl. auch *Peters*, Fehlerquellen, S. 172; ähnlich *Fezer*, Möglichkeiten, S. 59.

Ebenso fehlerhaft wäre auch eine Anpassung von Beweisen an die auf Grund anderer Beweise gewonnene Überzeugung, so etwa, wenn der Richter (von einem Sachverständigengutachten überzeugt) den weiteren Zeugenbeweis vom schon gewonnenen Ergebnis her beurteilt oder durch Umdeuten der gemachten Aussage einen Widerspruch zwischen Gutachten und Zeugenbeweis nivelliert.[351]

Fehler können auch durch die schlechte Qualität juristischer Erfahrungssätze bedingt werden.[352] So läuft die richterliche Sachverhaltsfeststellung nicht starr nach dem folgenden Phasenschema ab[353]: 1) Erkennen des Problems, 2) Erlangung der für die Rekonstruktion der Wirklichkeit notwendigen Informationen durch Beweisaufnahme, 3) Herstellung verschiedener Geschehensalternativen auf Grundlage der Beweise, 4) Subjektive Bewertung dieser Alternativen, 5) Auswahl der überzeugendsten Alternative, auf deren Grundlage dann das Urteil/Freispruch basiert. Tatsächlich finden alle diese „Phasen" nebeneinander statt.[354] Nach der „Vorwirkung der Theorie"[355] entscheidet der Richter, worüber Beweise erhoben werden sollen und welche Tatsachen als irrelevant erachtet werden. Nach diesem Vorgehen ermittelt er Tatsachen, von denen er glaubt, auf das Vorliegen bestimmter Tatbestandsmerkmale schließen zu können. Die Erfahrungssätze dienen dabei als „Brücke" zwischen einer gegenwärtigen, unmittelbar erkannten Wirklichkeit (dem Vorliegen bestimmter Beweismittel) und einer nicht gegenwärtigen (der tatbestandsrelevanten) Wirklichkeit.[356] Die vom Gericht angewendeten Theorien bestimmen also worüber überhaupt Beweis erhoben wird. Die Sachverhaltsfeststellung trifft nur dann zu, wenn die angewendeten Theorien richtig sind, wenn alle in Frage kommenden Theorien angewendet und die Randbedingungen vollständig und richtig ermittelt wurden.[357] Nicht nur bei der Anwendung der Erfahrungssätze des Sachverständigen kommt es also auf die (versteckten) Qualitäten an, sondern auch bei den juristischen Erfahrungssätzen bzgl. Beweiserhebung und -würdigung selbst.[358] Trotz der Existenz soziologisch bestätigter Theorien ist festzustellen, dass der Richter anders als der Naturwissenschaftler fast nie

---

351 Vgl. auch *Peters*, Fehlerquellen, S. 175.

352 Vertiefend dazu: *Stamp*, Die Wahrheit im Strafverfahren, S. 108 ff.

353 Darstellung auch bei *Käßer*, Wahrheitsforschung, S. 80 f.; *Stamp*, Die Wahrheit im Strafverfahren, S. 108.

354 *Käßer*, Wahrheitsforschung, S. 81; *Stamp*, Die Wahrheit im Strafverfahren, S. 108.

355 *Käßer*, Wahrheitsforschung, S. 82 ff.

356 *Käßer*, Wahrheitsforschung, S. 83.

357 *Käßer*, Wahrheitsforschung, S. 84 ff.; *Stamp*, Die Wahrheit im Strafverfahren, S. 109.

358 Negativbeispiele: BGH NStZ 1982, S. 478 f.; OLG Karlsruhe VRS 56, 359 f. („Alle Türken lügen vor Gericht", als Beispiel eines nicht begründbaren Erfahrungs-

ausschließlich durch die Anwendung gut bestätigter Erfahrungssätze zum Ziel kommt. Aufgrund des starken Einzelfallbezugs stehen, wenn überhaupt, teilweise nur wenig bestätigte Erfahrungssätze zur Verfügung.[359] Da die Erfahrungssätze zumeist nur in der „rudimentären Form qualitativer Alltagstheorien" vorkommen, spielen bei der Tatsachenfeststellung überwiegend vorwissenschaftliche Methoden eine Rolle.[360] Vor allem in komplizierten Fällen, bei denen eine Vielzahl an Erfahrungssätzen zur Anwendung kommen, entstehen Schwierigkeiten bei der Wahl der zu erhebenden Randbedingungen durch den Richter und damit Gefahren für die Wahrheitsfindung.[361] Dieses Problem lässt sich wohl nicht auflösen, allerdings kann eine gewisse Sensibilität und Mitbewusstsein dieses Umstandes schon Verbesserung bewirken.

Im Übrigen sei an dieser Stelle auch auf beim Richter vorkommende Phänomene hingewiesen wie „bias" und „noise"[362], eine Überforderung bei der Informationsverarbeitung[363] wie der „Redundanzeffekt"[364], eine „Urteils-Perseveranz"[365] sowie die Überschätzung von Wahrscheinlichkeiten[366] – das gilt für die Richter im Umgang mit digitalen Spuren noch ausgeprägter, aufrgund der extrem große Datenmengen und der oben beschriebenen Herausforderungen, die mit der Besonderheit der forensischen Informatik (Abgekoppeltheit von der physischen Welt und Universalität) einhergehen. In diesem Zusammenhang gilt es auch, endgültig das Vorurteil unter Richtern „Technik irrt nicht"[367] aufzulösen.[368] So werden digitale Beweise von einigen Juristen nach wie vor als zuverlässig und korrekt angesehen. Das sollte ein Grund zur Besorgnis sein, v. a. wenn man die Ergebnisse einer kürzlich von Page et al. (2018)[369] durchgeführten Analyse der Qualitätsmanagement-Verfahren (QM-Verfahren) innerhalb der forensischen Informatik betrachtet. Sie verglichen

satzes); Beispiel von *Stamp*, Die Wahrheit im Strafverfahren, S. 110 („Jeder Mensch mit geringem Einkommen nimmt stets Sachen in Zueignungsabsicht weg").

359 *Stamp*, Die Wahrheit im Strafverfahren, S. 111 m. w. N.

360 *Stamp*, Die Wahrheit im Strafverfahren, S. 111 m. w. N.

361 *Stamp*, Die Wahrheit im Strafverfahren, S. 111.

362 *Thaler/Sunstein*, Nudge, S. 29 ff.; *Kahnemann/Sibony/Sunstein*, Noise, S. 19 ff., 47 ff.

363 *Stamp*, Die Wahrheit im Strafverfahren, S. 114 ff.

364 *Schünemann*, GA 1978, S. 171 f.

365 *Schünemann*, GA 1978, S. 172 f.

366 *Schünemann*, ARSP Beih 22 (1985), S. 80.

367 Vgl. dazu auch *Mason/Seng*, Electronic Evidence, S. 101 ff. Zudem gibt es eine Studie von *Dressel/Farid*, Science Advances, 2018, die belegt, dass die Ergebnisse von Algorithmen nicht besser „funktionieren" als die menschlicher Beurteilungen.

368 *Marshall*, Digital Evidence and Electronic Signature Law Review (2020) Vol. 17, S. 2; *Sunde*, Non-technical Sources of Errors.

369 *Page et al.*, Science & Justice (2019) Vol. 59, S. 83.

dabei die QM-Verfahren zwischen Körperflüssigkeiten und DNA, Fingerabdrücken und der forensischen Informatik in der UK und stellten fest, dass die forensische Informatik mit den am wenigsten robusten QM-Verfahren arbeitet.[370]

II. Feststellbarkeit von Fehlern innerhalb des Vorgangs der Überzeugungsbildung

Fehler in der Überzeugungsbildung müssen oft zwangsweise hingenommen werden, weil richterliches Fehlverhalten häufig nicht als solches feststellbar ist. „Jener Raum der Überzeugungsbildung, der vom rein persönlichen Urteil des Tatrichters ausgefüllt wird, ist also wirklich frei."[371]

Feststellbar ist fehlerhaftes Verhalten nur dann, wenn und soweit es sichtbar gemacht werden kann. Aus Sicht des Revisionsrichters kann also gefragt werden, welche Erkenntnismittel und unter welchen Perspektiven die möglichen Fehler für den Rechtsmittelfehler sichtbar gemacht werden können (vgl. A. III.).

Die tatsächlich bestehenden revisionsgerichtlichen Erkenntnismöglichkeiten sind von der den Prüfungsumfang festlegenden gesetzlichen Revisionssystematik abzuheben, da jede Nachprüfungsmöglichkeit mit den der Revision zur Verfügung stehenden Instrumentarien der Fehlererkennung steht und fällt.[372] In erster Linie sind es die schriftlichen Erkenntnisquellen wie Urteilsgründe, Hauptverhandlungsprotokolle und der gesamte Akteninhalt, die dem Richter zur Verfügung stehen und an denen sich tatrichterliche Fehler erkennen und feststellen lassen.

So kann fehlerhaftes Verhalten häufig in Bezug auf Mängel in der Beweisaufnahme sichtbar gemacht werden – soweit der Pflicht zur schriftlichen Offenlegung der maßgebenden Überzeugungskriterien Folge geleistet wird (insb. § 267 Abs. 1 StPO als die Manifestation der tatrichterlichen Überzeugungsbildung).[373] So könnte der Tatrichter bei dem Versuch, das dargestellte Ergebnis zu rechtfertigen, bspw. falsche Erwägungen erkennen lassen. So ist die schriftliche Darstellung der tatrichterlichen Feststellungen eben nicht nur die Aneinanderreihung verschiedener einzelner Tatsachenpartikel, sondern ergibt im Gesamtrahmen mit der vom Ablauf der Beweisaufnahme in der Hauptverhandlung abgeleiteten Begründung eine eigene Würdigungsebene, in der selbstständige kriminalistische Fehler erkennbar werden können.

---

370 *Sunde/Dror*, Digital Investigation (2019) Vol. 29, S. 102.

371 *Walter*, Sachverständigenbeweis, S. 96.

372 *Walter*, Sachverständigenbeweis, S. 95.

373 *Walter*, Sachverständigenbeweis, S. 96 f.; *Peters*, Fehlerquellen, S. 38.

D. Ideen für eine Verbesserung

Abschließend sollen einige Ideen geteilt werden dahingehend, wie der Umgang mit dem IT- Sachverständigenbeweis im Rahmen der Beweiswürdigung nach § 261 StPO verbessert und greifbarer gemacht werden könnte.[374]

In der Literatur gibt es bereits einige Vorschläge bzgl. des Umgangs mit digitalen Beweismitteln bzw. zur Steigerung ihres Beweiswerts: Singelnstein etwa fordert, dass die eingesetzten Datenverarbeitungs- und analysemethoden unter eine unabhängige behördliche Aufsicht der Datenschutzbehörden zu stellen sind.[375] Eine solche Aufsicht könnte sich positiv auf den Beweiswert der zugrundeliegenden Softwareauswertungen auswirken. Dabei wären im Einzelfall die Effektivität der Kontrollrechte inklusive der Rechtsfolgen von Beanstandungen sowie der Umfang und die Transparenz der faktischen Kontrolle zu beachten.[376] Ernst plädiert in diesem Zusammenhang für eine digitale Souveränität des Staates, die in erster Linie ein Outsourcing von IT-Infrastruktur verbieten soll.[377] Mysegades überträgt diesen Gedanken auf die staatliche Entwicklung von Software. In der Praxis haben sich auch schon einige solcher Projekte bewährt; bspw. haben die Länder Nordrhein-Westfalen eine Predictive Policing-Software „SKALA“[378] und Bayern ein OSINT-Tool, den sog. Dark Web Monitor[379], staatlich bzw. interdisziplinär und unter Beteiligung der Wissenschaft und Öffentlichkeit entwickelt. Ein solches transparentes Vorgehen durch staatliche Stellen bei der Erstellung von Software, die später zu Beweiszwecken verwendet wird, beeinflusst den Beweiswert ohne Zweifel positiv.[380]

Ein Gedanke, der sich bei diesem Thema vielleicht intuitiv auftut, wäre etwa, als Minusmaßnahme zu strengen Beweisregeln, dass der Gesetzgeber dem Gericht gesetzliche Darstellungspflichten in der Beweiswürdigung auferlegen könnte. So könnte er etwa die Pflicht festschreiben, dass ein Tatsachengericht bei jeder Beweiswürdigung von IT-Sachverständigengutachten zumindest zu den Daubert-Kriterien[381] schriftlich Stellung nehmen muss: Testbar-

374 Vgl. dazu auch *Mysegades*, Software als Beweiswerkzeug, S. 526 ff.

375 *Singelnstein*, NStZ 2018, S. 1 (7); ähnlich auch *Heinson*, IT-Forensik, S. 138.

376 *Mysegades*, Software als Beweiswerkzeug, S. 543.

377 *Ernst*, Der Grundsatz digitaler Souveränität, 2020, S. 28 ff., 94 f.

378 Landeskriminalamt Nordrhein-Westfalen, Kooperative Evaluation des Projekts „SKALA“, 2018, https://polizei.nrw/sites/default/files/2018-06/160430_Evaluationsbericht_SKALA.pdf (17.02.2021), S. 5 ff., S. 25.

379 https://www.justiz.bayern.de/presse-und-medien/pressemitteilungen/archiv/2020/69.php [22.1.2024].

380 *Mysegades*, Software als Beweiswerkzeug, S. 543 f.

381 *Mysegades*, Software als Beweiswerkzeug, S. 207 ff., S. 221 ff.

keit/Falsifizierbarkeit, Veröffentlichung mit Peer Review, feststellbare Fehlerrate oder etwa die konfrontative Befragung des Sachverständigen mit laienhaft nachvollziehbarer Erläuterung der Methode mit Bezug auf den konkreten Einzelfall.[382] So könnte der Gesetzgeber zwar ein Mindestmaß an kritischer Prüfung der Methodik erzwingen, ohne dabei die freie richterliche Beweiswürdigung einzuschränken (die Darstellung der Kriterien hätte keinen bindenden Einfluss auf das gerichtliche Würdigungsergebnis). Allerdings sieht Mysegades die Gefahr, dass man mit einer solchen systematischen Neuheit die Gewaltenteilung aus dem „Gleichgewicht" bringen könnte, insbesondere mit Hinblick auf die richterliche Unabhängigkeit gem. Art. 92, 97 Abs. 1 GG. Die bestehenden Probleme im richterlichen Umgang mit digitalen Beweismitteln können vielmehr über das existierende System der freien richterlichen Beweiswürdigung mit Darstellungsmaßstäben der höchstrichterlichen Rechtsprechung gelöst werden.[383]

Der Schwerpunkt sollte zunächst bei der Entwicklung rationaler Entscheidungshilfen liegen, um die Ergebnisse des IT-Sachverständigenbeweises und sowohl seine Beweiskraft, als auch die zugrundeliegenden Schwachpunkte (auch auf juristischer Seite im Umgang damit) offenzulegen. Wenn die Regeln der praktischen Rationalität ernstgenommen und für den IT-Sachverständigenbeweis und die damit einhergehenden Besonderheiten weiterentwickelt werden, kann somit eine intersubjektive Diskutierbarkeit und Nachvollziehbarkeit geschaffen werden. Auch nach Knopp fehlt es bisher an unterstützenden Richtlinien für die Gerichte im Umgang mit digitalen Beweismitteln.[384] Ebenso sieht Mysegades[385] den Hebel zur Bewältigung der vorherrschenden Probleme bei der Würdigung digitaler Beweismittel in der richterlichen Methodenkritik. Dafür müssten Qualitätskriterien – zugeschnitten auf die Besonderheiten der forensischen Informatik – festgelegt werden, damit die Tatrichter daraus Anhaltspunkte ziehen können, um zu ermitteln inwieweit der IT-Sachverständige die spezifische Methodik eingehalten hat. In einigen Bereichen existieren bereits spezifische Kataloge oder Kriteriensammlungen, die eine Kontrolle der mittelbaren Wissens- und Methodenvermittlung durch Sachverständige ermöglichen.[386] Diese könnten als Vorbild dienen. Dabei ist

---

382 *Mysegades*, Software als Beweiswerkzeug, S. 541.

383 *Mysegades*, Software als Beweiswerkzeug, S. 542; ähnlich auch *Momsen*, KriPoZ 2018, S. 142 (147); *Momsen*, in: FS Beulke, S. 871 (880); *Savic*, Die digitale Dimension des Strafprozessrechts, S. 195 f., S. 321.

384 *Knopp*, GI-Jahrestagung 2009, S. 1552 (1560).

385 Software als Beweiswerkzeug, S. 124.

386 Für forensische Methoden bzgl. der Identifikation von Personen auf Bildern haben MAH/*Rösing/Hirthammer*, (2. Aufl.) § 79, Rn. 13 zehn Kriterien zusammengestellt, die für die Etablierung einer Methode im sachverständigen Feld sprechen: Die Methode sollte (1.) auf einem Kernbereich eines wissenschaftlichen Faches beruhen,

insbesondere die Pflicht zur Überprüfung der Einhaltung der Standards der forensischen Informatik (insb. die Integrität und Authentizität von digitalen Spuren, die Mitteilung über (nicht) mögliche Schlussfolgerungen bzw. Fehlerquellen und die Einhaltung der verfahrensrechtlichen Grenzen) im Rahmen des § 261 StPO zu berücksichtigen. Auch die anderen Standards der forensischen Informatik dienen als Indizien bei der Ermittlung der Beweiskraft des IT-Sachverständigenbeweises i. S. d. Beurteilung der Richtigkeitswahrscheinlichkeit der Datenverarbeitungs- und -analysemethoden und Erfahrungssätze.[387] Zukünftig werden so auch die Rechtsmittelgerichte verpflichtet, sich damit auseinanderzusetzen. Dadurch wird dazu beigetragen, dass die Methoden und Erfahrungssätze (zumindest teilweise) in Zukunft als standardisiert eingeschätzt werden können.

Weiter sollte das Grundlagenwissen der Verfahrensbeteiligten im Umgang mit dem IT-Sachverständigenbeweis (v. a. auf juristischer Seite in Bezug auf die forensische Informatik) ausgebaut werden.[388] Dabei helfen können v. a. auch die Forensikerinnen im Rahmen ihrer Gutachtenerstattung durch eine Adressierung an Nicht-Techniker, bspw. durch eine Zusammenfassung für Laien, Begriffsglossare, und Transparenz der verschiedenen Aussagekategorien und verwendeten Datenverarbeitungs- und -analysemethoden sowie das Ausweisen von Richtigkeitswahrscheinlichkeiten und Unsicherheiten (auch auf die Gefahr hin, dass das Gutachten „platzt"). Auch bei der mündlichen Gutachtenerstattung vor Gericht sollte insbesondere auf die Rhetorik geachtet werden und wünschenswerterweise auch auf geeignete Visualisierungsmög-

---

(2.), in Lehrbüchern behandelt sein, (3.) in Aufsätzen und Monografien weiter entwickelt werden, (4.) eine größere Zahl Anwender haben, (5.), zahlreiche verschiedene Fälle bearbeiten, sodass Weiterentwicklungen möglich sind, (6.) veröffentlichte Standards aufweisen, (7.) laufender Qualitätssicherung unterworfen sein, (8.) nach Bedarf auch neue Sachverständige ausgebildet sowie (9.) anhand eines Zulassungsverfahrens zugelassen werden und nicht nur ein fester Kreis bestehender Sachverständiger besteht und schließlich (10.) darf sie auf Zusammenarbeit der Sachverständigen im Feld beruhen; Einige Beispiele finden sich auch bei, SK-StPO/*Rogall*, Vor § 72 Rn. 129 m. w. N.

387 So auch die Forderung von *Mysegades*, Software als Beweiswerkzeug, S. 126 ff., dass die Tatrichter im Rahmen der Würdigung der sachverständigen Methodik auf abstrakte wissenschaftstheoretische Kriterien abstellen müssen wie die Objektivität, Reliabilität und Validität. Die Objektivität einer Methode beschreibt, ob unterschiedliche Anwender oder Interpreten zum gleichen Ergebnis gelangen. Die Reliabilität einer Methode meint die Zuverlässigkeit im Sinne der Abweichung zwischen Ergebnis und Wirklichkeit. Die Validität einer Methode betrifft die Erfassung des konkret erwünschten Merkmals durch die Methode. Grundvoraussetzung dafür, dass eine Methode als wissenschaftlich anzuerkennen ist, ist zudem, dass sie grundsätzlich falsifizierbar oder testbar ist. Nur dann steht sie dem jeder Wissenschaft zugrundeliegenden Prozess der kommunikativen, intersubjektiven Akzeptanz durch Diskurs offen.

388 So auch *Mysegades*, Software als Beweiswerkzeug, S. 544 f.

lichkeiten zurückgegriffen werden. Damit geht auch eine bessere technische Ausstattung der Gerichte einher.[389]

Auf Seiten der juristischen Verfahrensbeteiligten hilft es dabei sicherlich, so wie derzeit in der Praxis auch schon beobachtet werden kann, die Spezialisierungen der Strafverfolgungsbehörden[390] und der Strafverteidigung („Cyber-Strafverteidigung")[391] um den Umgang mit digitalen Spuren zu bündeln. Aber andere Vorschläge etwa wie „IT-Forensiker als Laienrichter" oder „Cyber-Strafkammern" oder ausgebildete Richterposten nach dem Vorbild des „special masters"[392] sind m. E. abzulehnen. Im Laufe der Untersuchung sollte deutlich geworden sein, dass die Technologie „universell", damit auch so vielseitig und schnell im Wandel ist und in jeden Lebensbereich reicht, dass schlicht nicht garantiert werden kann, dass auch die spezialisierten Strafkammern das benötigte Wissen vorweisen und besser würdigen könnten. Selbst ein IT-Sachverständiger auf der Richterbank ist im Einzelfall keine Gewähr für inhaltliche Richtigkeit und eine genaue Überprüfung des erstatteten Gutachtens.[393] Zudem wären diese spezialisierten Strafkammern und Richter, aufrgund des extrem hohen Aufkommens digitaler Spuren, mit nahezu jedem Verfahren betraut. Eine derartige Qualifikation der Richter hätte zudem den Nachteil, dass er dann nicht mehr nur in seinen alltagsvernünftigen Kategorien denken kann, wenn er schon von vorneherein durch das scheinbare Fachwissen eingeschränkt wird in seinem Blick über den Tellerrand hinaus zu einem Gesamtverständnis des Falles. Die Aspekte der Besonderheit des Einzelfalles können so leichter verloren gehen und damit dem Ganzen evtl. nicht mehr gerecht werden. Vielmehr sollten sich die Richterinnen auf ihre Entscheidungsautorität konzentrieren und sich ein gewisses Grundverständnis der forensischen Informatik aneignen, um bzgl. ihrer Besonderheit (sowie ihrer Stärken und Schwächen) sensibilisiert und achtsam entscheiden zu können. Dabei ist auf die Grenze einer vertieften Spezialisierung zu achten, denn alle erforderlichen Kenntnisse aus sämtlichen Naturwissenschaften, Medizin, Technik, Psychologie usw. kann und vermag die

389 So jedenfalls Berichte aus der Praxis.

390 So die in Bamberg ansässige Zentralstelle Cybercrime Bayern (ZCB) und die in Frankfurt a. M. sitzende Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT). Außerdem die verschiedenen Cyberkriminalisten oder sog. Cybercops in den deutschen Polizeidienststellen.

391 Vgl. bspw. https://rechtsanwaelte-wirtschaftsstrafrecht-berlin.de/dr-uwe-ewald/ [29.6.2023]; https://www.strafrecht.de/en/team/dr-eren-basar/ [29.6.2023]; https://www.tsambikakis.com/berater/diana-nadeborn [29.6.2023].

392 Vgl. *Mysegades*, Software als Beweiswerkzeug, S. 545 m. w. N.

393 Vgl. in Bezug auf andere forensische Disziplinen auch *Schröder*, Die kriminalpolitischen Aufgaben der Strafrechtsref., S. 76 f.; *Eb. Schmidt*, JZ 1961, S. 585; *Leferenz*, Kriminolog. Biol. Gegenwartsfragen H. 5, S. 4 ff.

Juristenausbildung nicht vermitteln. Anders als der nur auf einem Spezialgebiet tätige Wissenschaftler kann der Strafrichter nicht selbst sämtliches verfügbares „Handwerkszeug" verinnerlicht haben und nutzbar machen.[394] Dass der den Sachverhalt feststellende Richter im Strafverfahren sein Handwerk „weniger beherrscht" als z. B. der in Quellenarbeit ausgebildete Historiker, liegt deshalb nicht unbedingt an einer qualitativ minderwertigen Ausbildung, sondern ist vielmehr dem Strafprozess immanent.[395] Genau aus eben diesem Grund regeln auch die §§ 72 StPO die Zuziehung dieser bestimmten sachverständigen Personen. Während der Wissenschaftler im Normalfall für sein Spezialgebiet keiner sachverständigen Hilfe bedarf, liegt im Prozess der Ermittlungstätigkeit die Sachverhaltsfeststellung nicht allein bei dem, der zur Wahrheitsfindung berufen ist.[396]

Durch das eben Beschriebene kann gewährleistet werden, dass durch kundige und sensibilisierte Strafverfolgungsbehörden der Sachverhalt qualitativ hochwertig und möglichst objektiv aufbereitet werden kann, die gut vorbereiteten und hartnäckigen Verteidiger die Fragen stellen können, auf die es ankommt, und die selbstbewussten Richterinnen ihre Leitungspflicht aus § 78 StPO und die §§ 244 Abs. 2, 261 StPO zur Erforschung der Wahrheit und Urteilsfindung ernst nehmen und i. S. einer eigenen Plausibilitätskontrolle der Sachverständigenaussagen v. a. im Hinblick auf die Einhaltung der Standards der forensischen Informatik und der zugrundeliegenden Unsicherheiten bzw. Fehlertoleranzen zu einer gerechten Entscheidung finden. In diese Richtung formuliert auch schon der BGH eindeutig: „Der verfahrensrechtliche Ausgangspunkt liegt darin, dass der Tatrichter zu einem eigenen Urteil auch in schwierigen Fachfragen verpflichtet ist. Er hat die Entscheidung, auch über diese Fragen, selbst zu erarbeiten, ihre Begründung selbst zu durchdenken. Er darf sich dabei von Sachverständigen nur helfen lassen".[397]

So sollte auch schon bei „heranwachsenden" Verfahrensbeteiligten das Interesse am interdisziplinären Schnittpunkt zwischen Rechtswissenschaft und IT geweckt werden, wie etwa durch Angebote von Ringvorlesungen[398], der Möglichkeit eines LL.M.'s, in diesem Bereich[399] oder wissenschaftliche Forschungsgruppen zu bilden etc. Auch sollten in der Referendarausbildung die prozessualen Probleme des Sachverständigenbeweises eine größere Beach-

394 *Stamp*, Die Wahrheit im Strafverfahren, S. 113.

395 *Stamp*, Die Wahrheit im Strafverfahren, S. 113.

396 *Stamp*, Die Wahrheit im Strafverfahren, S. 114.

397 BGHSt 8, 118; So auch schon als Fazit von Walter vor fast 50 Jahren, vgl. *Walter*, Sachverständigenbeweis, S. 158.

398 https://www.cybercrime.fau.de/ [29.6.2023].

399 Vgl. in der Art https://legal-tech.de/legal-tech-masterstudiengaenge/ [29.6.2023].

tung finden, v. a. bzgl. der Auswahl und Leitung sowie der Beweiswürdigung.[400]

Die IT-forensische und juristische Wissenschaft könnte dazu aufgerufen werden, weiter an wissenschaftlich gesicherten Erfahrungssätzen, an Studien über die Verteilung von Merkmalen in der Bevölkerung zur Quantifizierung der Irrtumswahrscheinlichkeiten bei Assoziationen im Rahmen der Rekonstruktion des Tathergangs in der forensischen Informatik sowie an der Nachvollziehbarkeit und Standardisierung der verwendeten Techniken zu arbeiten.

400 So auch schon *Walter*, Sachverständigenbeweis, S. 125.

5. Teil

Zusammenfassung

Abschließend sollen nun die drei Forschungsfragen beantwortet und die Unstersuchung damit zusammengefasst werden.

1. Passt die tatsächlich ausgeführte Praxis der IT-Sachverständigen (noch) unter die Strafverfahrensvorschriften?
2. Wie kann eine möglichst (hochwertige) objektive Tatsachengrundlage für die tatrichterliche Überzeugungsbildung i. S. d. § 261 StPO in Bezug auf den IT-Sachverständigenbeweis in einem Strafverfahren geschaffen werden?
3. Wie sieht eine revisionssichere Beweiswürdigung des IT-Sachverständigenbeweises aus?

A. Passt die tatsächlich ausgeführte Praxis der IT-Sachverständigen (noch) unter die Strafverfahrensvorschriften?

Auf der Grundlage des geltenden Beweisrechts der StPO wurde gezeigt, dass diese Normen grds. geeignet sind, bei entsprechender Auslegung die spezifischen Problemlagen sowohl bei der forensischen Tätigkeit der IT-Sachverständigen als auch bei der Bewertung und Würdigung als Beweis im Strafverfahren zu lösen und letztlich den Richtern dabei zu helfen, die „forensische Wahrheit“ zu finden. An dem Untersuchungsergebnis von Rückert anknüpfend hat die Arbeit ergeben, dass der IT-Sachverständigenbeweis meist das bestmögliche und sachnächste Beweismittel ist im Umgang mit digitalen Spuren und die Richterinnen i. S. d. §§ 244 Abs. 2 und 261 StPO regelmäßig verpflichtet sein werden, einen IT-Sachverständigen zu beauftragen. In den aktuellen Strafverfahren spielt er deshalb eine entscheidende Rolle. Dabei ist der IT-Sachverständige in der StPO der Autoritätsperson des Gerichts bzw. im (der Hauptverhandlung vorgelagerten) Ermittlungsverfahren der Staatsanwaltschaft und ihren Ermittlungspersonen als ein persönliches Beweismittel zugeordnet. An dieser Stelle muss v. a. der verfahrensrechtlichen Besonderheiten der Bestellungspraxis durch die Staatsanwaltschaft bzw. ihrer Ermittlungspersonen im Ermittlungsverfahren Rechnung getragen werden. Damit

gehen einige Vorteile einher, aber eben auch erhebliche Nachteile, v. a. im Hinblick auf die prozessuale Waffengleichheit zum Nachteil des Beschuldigten und der Strafverteidigung. Die dominierende Stellung der Staatsanwaltschaft im Ermittlungsverfahren muss zunächst dadurch ausgeglichen werden, dass der Verteidigung vor Beauftragung nach Nr. 70 Abs. 1 RiStBV Gelegenheit zur Stellungnahme gegeben werden muss. Auch muss die Leitungspflicht der Richter nach § 78 StPO zunächst auf die Staatsanwältinnen übertragen und schließlich (zumindest nachträglich) von den Richtern ernst genommen werden. Letzteres soll insebsondere dann gelten, wenn die Sachverständigen lediglich von den Richtern bestätigt und in die Hauptverhandlung übernommen werden und die eigentliche Zusammenarbeit und Kommunikation zwischen Staatsanwaltschaft bzw. ihren Ermittlungspersonen und IT-Sachverständigen bereits im Ermittlungsverfahren passiert ist. Durch die nachträgliche Kontrolle der Einhaltung der Leitungspflicht soll sichergestellt werden, dass auch schon während des Ermittlungsverfahrens eine Leitung des IT-Sachverständigen durch die Auftraggeber stattgefunden hat. Auch um der oft gepredigten Gefahr des Kontrollverlustes der Richter entgegnen zu können (v. a. immer dann, wenn es um neue forensische Wissenschaften in Strafgerichten geht), muss diese Leitungspflicht des § 78 StPO ernstgenommen werden. Aus der Leitungspflicht nach § 78 StPO unter Berücksichtigung der Nr. 72 Abs. 2 RiStBV ergibt sich u. a. eine klare und eindeutige Auftragserteilung, die von möglichst bestimmt formulierten Beweisfragen umschrieben und begrenzt werden soll. Dabei gestaltet sich die Formulierung des Beweisthemas in der Auftragserteilung oft schwierig („Ping-Pong-Spiel“). Um diese Schwierigkeit aufzulösen, soll eine einheitliche Kommunikationsbasis zwischen Juristen und Forensikern und ein übereinstimmendes Verständnis für digitale Spuren geschaffen werden. Auch muss sichergestellt werden, dass sich der IT-Sachverständige im Rahmen seiner vorgegebenen Grenzen bewegt. Diese bestehen sowohl in den Beweisfragen als auch in den Regeln der Grundrechtseingriffe für Strafverfolgungsbehörden. Letztlich haben die Auftraggeber im Rahmen ihrer Leitungspflicht dafür Sorge zu tragen, dass die Weisungsfreiheit und der dadurch bedingten freien Methodenwahl des IT-Sachverständigen insoweit eingeschränkt werden muss, dass dieser eine Untersuchungsmethode bzw. Datenanalysemethode anwenden muss, bei der die Funktionalität bekannt ist, wenn diese mindestens gleich geeignet ist wie andere Methoden, bei denen die Funktionalität nicht bekannt ist („Vorrang der Methodik mit bekannter Funktionalität“).

Die Untersuchung verdeutlicht den sehr starken Einfluss der IT-Sachverständigen auf die Entscheidungsfindung der Richter nach § 261 StPO. Dahingehend haben die anderen Verfahrensbeteiligten ihre prozessualen Einflussmöglichkeiten bzgl. der Wahrheitsermittlung in Anspruch zu nehmen. Die zur selbstständigen Entscheidung berufenen Richter haben sicherzustellen, dass

die Entscheidungsautorität bei ihnen liegt, das gilt v. a. im Hinblick auf juristische Schlussfolgerungen unter einen Tatbestand und die Offenlegung von Unsicherheiten bei der Bestimmung der Beweiskraft im Rahmen der tatrichterlichen Überzeugungsbildung. Um das gewährleisten zu können, sind die IT-Sachverständigen dazu angehalten, ihre Gutachten bzw. ihre Arbeitsunterlagen im Hinblick auf die syllogistische Struktur der Urteilsfindung so aufzubauen, dass sie die verschiedenen erarbeiteten Aussagekategorien, die Anknüpfungstatsachen, die Methodiken und ihre Richtigkeitswahrscheinlichkeiten sowie die Grundannahmen und die zugrundeliegenden Unsicherheiten aufschlüsseln und transparent machen. Zudem muss der Strafverteidigung eine umfassende Akteneinsicht zugestanden werden, um die Tatsachenermittlung bzgl. des Tatvorwurfs nachvollziehen und überprüfen zu können. Nicht zuletzt sollen sich die Strafverteidiger so optimal auf die Hauptverhandlung vorbereiten können, um ihr Frage- und Beweisantragsrecht in Anspruch nehmen zu können. Allerdings muss m. E. über eine Verteilung der (oft sehr hohen) Kostenrechnungen der Sachverständigengutachten in Anbetracht des Verhältnismäßigkeitsgrundsatzes und der Waffengleichheit nachgedacht werden.

Der Zweck der Bestellung eines Sachverständigen besteht darin, die mangelnde Sachkunde des Auftraggebers auszugleichen. Nur ein Auftrag, der die Erreichung dieses Zwecks anstrebt, vermag daher eine Sachverständigenposition zu begründen. Die Rolle des IT-Sachverständigen ist entscheidend von der Rolle des Zeugenbeweises abzugrenzen, insb. von Ermittlungspersonen. Vertieft soll in diesem Zusammenhang der aktuelle Diskurs in Bezug auf die Anforderungen an die Qualität der besonderen Sachkunde des IT-Sachverständigenbeweises in Strafverfahren berücksichtigt werden. Eine notwendige Abgrenzung ergibt sich sowohl aus den unterschiedlichen Rechten und Pflichten, die sich an die jeweilige Stellung der Beweisperson knüpfen, als auch aus weiteren Konsequenzen wie bspw. der Begründung eines Ablehnungsrechtes. Dabei kommt es immer auf den Einzelfall an und ist entscheidend vom Zweck der Beauftragung abhängig zu machen. Auch lässt sich die Sachverständigentätigkeit nicht pauschal kategorisieren und im Hinblick auf eine erforderliche Sachkunde beurteilen. Jedenfalls dürfte diese aber – auch aus Sicht der aktuellen Rechtsprechung und der Forensiker selbst – in den allermeisten Fällen bei der Auswertung von IT-Asservaten notwendig sein; nicht zuletzt, weil die forensische Informatik noch „in Kinderschuhen“ steckt, bisher nicht als standardisiert beurteilt werden kann und auch aufgrund der Besonderheit der Technologie in einem ständigen Wandel ist.

Im Ergebnis kann festgehalten werden – abgesehen von den Bedenken hinsichtlich der Kostenverteilung der Sachverständigengutachten –, dass bei der Tätigkeit des IT-Sachverständigen und auch im Umgang mit ihm als Beweismittel die verfahrensrechtlichen Vorschriften eingehalten werden können. Die

Verfahrensbeteiligten haben sich nur immer wieder auf ihre Rechte und Pflichten, die die StPO vorsieht, zu besinnen und diese ernst zu nehmen – besonders auf einem schwierig handhabbaren forensischen Gebiet.

B. Wie kann eine möglichst (hochwertige) objektive Tatsachengrundlage für die tatrichterliche Überzeugungsbildung i. S. d. § 261 StPO in Bezug auf den IT-Sachverständigenbeweis in einem Strafverfahren geschaffen werden?

Ziel des IT-Sachverständigen sollte es zunächst sein, gerichtsverwertbare Gutachten zu erarbeiten in Bezug auf die gestellten Beweisfragen. Dabei soll ein ordentlicher und (teilweise) standardisierter Aufbau der vorbereitenden schriftlichen Gutachten helfen. Bei der mündlichen Gutachtenerstattung vor Gericht spielen die Ausdrucksweise der Vernehmungsperson und der ihr zur Verfügung stehenden Visualisierungsmöglichkeiten eine wichtige Rolle.

Die Qualität der Gutachtenerstattung (ob schriftlich oder mündlich) hat dabei unmittelbaren Einfluss auf die Beweiskraft der dabei ermittelten (Indizien-)Tatsachen, die das Gericht zu bewerten und würdigen hat. Diese steigt mit Richtigkeitswahrscheinlichkeit und Nachvollziehbarkeit der angewendeten Methoden und produzierten Ergebnisse. In diesem Zusammenhang müssen die IT-Sachverständigen die jeweiligen Anknüpfungstatsachen, die verschiedenen Aussagekategorien, die verwendeten Datenverarbeitungs- und -analysemethoden bzw. Erfahrungssätze sowie die Richtigkeitswahrscheinlichkeiten, die Grundannahmen, die Anfangswahrscheinlichkeiten und die Unsicherheiten sichtbar machen. Dafür müssen die Methoden und Erfahrungssätze kategorisiert (deterministisch, statistisch, selbstlernend bzw. als Blackbox-Tool) und entsprechend in die Zuverlässigkeitsskala eingeordnet werden. Denn je nach Einordnung bestimmt sich daran anschließend der Einfluss der sachverständigen Ergebnisse und die Bindungswirkung auf die richterliche Überzeugungsbildung. Entscheidend ist hierbei einerseits die Aussagekraft und Bindungswirkung der Sachverständigenergebnisse, aber andererseits auch der Umstand, welche Beweisfunktion das präsentierte Ergebnis in der Sachverhaltsfeststellung einnimmt. Im Rahmen der Einordnung in die Zuverlässigkeitsskala ist auch die Einhaltung der Mindeststandards der forensischen Informatik wichtig und dies zu dokumentieren; denn daraus ergeben sich unmittelbare Folgen für das Beweisrecht – nämlich sowohl die Pflicht, diese im Rahmen der Beweiswürdigung (zumindest teilweise) zu berücksichtigen, als auch eine Indizienwirkung für die Richtigkeitswahrscheinlichkeit der Methodik bzw. der Erfahrungssätze und der dadurch gewonnenen Ergebnisse in Anbetracht der Bestimmung der Beweiskraft.

C. Wie sieht eine revisionssichere Beweiswürdigung des IT-Sachverständigenbeweises aus?

Angefangen von der Feststellung, ob eine rechtmäßige Auftragserstattung erfolgte, das Gutachten von einem unbefangenen, besonders fachkundigen Sachverständigen in zuverlässiger und vertrauenswürdiger Weise erstattet wurde und der Überprüfung des vom IT-Sachverständigen beschrittenen Weges (etwa seiner Methode, der angewandten Erfahrungssätze und Mittel, der Art der Tatsachengewinnung einschließlich der dabei vorgenommenen Beurteilung), bis hin zur kritischen Untersuchung der Ausführungen des Gutachtens und ggf. der Arbeitsunterlagen hat der Richter sich eine selbständige Meinung über die Beantwortung der Beweisfrage zu bilden.

Was in einem Strafverfahren als „Wahrheit" gelten darf, hängt von der Betrachtungsweise und Methodologie der Betrachtung ab. Gesichert ist jedenfalls, dass jenes tatsächliche Stück der Welt, auf das eine Verurteilung sich stützen muss, sowohl empirisch wahr als auch nach den jeweils geltenden Standards der empirischen Wissenschaften aufgeklärt ist. Das wiederum hat der Richter zu verantworten. Nach dem Wahrheitsbegriff von Seel ist die Wahrheit ein Produkt des Herstellungsprozesses, wobei die Richter ihre subjektive Gewissheit auch den Verfahrensbeteiligten, den Rechtsmittelgerichten und der Öffentlichkeit objektiv zugänglich zu machen haben – mithilfe der Regeln der praktischen Rationalität. Um vor der Rechtsordnung Bestand zu haben, muss die Würdigung vollständig sein, die allgemeinen Regeln schlussfolgernden Denkens müssen befolgt werden (wobei insb. die Einhaltung der Standards der forensischen Informatik Berücksichtigung finden soll) und die objektiven Elemente zur Bestimmung der persönlichen Gewissheit müssen intersubjektiv diskutierbar und nachvollziehbar gemacht werden. Bei der Bestimmung der objektiven Stärke der tatrichterlichen Überzeugung muss die Zuverlässigkeit der Tatsachengrundlage erörtert werden. Das gilt, weil es sich bei den Erfahrungssätzen und Methodiken der forensischen Informatik (noch) um „nicht gesicherte Standards" handelt. So muss v. a. auch bei der Frage der Be- und Verwertung des IT-Sachverständigenbeweises i. R. d. § 261 StPO die Tatsachengrundlage (wie die Anknüpfungstatsachen, die Anfangswahrscheinlichkeiten, die Grundannahmen), die daraus gezogenen Schlussfolgerungen und die darauf aufbauenden Hypothesen (in Bezug auf die Beantwortung der Beweisfragen) erörtert sowie die objektive Wahrscheinlichkeit der Richtigkeit dieser Hypothese bestimmt werden. Auch hier muss die Bestimmung der Überzeugungskraft der Ergebnisse der Sachverständigentätigkeit intersubjektiv diskutierbar und nachvollziehbar in den Urteilsgründen dargestellt werden.

Dabei kommt es also auf die Richtigkeitswahrscheinlichkeit der konkret angewendeten Erfahrungssätze und verwendeten Datenverarbeitungs- und

-analysemethoden an. Diese müssen zunächst genau benannt werden und können dann entsprechend der jeweiligen Kategorie (deterministische, statistische und selbstlernende Methoden) durch die Verfahrensbeteiligten in eine Zuverlässigkeitsskala eingeordnet werden: Als gesicherte wissenschaftliche Erkenntnisse; als wissenschaftliche Erkenntnis mit wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit, oder als (einfache) Erfahrungssätze zur Richtigkeitsbeurteilung bzw. unter keine Regeln zur Beurteilung der Richtigkeitswahrscheinlichkeit. Je nachdem muss das Gericht den IT-Sachverständigenaussagen folgen oder die Erkenntnisse sind für das Tatgericht eben nicht bindend. Im letzteren Fall muss das Tatgericht vielmehr die Wahrscheinlichkeitsaussage in seine Beweiswürdigung einbeziehen und die Richtigkeit der Aussage im jeweiligen Einzelfall anhand weiterer Indizien bestätigen oder widerlegen. In Fällen von Blackbox-Tools kann es auch sein, dass das Ergebnis des Datenbearbeitungsvorgangs keinen Beweiswert hat und nicht in die Beweiswürdigung einbezogen werden darf.

Dabei ist insbesondere die Pflicht zur Überprüfung und Würdigung der Einhaltung der Standards der forensischen Informatik (die Integrität und Authentizität von digitalen Spuren, die Mitteilung über (nicht) mögliche Schlussfolgerungen bzw. Fehlerquellen und die Einhaltung der verfahrensrechtlichen Grenzen) im Rahmen des § 261 StPO zu berücksichtigen. Auch die anderen Standards der forensischen Informatik dienen zudem als Indizien bei der Ermittlung der Beweiskraft des IT-Sachverständigenbeweises i. S. d. Beurteilung der Richtigkeitswahrscheinlichkeit der Datenverarbeitungsmethoden und Erfahrungssätze. Zukünftig werden so auch die Rechtsmittelgerichte verpflichtet, sich damit auseinanderzusetzen. Dadurch wird dazu beigetragen, dass die Methoden und Erfahrungssätze (zumindest teilweise) in Zukunft als standardisiert eingeschätzt werden könnten.

Auch haben die Gerichte die (über die der forensischen Informatik hinausgehenden) Besonderheiten der verschiedenen Aussagekategorien in ihrer Würdigung zu berücksichtigen und entsprechend auf die damit einhergehenden Eigenheiten einzugehen (bspw. Übernahme von Erfahrungssätzen, Grenze der rechtlichen Schlussfolgerung durch den IT-Sachverständigen oder die Beachtung der Erforderlichkeit der besonderen Sachkunde bei Wahrnehmungen).

Dreh- und Angelpunkt für die Würdigung der Objektivität des Gutachtens und die Einhaltung der Grenzen durch den IT-Sachverständigen dürfte die Leitungspflicht aus § 78 StPO und die Formulierung des Beweisthemas sein: Je genauer die Ausgestaltung der Auftragserteilung und der Leitung sowie deren Dokumentation in den Akten, desto besser ist die Überprüfbarkeit der ordnungsgemäßen sachverständigen Tätigkeit.

Die besondere Schwierigkeit der Beweiswürdigung besteht beim Sachverständigenbeweis darin, dass das Vorhandensein der Sachverständigen die Kette von Indizien bis hin zum Beweisthema verlängert. Zwar ermöglicht bzw. erleichtert der Sachverständige erst die Beweiswürdigung, da ein Indiz in der Kette nur vom Sachverständigen geschaffen wird (Befundtatsachen), oder nur er die erforderliche Sachkunde besitzt, um die Bedeutung des vorhandenen Indizes für das Beweisthema zu erfassen. Allerdings kommen auch die mit einem persönlichen Beweismittel verbundenen Probleme hinzu, die die Richter berücksichtigen müssen.

Nicht zuletzt hilft eine ganz allgemeine Sensibilisierung der zur Entscheidung berufenen Verfahrensbeteiligten über die IT-forensischen Schritte und Eigenschaften digitaler Spuren und deren Einfluss auf den Beweiswert. Eine Auseinandersetzung mit der forensischen Informatik schafft Grundlagenwissen; das geschieht regelmäßig schon durch eine enge Zusammenarbeit zwischen Juristen und IT-Sachverständigen, wie der gemeinsamen Formulierung der Beweisfragen und der weiteren Leitung und Würdigung der Tätigkeit i. S. v. §§ 78 und 261 StPO.

> „… If parties and investigative authorities choose to use the fruits of technology, they must also accept the need to prove the authenticity and integrity of the evidence produced by technology, even though the cost of such proof might be considered to be high. This is particularly the case where authentification evidence will shed light on the latent assumptions and hidden errors inherent in electronic evidence, which could affect the accuracy of the electronic evidence itself.“[1]

[1] *Mason/Seng*, Electronic Evidence, S. 48.

6. Teil

Ein Ausblick

Bei der Einführung neuer Technologien geht es selten linear zu, meistens greifen die Gesetze eines Lawinenabgangs: Erst passiert sehr lange sehr wenig, dann ganz schnell ganz viel. Das heißt, dass sich die Rechtspraxis unbedingt mit der Thematik der digitalen Beweismittel auseinandersetzen muss, auch mit dem vorausschauenden Blick auf zukünftige Technologien, um nicht immer der Hase im Wettlauf zu sein. Dabei gilt es dem Zitat „The justice system is known for many things, but efficiency is not one of them. Neither is being up-to-speed with technology. One joke goes that the unofficial IT slogan of the courts is, ‚Yesterday's technology, tomorrow!' "[1] endlich ein Ende zu bereiten.

Mit der umfassenden und zunehmenden Nutzung der Technologie im Alltag (sowohl durch die Strafverfolgungsbehörden als auch durch Kriminelle) wird die Bedeutung der forensischen Informatik und die Abhängigkeit von digitalen Beweismitteln weiter zunehmen. Daher ist es wichtig zu überlegen, wie diese forensische Disziplin so robust und zuverlässig wie möglich gestaltet werden kann.[2] Im Sinne von „any worthwile effort often requires the input of a community"[3] besteht v. a. auch ein Aufruf an die Forschung, daran mitzuwirken. Die IT-forensische und juristische Wissenschaft hat dabei die Aufgabe, weiter an wissenschaftlich gesicherten Erfahrungssätzen, an Studien über die Verteilung von Merkmalen in der Bevölkerung zur Quantifizierung der Irrtumswahrscheinlichkeiten bei Assoziationen im Rahmen der Rekonstruktion des Tathergangs in der forensischen Informatik, sowie an der Nachvollziehbarkeit und Standardisierung der verwendeten Techniken zu arbeiten. Aus juristischer Perspektive sollen dabei u. a. die Entwicklung der Standards der forensischen Informatik eng begleitet werden und deren Einhaltung überprüft werden.[4]

---

[1] In freier Übersetzung: Die Justiz ist für vieles bekannt, aber nicht für Effizienz und ebenso wenig dafür, technologisch aufgeschlossen zu sein. Ein Witz geht so: Der inoffizielle IT-Slogan der Gerichte ist: „Die Technologie von gestern ist gerade gut genug für morgen!", vgl. *Ewald*, Digitale Beweismittel und neue Wege der Strafverteidigung, S. 267 m. w. N.

[2] *Sunde/Dror*, Digital Investigation (2019) Vol. 29, S. 101.

[3] *Dubberley/Koenig/Murray*, Digital witness, Acknowledgements, xi.

[4] So passieren derzeit immer noch Fehler aufgrund fehlender wissenschaftlicher Daten, Forschung und Standards, *Sunde/Dror*, Digital Investigation (2019) Vol. 29, S. 101 m. w. N.

Die Befürchtung des immer größer werdenden Abhängigkeitsverhältnisses zu bestimmten Wissenschaftsgruppen, von denen einige den Anspruch erheben mögen, richterliche Aufgaben zu übernehmen, haben schon in der Zeit vor der StPO bestanden.[5] Dem kann jedoch einerseits durch die Vertreter der jeweiligen Wissenschaften entgegnet werden, indem sie eine derartige Zielsetzung weit von sich weisen.[6] Andererseits ist es die Aufgabe der zur Entscheidung berufenen Richter, die Entscheidungsautorität, -kompetenz und -verantwortung bei sich zu behalten.[7] Dabei haben v. a. die Richter und Staatsanwältinnen ihre Pflicht aus § 78 StPO ernst zu nehmen und die Tätigkeit des IT-Sachverständigen zu leiten (mit all den damit einhergehenden Ausprägungen).

Letztlich müssen sich die Auftraggeber ein erforderliches Mindestmaß an Grundkenntnissen auf dem Gebiet der forensischen Informatik aneignen, um den Gutachter sachgemäß auszuwählen, zu leiten und das Gutachten nachzuprüfen und zu würdigen. Entsprechendes gilt auch für die anderen Verfahrensbeteiligten. Aktuell fehlt es den Verfahrensbeteiligten in Strafverfahren u. a. an Wissen und Mut bzgl. digitaler Beweismittel.[8] Der interdisziplinäre Schnitt- und zugleich Knackpunkt in diesem Zusammenhang ist m. E. die „Kunst, die richtigen Fragen zu stellen".[9] Häufig werden nur „sichere" Fragen gestellt, bei denen die Antwort schon bekannt ist bzw. bereits vermutet wird. Aber die Fragen, die im Rahmen der Würdigung eines IT-Sachverständigenbeweises gestellt werden müssen, sollen dazu führen, dass die Stärken der ermittelten Befunde hervorgehoben oder aber auch die Schwachstellen aufgedeckt werden können, wie bspw. „bias" oder Unsicherheiten der angewendeten Software. Ausschließlich so können die sachverständigen bzw. richterli-

---

5 Vgl. so schon *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 49.

6 So z. B. *Cabanis*, NJW 1978, 2331: „Eine Richterrolle strebt aber gerade der seriöse Sachverständige nicht an"; oder „Kein Seinswissenschaftler sollte eine dem Richter auferlegte Verantwortung übernehmen"; *Gerchow*, in: FS-Schmidt-Leichner, S. 71: „Eben das ist die Position, die wir alle nicht wünschen"; *Karwat*, DRiZ 1972, 204: „Der gewissenhafte Sachverständige hat kein Interesse, selbst den Richter zu spielen"; *Langelüddeke/Bresser*, Gerichtliche Psychiatrie, S. 7: „Davon können wir uns nur nachdrücklich distanzieren"; *Leferenz*, Krim. Biol. Ggw.fragen, Heft 5, S. 1. (8): „Dass er sich im Allgemeinen nicht danach drängt, Verantwortung zu übernehmen, die nicht sein Fachgebiet, sondern juristische Bewertung betreffen"; *Leithoff*, Sachverständigengutachten, S. 48: „Wir berufsmäßigen Sachverständigen … sind froh, dass wir nach der Erstattung unseres Gutachtens die Entscheidung dem Gericht überlassen dürfen"; *Schwarz/Wille*, NJW 1971, 1061: „Wir respektieren vorbehaltlos die rein juristische Entscheidungskompetenz".

7 So auch der Appell von *Dippel*, Die Stellung des Sachverständigen im Strafprozess, S. 58 an die Strafrichter, eine Selbstentmachtung nicht zuzulassen bzw. rückgängig zu machen.

8 https://www.lto.de/recht/meinung/m/erst-wenn-die-strafjustiz-effektiver-arbeitet-kann-sie-mehr-personal-fordern-kommentar/ [29.6.2023].

9 *Browne/Keeley*, Asking the Right Questions, S. 17 ff.

chen Schlussfolgerungen transparent gemacht werden. Und nur auf dieser Basis kann eine „gute" Entscheidung fußen: „Move the conversation from the known to the unknown". So würde wohl auch Albert Einstein als „Cyberstrafverteidiger" die ersten 55 Minuten darüber nachdenken, welche Frage er an die IT-Sachverständige stellen soll, und nur fünf Minuten über ihre Antwort.[10]

[10] „Wenn ich eine Stunde Zeit hätte, um ein Problem zu lösen, würde ich 55 Minuten damit verbringen, über das Problem nachzudenken und fünf Minuten über die Lösung".

Literaturverzeichnis

Ahlf, Ernst-Heinrich: Zur Ablehnung des Vertreters von Behördengutachten durch den Beschuldigten im Strafverfahren, MDR 1978, S. 981 – 983

Ahrens, Hans-Jürgen: Der Beweis im Zivilprozess, Köln 2015

Albrecht, Peter-Alexis: Überzeugungsbildung und Sachverständigenbeweis in der neueren strafrechtlichen Judikatur zur freien Beweiswürdigung (§ 261 StPO), NStZ 1983, S. 486 – 492

Alpaydin, Ethem: Maschinelles Lernen, Berlin 2019

Alsberg, Max: Anm. zu RG JW 1929, S. 859 ff.

Alsberg, Max: Freie Ablehnbarkeit eines beantragten Sachverständigenbeweises im Strafprozess?, LZ 1915, S. 482 ff.

Alsberg, Max/*Nüse*, Karl/*Meyer*, Karlheinz: Der Beweisantrag im Strafprozess, 3. Auflage, Köln 1983 (zit.: Alsberg/Nüse/Meyer-*Bearbeiter*, Der Beweisantrag im Strafprozess)

Anderson, Terence/*Schum*, David/*Twining*, William: Analysis of Evidence, 2. Auflage, London 2010

Arab-Zadeh, Amir: Des Richters eigene Sachkunde und das Gutachterproblem im Strafprozess, NJW 1970, S. 1214 ff.

Arndt, Adolf: Der Fall Rohrbach als Mahnung, NJW 1962, S. 25 ff.

Artkämper, Heiko/*Artkämper*, Leif Gerrit: Kriminaltechnische und rechtsmedizinische Untersuchungen. Möglichkeiten und Mythen; Fakten, Fehler und Beweiswerte, Kriminalistik 2018, S. 384 ff.

Arzt, Gunther: Anmerkung zu BGH v. 6.9.1968 – Az. 4 StR 339/68, JZ 1969, S. 438 ff.

Bäcker, Matthias/*Freiling*, Felix/*Schmitt*, Sven: Selektion von der Sicherung – Methoden zur effizienten forensischen Sicherung von digitalen Speichermedien, Datenschutz und Datensicherheit – DuD (2010) Vol. 34, S. 80 ff.

Barton, Stephan: Der psychowissenschaftliche Sachverständige im Strafverfahren, Heidelberg 1983 (zit.: *Barton*, Der psychowissenschaftliche Sachverständige)

Basar, Eren/*Hiéramente*, Mayeul: Datenbeschlagnahme in Wirtschaftsstrafverfahren und die Frage der Datenlöschung, NStZ 2018, S. 68 ff.

Baur, Alexander: Die tatrichterliche Überzeugung, Überlegungen zu ihrer Bedeutung und revisionsgerichtlichen Prüfbarkeit, ZIS 2019, S. 119 ff.

Baur, Hanno/*Schmid*, Viola (Hrsg.): Studienarbeit von cand. Wirtsch. Inf. Hanno Baur: Zur „Beweiskraft informationstechnologischer Expertise“, TU Darmstadt (Stand: 6/2010)

Bayerlein, Walter: Praxishandbuch Sachverständigenrecht, 5. Auflage, München 2015

Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf, Jürgen (Hrsg.), 41. Edition, Stand: 01.10.2021, München 2021

Beling, Ernst: Deutsches Reichsstrafprozessrecht, Berlin 1928

Bender, Rolf/*Nack*, Armin/*Treuer*, Wolf-Dieter: Tatsachenfeststellung vor Gericht, 4. Auflage, München 2014

Benecke, Mark: Genetischer Fingerabdruck, – Enzyklopädie Naturwissenschaft und Technik, 2. Auflage 6. Ergänzungslieferung, 2001

Bennecke, Hans/*Beling*, Ernst: Lehrbuch des Deutschen Reichs-Strafprozessrechts, Breslau 1900 (zit.: *Bennecke/Beling*, Lehrbuch des Deutschen Reichs-Strafprozessrechts)

Beukelmann, Stephan: Outsourcing bei Polizei und Strafjustiz, NJW-Spezial 2008, S. 280 ff.

Beulke, Werner/*Swoboda*, Sabine: Strafprozessrecht, 14. Auflage, Heidelberg 2018 (zit.: *Beulke/Swoboda*, Strafprozessrecht)

Biasiotti, Solanke: Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining, KI – Künstliche Intelligenz (2022) Vol. 36 S. 143 – 161

Billard, David/*Hauri*, Rolf: Making sense of unstructured flash-memory dumps, ACM New York 2010

Binding, Karl: Grundriss des Deutschen Strafprozessrechts, 5. Auflage, Leipzig 1904

Birkmeyer, Karl: Deutsches Strafprozessrecht, Berlin 1898

Birnbaum, Johann: Über den Beruf der Sachverständigen im Criminalprozeß, Neues Archiv des Criminalrechts, Band 14, Teil 2, S. 182 ff.

Bittmann, Folker: Rechtsfragen um den Einsatz des Wirtschaftsreferenten, wistra 2011, S. 47 ff.

Blau, Günter: Der Strafrechtler Psychologischer Sachverständiger, ZStW 78 (1966), S. 153 ff.

Blechschmitt, Lisa: Strafverfolgung im digitalen Zeitalter – Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018, S. 361 ff.

Bleutge, Peter: Besondere Sachkunde, DS 2007, S. 65 ff.

Bleutge, Peter: Der öffentlich bestellte Sachverständige, DRiZ 1977, 170, S. 172 ff.

Bleutge, Peter: Die Hilfskräfte des Sachverständigen – Mitarbeiter ohne Verantwortung? NJW 1985, S. 1185 ff.

Bleutge, Peter: Sachverständigenrecht: Themenfelder gestern, heute und morgen Keine Realisierung von Visionen, Verharren im alten Trott? Der Bausachverständige Sonderheft (2015), S. 10 ff. (zit.: *Bleutge*, Sachverständigenrecht)

Blomeyer, Jürgen: Die Revisibilität von Verfahrensfehlern im Strafprozess (Kausalität und Finalität im Revisionsrecht), JR 1971, S. 144 ff.

Bockelmann, Paul: Strafrichter und psychologischer Sachverständiger, GA 1955, S. 327 ff.

Böhme, Albrecht: Zum Begriff der Überzeugung beim Urteil, DRiZ 1960, S. 20 ff.

Boetticher, Axel/*Kröber*, Hans-Ludwig/*Müller-Isberner*, Rüdiger/*Böhm*, Klaus M.: Mindestanforderungen für Prognosegutachten, NStZ 2006, S. 537 – 544

Boetticher, Axel/*Nedopil*, Norbert/*Bosinski*, Hartmut/*Saß*, Henning: Mindestanforderungen für Schuldfähigkeitsgutachten, NStZ 2005, S. 57 – 62

Bohne, Gotthold: Zur Psychologie der richterlichen Überzeugungsbildung, Darmstadt 1948 (Neudruck 1967)

Bork, W.-R./*Stein*, S./*El-Khadra-Klut*, N./*Fritsch*, R.: Richtlinie zur Qualitätssicherung bei forensisch-chemischen Untersuchungen von Betäubungs- und Arzneimitteln, Toxichem Krimtech 87 (2020), S. 35 – 76

Brammsen, Joerg: Der abgelehnte vorbefasste Privatgutachter – zweierlei Maß im Strafprozess? ZStW 119 (2007) Heft 1, S. 93 ff.

Braun, Frank/*Roggenkamp*, Jan: Privatisierung technisch gestützter Ermittlungsmaßnahmen? Neue Kriminalpolitik, 2012, Vol. 24, S. 141 ff.

Bremer, Heinz: Der Sachverständige, 2. Auflage, Heidelberg 1973

Brodowski, Dominik: Bitcoins und Verfall; Ausspähen von Daten; Datenveränderung, StV 2019 (Heft 6), S. 385 ff.

Brodowski, Dominik: Die Beweisführung mit digitalen Spuren und das Unmittelbarkeitsprinzip, in: Buschmann/Almuth, Gläß/Anne-Christin, Gonska/Hans-Henning, Philipp/Markus, Zimmermann/Ralph (Hrsg.): Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, Berlin 2018, S. 83 ff.

Browne, M. Neil/*Keeley*, Stuart M.: Asking the Right Questions, Harlow 2015

Bruns, Hans-Jürgen: Leitfaden des Strafzumessungsrechts, Eine systematische Darstellung für die strafrichterliche Praxis, München 1971 (zit.: *Bruns*, Leitfaden)

Burcher, Morgan: Social Network Analysis and Law Enforcement – Applications for Intelligence Analysis, London 2020.

Butler, Andrew/*Choo*, Kim-Kwang Raymond: IT standards and guides do not adequately prepare IT practitioners to appear as expert witnesses: An Australian perspective, Security Journal (2016) Vol. 29, S. 306 ff.

Cabanis, Detlef: Glaubwürdigkeitsgutachten, NJW 1978, S. 2329 ff.

Carrier, Brian: File System Forensic Analysis, London 2005

Carrier, Brian/*Spafford*, Eugene: Getting Physical with Digital Investigation Process, Journal of Digital Evidence (2003) Vol. 2, S. 177 ff.

Carvey, Harlan/*Altheide*, Cory: Tracking USB storage: Analysis of windows artifcats generated by USB storage devices, Digital Investigation (2005) Vol. 2, S. 94 ff.

Casey, Eoghan: Digital Evidence and Computer Crime – Forensic Science, Computers, and the Internet, London 2004, 2011, 2016 (zit.: *Casey*, Digital Evidence and Computer Crime)

Casey, Eoghan: The chequered past and risky future of digital forensics, Forensic Science 2019 Vol. 6, S. 649 – 664

Casino, Fran/*Dasaklis*, Thomas/*Spathoulas*, Georgios/*Anagnostopoulos*, Marios/*Ghostal*, Amrita/*Borocz*, Istvan/*Solanas*, Agusti/*Conti*, Mauro/*Patsakis*, Constantinos: Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews, IEEE Access (2022) Vol. 10, Nr. 25468 ff.

Cleve, Jürgen/*Lämmel*, Uwe: Data Mining, 3. Auflage, Berlin 2020

Coglianese, Cary/*Lehr*, David: Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, The Georgetown Law Journal 2017, Vol. 105, S. 1147 ff.

Cramer, Steffen: Anmerkungen zu § 81f Abs. 2 S. 3 StPO – Geheimhaltungsschutz und Gutachtenverweigerung, NStZ 1998, S. 498 ff.

Crefeld, Wolf: Bedarf es einer Ethik des Sachverständigen? Ein Plädoyer, den „objektiven" durch den ärztlich engagierten Sachverständigen zu ersetzen, R&P 1994, S. 102 ff.

Dahs, Hans: Handbuch des Strafverteidigers, 8. Auflage, Köln 2015

Dahs, Hans/*Dahs*, Hans: Die Revision im Strafprozess, 5. Auflage, München 1993 (zit.: *Dahs/Dahs*, Revision)

Dästner, Christian: Zur Anwendbarkeit des § 74 StPO auf Polizeibeamte als Sachverständige, MDR 1979, S. 545 ff.

De Arcos Tejerizo, María: Digital evidence and fair trial rights at the International Criminal Court, Leiden Journal of International Law (2023), S. 1 ff.

Den Hartog, J. D.: The case law of the European Court of Human Rights regarding the use of expert Statements in criminal procedures, in: Nijboer, J. F./Callen, C. R./Kwak N. (Hrsg.): Forensic expertise and the law of evidence, Amsterdam 1993, S. 148 ff.

Deppenkemper, Gunter: Beweiswürdigung als Mittel prozessualer Wahrheitserkenntnis – Eine dogmengeschichtliche Studie zu Freiheit, Grenzen und revisionsgerichtlicher Kontrolle tatgerichtlicher Überzeugungsbildung (§ 261 StPO, § 286 ZPO), Göttingen 2004

Detter, Klaus: Der Sachverständige im Strafverfahren – eine Bestandsaufnahme, NStZ 1998, S. 57 ff.

Detter, Klaus: Der von der Verteidigung geladene psychiatrische Sachverständige – Konfliktverteidigung oder Ohnmacht der Tatgerichte? Festschrift für Lutz Meyer-Goßner, München 2001, S. 431 ff.

Deuber, Dominic/*Gruber*, Jan/*Humml*, Merlin/*Ronge*, Viktoria/*Scheler*, Nicole: Argumentation Schemes for Blockchain Deanonymization, presented on JURISIN 2022, https://doi.org/10.48550/arXiv.2305.16883

Deuber, Dominic/*Ronge*, Viktoria/*Rückert*, Christian: SoK: Assumptions Underlying Cryptocurrency Deanonymizations Proceedings on Privacy Enhancing Technologies (2022), Vol. 3, S. 670 – 691

Dewald, Andreas/*Freiling*, Felix: Forensische Informatik, 2. Auflage, Norderstedt 2015

Dierlamm, Alfred: Das rechtliche Gehör vor der Auswahl eines Sachverständigen im Ermittlungsverfahren. Festschrift von Egon Müller, Baden-Baden 2008, S. 117 ff.

Dilcher, Hermann: Der Beweis durch Sachverständige in der Geschichte, Der öffentlich bestellte und vereidigte Sachverstände, 1975 (zit.: *Dilcher*, Der Beweis durch Sachverständige)

Dippel, Karlhans: Ausgewählte Themen des Beweises durch Sachverständige im Strafverfahren. Festschrift für Egon Müller, Baden-Baden, S. 125 ff.

Dippel, Karlhans: Die Stellung des Sachverständigen im Strafprozess – Eine Studie unter besonderer Berücksichtigung der Zulässigkeit und der Folgen eigener Ermittlungen des Sachverständigen nach geltendem und künftigem Recht, Heidelberg 1986 (zit.: *Dippel*, Die Stellung des Sachverständigen im Strafprozess)

Ditzen, Wilhelm: Über Zeugenbeweisanträge im Strafverfahren, ZStW 10 (1890), S. 111 ff.

Dodge, Alexa: The digital witness: The role of digital evidence in criminal justice responses to sexual violence, Feminist Theory, 2018, Vol. 10 (3), S. 303 ff.

Dohna, Alexander Graf zu: Strafprozessrecht, 3. Auflage, 1929

Döhring, Erich: Fachliche Kenntnisse des Richters und ihre Verwertung im Prozess, Zugleich eine Besprechung des BGH-Urteils v. 22.3.1967, JZ 1968, S. 642 ff.

Dölp, Michael: Der Sachverständige im Strafprozess: Gedanken über eine nachhaltige strukturelle Veränderung im Verfahrensrecht, Zeitschrift für Rechtspolitik (2004) Vol. 7, S. 235 – 237

Dose, Norbert: Der Sitzungsvertreter und der Wirtschaftsreferent der Staatsanwaltschaft als Zeuge in der Hauptverhandlung, NJW 1978, S. 349 ff.

Dressel, Julia/*Farid*, Hany: The accuracy, fairness, and limits of predicting recidivism, Science Advances, Vol. 4 2018, S. 1 ff.

Drösser, Christoph: Total Berechenbar? Wenn Algorithmen entscheiden, 2. Auflage, München 2019

Dror, Itiel: The bias snowball and the bias cascade effects: Two distinct biases that may impact forensic decision making, Journal of Forensic Science (2017) Vol. 62

Dror, Itiel: The Error in „Error Rate“: Why Error Rates Are So Needed, Yet So Elusive, Journal of Forensic Sciences (2020)

Dror, Itiel: The paradox of human expertise: why experts can get it wrong. In: Kapur, N. (Hrsg.) The paradoxical brain. Cambridge University Press, 2011 Cambridge, S. 177 ff.

Dubberly, Sam/*Koenig*, Alexa/*Murrey*, Daragh: Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, Oxford 2020

Ehrenzweig, Albert: Die freie Überzeugung des Richters, JW 1929, S. 85 ff.

Eisenberg, Ulrich: Beweisrecht der StPO (Spezialkommentar), 9. Auflage, München 2015 (zit.: *Eisenberg*, Beweisrecht der StPO)

Eisenberg, Ulrich: Zur Ablehnung des Sachverständigen im Strafverfahren wegen Besorgnis der Befangenheit, NStZ 2006, S. 368 ff.

Eisenmenger, Wolfgang: Ärztliches Strafrecht: Kompetenz des Rechtsmediziners im Strafverfahren in 25 Jahre Arbeitsgemeinschaft – 25 Jahre Arzthaftung (2011), S. 49 ff.

Engisch, Karl: Logische Studien zur Gesetzanwendung, Sitzungsberichte der Heidelberger Akademie der Wissenschaft, 3. Aufl. Heidelberg 1963 (zit.: *Engisch*, Logische Studien)

Erb, Volker: Die Abhängigkeit des Richters vom Sachverständigen, ZStW 121 (2009), S. 883 ff.

Ernst, Christian: Der Grundsatz digitaler Souveränität, Eine Untersuchung zur Zulässigkeit des Einbindens privater IT-Dienstleister in die Aufgabenwahrnehmung der öffentlichen Verwaltung, Berlin 2020

Etter, Eberhard: Der polizeiliche EDV-Sachverständige im Strafverfahren, CR 1986, S. 166 ff.

Ewald, Uwe: Digitale Beweismittel und neue Wege der Strafverteidigung – Welche Herausforderungen stellt die Ausweitung informationstechnologischer Überwachungs- und Ermittlungsmethoden an die Strafverteidigung? Strafverteidigertag (2018), S. 267 ff.

Ewald, Uwe: Reason and Truth in international criminal justice – a criminological perspective on the construction of evidence in international trials, in: Smeulers, Alette/ Haveman, Roelof (Hrsg.), Supranational Criminology: Towards a Criminology of International Crimes, Portland 2008, S. 399 ff.

Fährmann, Jan: Digitale Beweismittel und Datenmengen im Strafprozess – Digitalisierung als rechtsstaatliche Herausforderung an Justiz, Polizei und Gesetzgeber, MMR 2020, S. 228 – 233

Falck, Ernst: Der technische Sachverständige im Strafprozess, JR 1955, S. 286 ff.

Farthofer, Hilde: Der Sachverständige und der Verrat von Wirtschaftsgeheimnissen, HRRS (7/2021), S. 313 ff.

Ferguson, Andrew: The Rise of Big Data Policing – Surveillance, Race, and the Future of Law Enforcement, New York 2017

Fezer, Gerhard: Die erweiterte Revision – Legitimierung der Rechtswirklichkeit? Tübingen 1974 (zit.: *Fezer*, Revision)

Fezer, Gerhard: Die Folgen der Sachverständigenablehnung für die Verwertung seiner Wahrnehmungen, JR 1990, S. 397 ff.

Fezer, Gerhard: Möglichkeiten einer Reform der Revision in Strafsachen, Tübingen 1975 (zit.: *Fezer*, Möglichkeiten)

Fezer, Gerhard: Strafprozessrecht, 2. Aufl., München 1995 (zit.: *Fezer*, Strafprozessrecht)

Fezer, Gerhard: Tatrichterlicher Erkenntnisprozess – „Freiheit" der Beweiswürdigung, StV 1995, S. 95 ff.

Fincke, Martin: Die Pflicht des Sachverständigen zur Belehrung des Beschuldigten, ZStW 86 (1974), S. 656 ff.

Flaglien, Anders: The Digital Forensics Process, in: Flaglien, Anders/Sunde, Inger/Dilijonaite, Ausra/Hamm, Jeff/Petter, Jens (Hrsg.), Digital Forensics (2017), S. 13 ff.

Foerster, Klaus/*Dreßing*, Harald: Die Erstattung des Gutachtens (Kapitel 5), in: Dreßing, Harald/Habermeyer, Elmar (Hrsg.): Psychiatrische Begutachtung – Ein praktisches Handbuch für Ärzte und Juristen, 6. Aufl., München 2015, S. 62 – 69

Foth, Eberhard/*Karcher*, Walter: Überlegungen zur Behandlung des Sachbeweises im Strafverfahren, NStZ 1989, S. 166 ff.

Frank, Robert: Quality measurements of digital forensics analysis reports, Masterarbeit; Lehrstuhl für Informatik 1, (bei Freiling, Felix/Sack, Konstantin), 2018

Freeman, Lindsay: Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials, Fordham International Law Journal (2018) Vol. 41, Issue 2, S. 283 ff.

Freiling, Felix/*Gruhn*, Michael: What is Essential in Digital Forensic Analysis? IMF (2015), S. 40 ff.

Frielinghaus, Volker: Über psychodynamische Einwirkungen auf juristische Denk- und Interpretationsmechanismen, Vorgänge (1971) Vol. 5, S 163 ff.

Freiling, Felix/*Hösch*, Leonhard: Controlled experiments in digital evidence tampering, Digital Investigation 24S (2018), S. 83 ff.

Freiling, Felix/*Schwittay*, Bastian: A Common Process Model for Incident Response and Computer Forensics, in: Frings, Sara/Göbel, Oliver/Günther, Detlef/Hase, Hardo/Nedon, Jens/Schadt, Drik/Brömme, Arslan (Hrsg.): IT-Incidents Management & IT-Forensics – IMF 2007 Stuttgart, S. 19 ff.

Frenken, J.: Glanz und Elend der Gerichtssachverständigen, DRiZ 1957, S. 169 ff.

Frenken, J.: Kritische Betrachtungen über Sachverständigengutachten als Urteilsgrundlage, DAR 1956, S. 291 ff.

Friederichs, Helmut: Sachverständigengruppe und ihr Leiter – Fortentwicklung des Sachverständigenbeweisrechts? Zugleich eine Stellungnahme zu BGHSt 22, 268, JZ 1974, S. 257 ff.

Fröwis, Michael/*Gottschalk*, Thilo/*Haslhofer*, Bernhard/*Rückert*, Christian/*Pesch*, Paulina: Safeguarding the evidential value of forensic cryptocurrency investigations, Forensic Science International: Digital Investigation (2020) Vol. 33, Nr. 200902 ff.

Gabriel, Peter/*Huckenbeck*, Wolfgang/*Kürpiers*, Frank: Über die Fragwürdigkeit der Berechnung einer Identitätswahrscheinlichkeit in anthropologischen Gutachten, NZV 2014, S. 346 – 349.

Galloway, Scott: the four – Die geheime DNA von Amazon, Apple, Facebook und Google, 4. Aufl., Kulmbach 2023

Garfinkel, Simson: Digital forensics research: The next 10 years, Digital Investigation (2010), Vol. 7, S. 64 ff.

Garfinkel, Simson: Digital Forensics Research: The Next 10 Years, DFRWS 2010

Garfinkel, Simson/*Farrell*, Paul/*Roussev*, Vassil/*Dinolt*, George: Bringing science to digital forensics with standardized forensic corpora, Digital Investigation (2009) Vol. 6, S. 3 ff.

Garrett, Brandon: Autopsy of a crime lab – Exposing flaws in forensics, Oakland 2021

Gebauer, Gerhard: Das versorgungsärztliche Gutachten im sozialgerichtlichen Verfahren, MedSachv. 53 (1957), S. 30 ff.

Gebhard, Angelina/*Michalke*, Reinhart: Der Zweck heiligt die Mittel nicht – Der EncroChat-Komplex und die Grenzen strafprozessualer Beweisverwertung, NJW 2022, S. 655 – 659

Geerds, Friedrich: Juristische Probleme des Sachverständigenbeweises, ArchKrim 137 (1966), S. 61 ff.

Gehm, Matthias: Problemfeld Schätzung im Steuer- und Steuerstrafverfahren, NZWiSt 2012, S. 408 ff.

Gerchow, Joachim: Der Sachverständigenbeweis aus rechtsmedizinischer Sicht, in: Festschrift für Erich Schmidt-Leichner zum 65. Geburtstag, München 1977, S. 67 ff.

Gerchow, Joachim: Bemerkungen zur sog. Krise des Sachverständigenbeweises, in: Gerichtliche Medizin und Kriminalistik, Festschrift zum 60. Geburtstag von Emil Weinig, Lübeck 1964, S. 48 ff.

Gerchow, Joachim: Bemerkungen zur sog. Krise des Sachverständigenbeweises, Arch. Krim. 134 (1964), S. 125 ff.

Gercke, Björn/*Leimenstoll*, Ulrich/*Stirner*, Kerstin (Hrsg.): Hdb. Medizinstrafrecht, 1. Aufl., Hürth 2020, Rn. 1629 ff.

Gercke, Björn/*Wollenschläger*, Sebastian: Videoaufzeichnungen und digitale Daten als Grundlage des Urteils – Revisionsrechtliche Kontrolle in den Grenzen des Rekonstruktionsverbots, StV 2013, S. 106 ff.

Gerland, Heinrich: Der deutsche Strafprozess, Mannheim 1927

Geschonneck, Alexander: Computer Forensik – Computerstraftaten erkennen, ermitteln, aufklären, 6. Aufl. Heidelberg 2014

Gigerenzer, Gerd/*Todd*, Peter: Simple heuristics that make us smart, ABC Research Group (2000) Vol. 23, S. 727 ff.

Girnth, Joachim: Der Augenscheinsmittler und seine Einordnung in die Beweismittel des Strengbeweises, Bonn 1997 (zit.: *Girnth*, Der Augenscheinsmittler)

Glaser, Julius: Beiträge zur Lehre vom Beweis im Strafprozess, Leipzig 1883 (zit.: *Glaser*, Beiträge)

Glaser, Julius: Handbuch des Strafprozesses, Bd. 1, Leipzig 1883 (zit.: *Glaser*, Handbuch)

Gless, Sabine: AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials Georgetown Journal of International Law 2020, Vol. 51, No. 2, S. 195 ff.

Gönner, Nikolaus: Handbuch des deutschen gemeinen Prozesses Bd. 2, Erlangen 1801

Göppinger, Hans: Das Gutachten, in: Göppinger, Hans/Witter, Hermann (Hrsg.), Handbuch der forensischen Psychiatrie Bd. 2, Berlin 1972, S. 1532 ff.

Gössel, Karl: Behörden und Behördenangehörige als Sachverständige vor Gericht, DRiZ 1980, S. 363 ff.

Gössel, Karl: Strafverfahrensrecht, Stuttgart 1977

Goldschmidt, James: Der Prozess als Rechtslage, Berlin 1925

Gollmann, Dieter: Computer Security, 3. Aufl. Sabonn 2011

Gollwitzer, Walter: Behördengutachter in der Hauptverhandlung des Strafprozesses. Festschrift für Walther Weißauer, Heidelberg 1986, S. 23 ff.

Grimm, Paul/*Grossman*, Maura/*Cormack*, Gordon: Artificial Intelligence as Evidence, 19 NW. J. TECH. & INTELL. PROP. 9 (2021), S. 1 ff.

Grolman, Karl: Theorie des gerichtlichen Verfahrens, 3. Aufl., Darmstadt 1810

Gross, Hans/*Geerds*, Friedrich: Handbuch der Kriminalistik Bd. 1, 1977

Gschwind, M./*Peterson*, F./*Rautenberg*, E.: Die Beurteilung psychiatrischer Gutachten im Strafprozess, Stuttgart 1982

Gutmann, Alexander: Die Aufklärungspflicht des Gerichts und der Beweiserhebungsanspruch der „Parteien" im Strafprozess, JuS 1962, S. 369 ff.

Haddenbrock, Siegfried: Der Psychiater im Strafprozess, DRiZ 1974, S. 37 ff.

Hahn, Carl: Die gesamten Materialien zur Strafprozessordnung, 3. Bd. (Mat. zur StPO), 1. Abteilung, Berlin 1880

Hamm, Rainer: Die Revision in Strafsachen, 7. Aufl., Berlin 2010

Hanack, Ernst-Walter: Die Rechtsprechung des BGH zum Strafverfahrensrecht, JZ 1972, S. 114 ff.

Hanack, Ernst-Walter: Zur Austauschbarkeit von Beweismitteln im Strafprozess, JZ 1970, S. 561 ff.

Hare, Eric/*Hofmann*, Heike/*Carriquiry*, Alicia: Algorithmic approaches to match degraded land impressions, Law, Probability and Risk 2017, Vol. 16, Nr. 4, S. 203 ff.

Harms, Sven: Das Augenscheinsersatzobjekt im Strafprozess, Hamburg 2006

Harrington, Sean: Collaborating with a digital forensics expert: Ultimate tag-team or disastrous duo? William Mitchell Law Review, (2011) Vol 38, S. 353 ff.

Hartley, Stephanie/*Winburn*, Allysha: hierarchy of expert performance as applied to forensic anthropology, Journal of forensic science, (2021) Vol. 66, S. 1 ff.

Hartmann, Hans/*Rubach*, Walter: Verteidiger und Sachverständiger – Eine Falldarstellung, StV 1990, S. 425 ff.

Hassemer, Winfried: Einführung in die Grundlagen des Strafrechts, München 1990 (zit.: *Hassemer*, Grundlagen des Strafrechts)

Hassemer, Winfried: Grenzen des Wissens im Strafprozess. Neuvermessung durch die empirischen Wissenschaften vom Menschen? ZStW 121 (2009), S. 830 ff.

Hauber, Rudolf: Die Funktionsverteilung zwischen Richtern und Sachverständigen im deutschen Jugendgerichtsverfahren, Zugleich ein Beitrag zur Gestaltung einer künftigen Jugendgerichtsverfassung, Diss. Freiburg 1976 (zit.: *Hauber*, Die Funktionsverteilung zwischen Richtern und Sachverständigen)

Hauer, Judith: Anmerkungen und Gedanken zum Fall Mollath – Verschwörung oder Gleichgültigkeit? ZRP 2013, S. 209 ff.

Heger, Martin/*Pohlreich*, Erol: Strafprozessrecht, 2. Auflage, Stuttgart 2018

Hegler, August: Die Unterscheidung des Sachverständigen vom Zeugen im Strafprozess, AcP 104 (1909), S. 151 ff.

Heinson, Dennis: IT-Forensik – Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen, Tübingen 2015 (zit.: *Heinson*, IT-Forensik)

Hellmann, Uwe: Strafprozessrecht, 2. Auflage, Berlin 2006

Henke, Matthias Felix: Zur Darstellung von DNA-Gutachten im Strafurteil, NStZ 2023, S. 13 ff.

Henkel, Heinrich: Strafverfahrensrecht, 2. Auflage, Stuttgart 1968

Hepner, Walter: Richter und Sachverständiger, Kriminologische Schriftenreihe (Band 21); Herausgeber Mergen, Armand, Hamburg 1966 (zit.: *Hepner*, Richter und Sachverständiger)

Herdegen, Gerhard: Bemerkungen zur Beweiswürdigung, NStZ 1987, S. 196; StV 1992, S. 531; NStZ 1999, S. 177; NJW 2003, S. 3515 ff.

Herdegen, Gerhard: Die strafprozessualen Beweiswürdigungstheorien des BGH, in: Festschrift für Ernst-Walter Hanack, Berlin 1999, S. 311 ff.

Herdegen, Gerhard: Was ist unter „Beweiswürdigung" i. S. v. § 261 StPO zu verstehen?, in: Festschrift für Ulrich Eisenberg zum 70. Geburtstag, München 2009, S. 527 ff.

Hess, Marie-Theres: Digitale Technologien und freie Beweiswürdigung – Eine Untersuchung der Einflüsse von technologie-gestützten Beweisen und Legal-Tech-Anwendungen auf die Sachverhaltsfeststellung im Strafprozess, Baden-Baden 2024 (zit.: *Hess*, Digitale Technologien und freie Beweiswürdigung)

Hetzer, Wolfgang: Wahrheitsfindung im Strafprozess unter Mitwirkung psychiatrisch/psychologischer Sachverständiger, Schriften zum Strafrecht, Bd. 49, Berlin 1982

Hippel, von Robert: Lehrbuch des Strafrechts, Berlin 1932

Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, 57. Auflage, München 2022

Hoppen, Peter/*Streitz*, Siegfried: Die Tätigkeit des IT-Sachverständigen, CR 2007 Heft 4, S. 270 ff.

Horsman, G.: ‚I couldn't find it your honor, it mustn't be there!' – tool errors, tool limitations and user errors in digital forensics, Science Justice 2018, S. 433 – 440

Hughes, Nicolas/*Karabiyik*, Umit: Towards reliable digital forensics investigations through measurement science, WIREs Forensic Science 2020 (Vol. 2), S. 1364 – 1374

Jackson, Rhiannon/*McAreavey*, Maria: Black-box Medicine: protecting patient privacy without preventing innovation, Retskraft – Copenhagen Journal of Legal Studies (2019) Vol. 3, S. 1 ff.

Jähnke, Burkhard: Über die Befugnis des Revisionsgerichts zur Nachprüfung der tatrichterlichen Beweiswürdigung, in: Festschrift für Ernst-Walter Hanack, Berlin 1999, S. 355 ff.

Jahn, Matthias/*Brodowski*, Dominik: Digitale Beweismittel im deutschen Strafprozess – Ermittlungsverfahren, Hauptverhandlung und Revision, in: Hoven, Elisa, Kudlich, Hans (Hrsg.), Digitalisierung und Strafverfahren, Baden-Baden 2020, S. 67 ff.

Jahn, Matthias/*Brodowski*, Dominik: Digitale Beweismittel in strafprozessualer Hauptverhandlung und Revision, in: Hecker, Bernd, Weißer, Bettina, Brand, Christian (Hrsg.), Festschrift für Rudolf Rengier zum 70. Geburtstag, München 2018, S. 409 ff.

Jansen, Dennis: Technische Möglichkeiten und Risiken zur Beweissicherung bei Webseiten, CR 2018, S. 334 ff.

Jansen, Gabriele: Überprüfung aussagepsychologischer Gutachten, StV 2000, S. 224 – 229

Jansen, Gabriele: Zeuge und Aussagepsychologie, 2. Auflage, Heidelberg 2012

Jessnitzer, Kurt: Der gerichtliche Sachverständige, 5. Auflage, Berlin 1975 (zit.: *Jessnitzer*, Der gerichtliche Sachverständige)

Jessnitzer, Kurt: Strafverteidiger und Sachverständiger, StV 1982, S. 177 ff.

Jessnitzer, Kurt/*Frieling*, Günter: Der gerichtliche Sachverständige – ein Handbuch für die Praxis, 10. Aufl., Köln 1992 (zit.: *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige)

Jessnitzer, Kurt/*Ulrich*, Jürgen: Der gerichtliche Sachverständige – ein Handbuch für die Praxis, 11. Aufl., Köln 2001 (zit.: *Jessnitzer/Ulrich*, Der gerichtliche Sachverständige)

Jones, Andrew/*Vidalis*, Stilianos: Rethinking Digital Forensics, Annals of Emerging Technologies in Computing (AETiC) 2019 (Vol. 3), S. 41 – 52

Jung, Heike: Über die Wahrheit und ihre institutionellen Garanten, JZ 23/2009, S. 1129 ff.

Käßer, Wolfgang: Wahrheitsforschung im Strafprozess, Berlin 1974 (zit.: Käßer, Wahrheitsforschung)

Kahneman, Daniel/*Sibony*, Olivier/*Sunstein*, Cass: Noise – Was unsere Entscheidungen verzerrt – und wie wir sie verbessern können, München 2021

Kahneman, Daniel/*Tversky*, Amos: On the reality of cognitive illusions. Psychological Review (1996) Vol. 103(3), S. 582 ff.

Kaiser, Günter: Kriminologie, 3. Auflage, Heidelberg 1976

Kakadiya, Rutvik/*Lemos*, Reuel/*Mangalan*, Sebin/*Pillai*, Meghna/*Nikam*, Sneha: AI Based Automatic Robbery/Theft Detection using Smart Surveillance in Banks, 2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA), S. 201 ff.

Karlsruher Kommentar zur Strafprozessordnung – mit GVG, EGGVG und EMRK, Hannich, Rolf (Hrsg.), 8. Auflage, München 2019

Karlsruher Kommentar zur Strafprozessordnung – mit GVG, EGGVG und EMRK, Hannich, Rolf (Hrsg.), 9. Auflage, München 2023

Karpinski, Kurt: Der Sachverständige im Strafprozess, NJW 1968, S. 1173 ff.

Karwat, H.: Der Beweisbeschluss in Bauprozessen aus der Sicht des Sachverständigen, DRiZ 1972, S. 204 ff.

Kaur, Harmanpreet/*Nori*, Harsha/*Jenkins*, Samuel/*Caruana*, Rich/*Wallach*, Hanna/*Vaughan*, Jennifer: Interpreting Interpretability: Understanding Data Scientists' Use of Interpretability Tools for Machine Learning, CHI 2020, Paper 92

Keller, Rainer: Verwissenschaftlichung vers. Rationalität der strafprozessualen Beweiswürdigung?, GA 1999, S. 255 – 271

Kerameus, Konstantinos: Die Entwicklung des Sachverständigenbeweises im deutschen und griechischen Zivilprozess, in: Prozessrechtliche Abhandlungen, Heft 26, Berlin 1963

Kindhäuser, Urs: Das Beweismaß des Strafverfahrens – Zur Auslegung von § 261 StPO, Jura 1988, S. 290 ff.

Kindhäuser, Urs: Strafprozessrecht, 3. Auflage, Berlin 2013

Kipker, Dennis-Kenji (Hrsg.): Cybersecurity, München 2020

Kirk, Paul: Crime Investigation, 2. Auflage, 1974

Kleinknecht, Theodor/*Meyer*, Karlheinz: Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 37. Auflage, München 1985 (zit.: *Kleinknecht/Meyer*, Strafprozessordnung)

KMR, Kommentar zur Strafprozessordnung, v. Heintschel-Heinegg, Bernd/Stöckel, Heinz (Hrsg.), 108. Lieferung, Köln 2021

Knopp, Michael: Digitalfotos als Beweismittel, ZRP 2008, S. 156 ff.

Knopp, Michael: Rechtliche Perspektiven zur digitalen Beweisführung, in: Fischer, Stefan/Maehle, Erik/Reischuk, Rüdiger (Hrsg.), Informatik 2009: Im Focus das Leben, Beiträge der 39. Jahrestagung der Gesellschaft für Informatik e. V. (GI), 28.9. – 2.10.2009, Bonn, 2009, S. 1552 – 1566

Kochheim, Dieter: Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., München 2018 (zit.: *Kochheim*, Cybercrime und Strafrecht in der IuK-Technik)

Kohlhaas, Max: Änderung des Sachverständigenbeweises im Strafprozess? NJW 1962, S. 1329 ff.

Köller, Norbert/*Nissen*, Kai/*Rieß*, Michael/*Sadorf*, Erwin: Probabilistische Schlussfolgerungen im Schriftgutachten – Zur Begründung und Vereinheitlichung von Wahrscheinlichkeitsaussagen im Sachverständigengutachten, BKA (Hrsg.), Polizei + Forschung Bd. 26, München 2004 (zit.: *Köller/Nissen/Rieß/Sadorf*, Probabilistische Schlussfolgerungen im Schriftgutachten)

Kotsoglou, Kyriakos: Forensische Erkenntnistheorie, Der Inferentielle Kontextualismus und die Funktion der kontextrelevanten Zweifel im Strafverfahren – Zugleich eine analytische Perspektive zur Sachverhaltsfeststellung, Berlin 2015 (zit.: *Kyriakos*, Forensische Erkenntnistheorie)

Krauß, Detlef: Die strafrechtliche Problematik kriminologischer Ziele und Methoden. Eine Untersuchung am Beispiel des psychologischen und psychiatrischen Sachverständigen im Strafprozess; Aktuelles Recht Band 13, Frankfurt a. M. 1971

Krauß, Detlef: Richter und Sachverständige im Strafverfahren, ZStW 85 (1973), S. 320 ff.

Krekeler, Wilhelm: Der Beweiserhebungsanspruch des Beschuldigten im Ermittlungsverfahren, NStZ 1991, S. 367 ff.

Krekeler, Wilhelm: Der Beweiserhebungsanspruch des Beschuldigten im Ermittlungsverfahren: de lege lata und de lege ferenda, Bonn 1991 (zit.: *Krekeler*, Der Beweiserhebungsanspruch)

Krekeler, Wilhelm: Der Sachverständige im Strafverfahren, insbesondere im Wirtschaftsstrafverfahren, wistra 1989, S. 52 ff.

Krekeler, Wilhelm/*Löffelmann*, Markus/*Sommer*, Ulrich: Anwaltkommentar, 2. Auflage, Köln 2010

Kruse, Wolfgang: Der ärztliche Sachverständige in der Rechtsprechung, DÄBl. 1978, S. 2919 ff.

Kube, Edwin/*Leineweber*, Heinz: Polizeibeamte als Zeugen und Sachverständige, 2. Auflage, Köln 1980

Kuchinke, Kurt: Grenzen der Nachprüfbarkeit tatrichterlicher Würdigung und Feststellungen in der Revisionsinstanz, Bielefeld 1964 (zit.: *Kuchinke*, Grenzen der Nachprüfbarkeit)

Kudlich, Hans/*Nicolai*, Florian: Immer wieder Neuigkeiten im Strafprozessrecht – Das Gesetz zur Modernisierung des Strafverfahrens, JA 2020, S. 881 ff.

Kühne, Hans-Heiner: Strafprozessrecht, 8. Auflage, Heidelberg 2010

Kunz, Karl-Ludwig: Tatbeweis jenseits eines vernünftigen Zweifels – Zur Rationalität der Beweiswürdigung bei der Tatsachenfeststellung, ZStW 121 (2009) Heft 3, S. 572 – 606

Kusch, Klaus Günther: Der Indizienbeweis des Vorsatzes im gemeinen deutschen Strafverfahrensrecht, Hamburg 1963 (zit.: *Kusch*, Indizienbeweis)

Kusch, Roger: Aus der Rechtsprechung des BGH zum Strafverfahrensrecht – August bis Dezember 1993, NStZ 1994, S. 227 ff.

Kusch, Roger: Aus der Rechtsprechung des BGH zum Strafverfahrensrecht – Januar bis Juni 1996 – 2. Teil, NStZ 1997, S. 367 ff.

Labudde, Dirk/*Spranger*, Michael: Forensik in der digitalen Welt – Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt, Berlin 2017 (zit.: *Labudde et al.*, Forensik in der digitalen Welt)

Landau, Herbert: Die jüngere Rechtsprechung des Bundesverfassungsgerichts zu Strafrecht und Strafverfahrensrecht, NStZ 2015, S. 665 ff.

Langelüddeke, Albrecht/*Bresser*, Paul: Gerichtliche Psychiatrie, 3. Auflage, Berlin 1971

Laufs, Adolf: Arztrecht, NJW Schriftenreihe der Neuen Juristischen Wochenschrift, Heft 29, 2. Auflage, München 1978

Leferenz, Heinz: Richter und Sachverständige, in: Kriminalbiologische Gegenwartsfragen, Heft 5, Vorträge bei der XI. Tagung der Kriminalbiologischen Gesellschaft vom 4. bis 8.10.1961 in Wien, Hrsg. v. Th. Würtenberger und J. Hirschmann, Stuttgart 1962, S. 1. (zit.: *Leferenz*, Krim. Biol. Ggw.fragen, Heft 5)

Leferenz, Heinz: Self-Trust – A study of Reason, Knowledge and Autonomy, Oxford 1997 (zit.: *Lehrer*, Self-Trust)

Lehmann, Jens: Der Anspruch auf Einsicht in die Unterlagen des Sachverständigen, GA 2005, S. 639 – 647

Leithoff, Horst: Sachverständigengutachten vor Gericht, in: Der Sachbeweis im Strafverfahren, Arbeitstagung des BKA Wiesbaden vom 23 bis 26.10.1978, hrsg. v. BKA Wiesbaden, BKA-Vortragsreihe, Bd. 24, Wiesbaden 1979, S. 43 (zit.: *Leithoff*, Sachverständigengutachten)

Lemme, Dirk: Zur Ablehnung des Wirtschaftsreferenten der Staatsanwaltschaft gem. § 74 StPO, wistra 2002, S. 281 ff.

Lenckner, Theodor: Strafe, Schuld und Schuldfähigkeit, in: Göppinger, H./Witter, H.: Handbuch der forensischen Psychiatrie, Bd. I, Teil A „Die rechtlichen Grundlagen", Berlin 1972, S. 3 ff.

Lent, Friedrich: Die Abgrenzung des Sachverständigen vom Zeugen im Zivilprozess, ZZP 60 (1936), S. 9 ff.

Ley, Eberhard: Die Pflicht des Strafrichters zur Anhörung weiterer Sachverständiger, München 1966 (zit.: *Ley*, Die Pflicht des Strafrichters zur Anhörung weiterer Sachverständiger)

Ligges, Wolfgang: Die Stellung des Sachverständigen im deutschen Strafprozessrecht, Münster 1963 (zit.: *Ligges*, Die Stellung des Sachverständigen)

Lobe, Adolf: Richert und Sachverständiger, DRiZ 1913, S. 362 ff.

Lorch, Benedikt/*Scheler*, Nicole/*Riess*, Christian: Compliance Challenges in Forensic Image Analysis Under the Artificial Intelligence Act, https://doi.org/10.48550/arXiv.2203.00469

Löwe/Rosenberg: Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Erb, Volker/Esser, Robert/Franke, Ulrich/Graalmann-Scheerer, Kirsten/Hilger, Hans/Ignor, Alexander (Hrsg.), Band 2: Einleitung; §§ 48 – 93, 27. Auflage, Berlin 2017; 24. Auflage v. Rieß, Peter (Hrsg), Berlin 1984; 22. Auflage Berlin 1971

Löwe/Rosenberg: Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Erb, Volker/Esser, Robert/Franke, Ulrich/Graalmann-Scheerer, Kirsten/Hilger, Hans/Ignor, Alexander (Hrsg.), Band 6: §§ 212 – 255a, 27. Auflage, Berlin 2019

Löwe/Rosenberg: Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Erb, Volker/Esser, Robert/Franke, Ulrich/Graalmann-Scheerer, Kirsten/Hilger, Hans/Ignor, Alexander (Hrsg.), Band 6: §§ 212 – 255a, 27. Auflage, Berlin 2019

Löwe/Rosenberg: Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Erb, Volker/Esser, Robert/Franke, Ulrich/Graalmann-Scheerer, Kirsten/Hilger, Hans/Ignor, Alexander (Hrsg.), Band 7: §§ 256 – 295, 27. Auflage, Berlin 2020

Löwe/Rosenberg: Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Hanschke/Klaus-Peter/Jesse, Björn/Matt, Holger (Hrsg.), Band 8: §§ 2296 – 358, 27. Auflage, Berlin 2020

Lürken, Günter: Auswahl und Leitung des Sachverständigen im Strafprozess (§§ 73, 78 StPO), NJW 1968, S. 1161 ff.

Lundt, P. V./*Jahn*, E.: Gutachten des Bundesgesundheitsamtes – Zur Frage Alkohol bei Verkehrsstraftaten, Bad Godesberg 1966

Macki, John Leslie: Truth, Probability and Paradox, Oxford, 1974.

Mandia, Kevin/*Prosise*, Chris/*Pepe*, Matt: Incident Response & Computer Forensics, 2. Auflage, 2003

Maras, Marie-Helen: Computer Forensics – Cybercriminals, Laws, and Evidence, 2. Auflage, Burlington (Massachusetts, USA) 2014

Marberth-Kubicki, Annette: Computer- und Internetstrafrecht, 2. Auflage, München 2010 (zit.: Marberth-Kubicki, Computer- und Internetstrafrecht)

Marmann, Hans: Aufklärungspflicht durch Sachverständigengutachten und freie Beweiswürdigung, GA 1953, S. 136 ff.

Marshall, Paul: The harm that judges do – misunderstanding computer evidence: Mr Castleton's story an affront to the public conscience, Digital Evidence and Electronic Signature Law Review, 17 (2020), S. 25 ff.

Martini, Mario: Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, Berlin 2019

Martini, Mario: Zeitliche Höchstgrenzen der Forderungsdurchsetzung im öffentlichen Recht als Herausforderung für den Rechtsstaat, NVwZ-Extra 2014, S. 1 – 23

Mason, Stephen/*Seng*, Daniel: Electronic Evidence, 4. Auflage, London 2017 (zit.: *Mason/Seng*, Electronic Evidence)

Maunz, Theodor/*Dürig*, Günter (Begr.)/*Herzog*, Roman/*Scholz*, Rupert/*Herdegen*, Matthias/*Klein*, Hans (Hrsg.): Grundgesetz, Kommentar, 95. Ergänzungslieferung, München 2021

Mayer, Hellmuth: Der Sachverständige im Strafprozess, in: Festschrift für Edmund Mezger, München 1954, S. 455 ff.

Mayer-Schönberger, Viktor/*Cukier*, Kenneth: Big Data, A Revolution That Will Transform How We Live, Work and Think, Boston 2013

Meier, Stefan: Digitale Forensik im Unternehmen, Regensburg 2016 (zit.: *Meier*, Digitale Forensik im Unternehmen)

Mengel, Friedrich-Wilhelm: Die Erhebung des Sachverständigenbeweises im Strafprozess, Eine Untersuchung der richterlichen Befugnisse und Verpflichtungen aus § 78 StPO, Diss., Köln 1978

Meseke, Bodo: Digitale Forensik – Praxiswissen Cybercrime für Manager, Berlin 2019 (zit.: *Meseke*, Digitale Forensik)

Meyer, Paul/*Höver*, Albert/*Bach*, Wolfgang/*Oberlack*, Henning: Die Vergütung und Entschädigung von Sachverständigen, Zeugen, Dritten sowie von ehrenamtlichen Richtern nach dem JVEG, 26. Auflage, Köln 2014

Meyer-Goßner, Lutz/*Schmitt*, Bertram: Strafprozessordnung, 60. Auflage, München 2017; 51. Auflage, München 2008

Mezger, Edmund M.: Der psychiatrische Sachverständige im Prozess, AcP 117 (1918), Beilageheft, S. 1 ff.

Miebach, Klaus: Die freie richterliche Beweiswürdigung in der neueren Rechtsprechung des BGH, NStZ 2020, S. 72 – 80

Miebach, Klaus: Die freie richterliche Beweiswürdigung in der neueren Rechtsprechung des BGH, NStZ 2021, S. 403 ff.

Mittermaier, Joseph: Beiträge zur Lehre vom Beweise durch Sachverständige, AcP 2 (1819), S. 119 – 140

Mittermaier, Joseph: Die Gesetzgebung und Rechtsübung über Strafverfahren, Erlangen 1856 (zit.: *Mittermaier*, Strafverfahren)

Mittermaier, Joseph: Stellung und Wirksamkeit der Sachverständigen im Strafverfahren, GA 1853, S 7 ff.; S. 107 ff.

Möser, Malte/*Böhme*, Rainer: Join Me on a Market for Anonymity, WEIS 2016

Mösl, Albert: Sachverständigengutachten und freie Beweiswürdigung im Strafprozess, DRiZ 1970, S. 110 ff.

Momsen, Carsten: Die Renaissance des Polygraphen? Wie effektiv lassen sich amerikanische Verteidigungsstrategien im deutschen Strafverfahren nutzen? KriPoZ 2018, S. 142 ff.

Momsen, Carsten: Digitale Beweismittel auf Sicht der Strafverteidigung, in: Beck, Susanne/Meier, Bernd-Dieter/Momsen, Carsten (Hrsg.): Cybercrime und Cyberinvestigations – Neue Herausforderungen der Digitalisierung für Strafrecht, Strafprozessrecht und Kriminologie, Baden-Baden 2015, S. 67 ff.

Momsen, Carsten: Zum Umgang mit digitalen Beweismitteln im Strafprozess, in: Fahl, Christian/Müller, Eckart/Satzger, Helmut/Swoboda, Sabine, (Hrsg.), Festschrift für Werner Beulke zum 70. Geburtstag, Heidelberg 2015, S. 871 ff.

Momsen, Carsten: Strafrechtliche Relevanz von Datensicherheit und Datenschutz im Unternehmen, in: Franz, Walter (Hrsg.): Handbuch Industrie 4.0: Recht, Technik, Gesellschaft, Berlin 2020, S. 61 ff.

Momsen, Carsten/*Hercher*, Nils: Digitale Beweismittel im Strafprozess: Eignung, Gewinnung, Verwertung, Revisibilität, Beitrag zum 37. Strafverteidigertag, Freiburg 2013, S. 173, (zit.: *Momsen/Hercher*, Digitale Beweismittel im Strafprozess)

Momsen, Carsten/*Rackow*, Peter/*Schwarze*, Mathis: Dolmetscher und Sprachverständige als Ermittlungshelfer? – Rechtsfragen des Einsatzes von Sprachverständigen beziehungsweise Dolmetschern – zugleich Anmerkung zu dem Urteil des LG Hamburg vom 9.5.2016 – 608 KLs 1/15, NStZ 2018, S. 625 ff.

Moussa, Ahmed Fekry: Electronic evidence and its authenticity in forensic evidence, Egyptian Journal of Forensic Sciences (2021), S. 1 ff.

Müller, Egon: Über Probleme des Sachverständigenbeweises im staatsanwaltschaftlichen Ermittlungsverfahren, in: Festschrift für Gerhard Lüke, München 1997, S. 493 ff.

Müller, Henning Ernst/*Eisenberg*, Ulrich: Anmerkung zu BGH, Beschl. v. 28.8.2018 – 5 StR 50/17 –, JR 2019, S. 46 – 49

Müller, Klaus: Der Sachverständige im gerichtlichen Verfahren, 3. Auflage, Heidelberg 1988

Müller, Nico: Die digitale Durchsuchung Abbilderstellung im Strafprozess (Bachelorarbeit), Lehrstuhl für Informatik 1 (Freiling, Felix/Müller, Tilo/Scheler, Nicole), Erlangen 2022

Müller, Sebastian: Internetermittlungen und der Umgang mit digitalen Beweismitteln im (Wirtschafts-)Strafverfahren, NZWiSt 2020, S. 9 ff.

Münchener Anwaltshandbuch MAH – Strafverteidigung, Müller, Eckhart/Schlothauer, Reinhold/Knauer, Christoph (Hrsg.), 2. Auflage, München 2014

Münchener Anwaltshandbuch MAH – Strafverteidigung, Müller, Eckhart/Schlothauer, Reinhold/Knauer, Christoph (Hrsg.), 3. Auflage, München 2022

Münchener Kommentar zum Strafgesetzbuch, Sander, Günther (Hrsg.), Band 4: §§ 185 – 262, 4. Auflage 2021, München 2021

Münchener Kommentar zur Strafprozessordnung, Kudlich, Hans (Hrsg.), Band 1: §§ 1 – 150, 1. Auflage, München 2014

Münchener Kommentar zur Strafprozessordnung, Kudlich, Hans (Hrsg.), Band 1: §§ 1 – 150, 2. Auflage, München 2023

Münchener Kommentar zur Strafprozessordnung, Schneider, Hartmut (Hrsg.), Band 2: §§ 151 – 332, 1. Auflage, München 2016

Münchener Kommentar zur Strafprozessordnung, Schneider, Hartmut (Hrsg.), Band 2: §§ 151 – 332, 2. Auflage, München 2024

Mysegades, Jan: DNA-Auswertung in der Black Box? – Gerichtliche Beweisführung durch statistische Computerprogramme, in: Taeger, Jürgen (Hrsg.), Recht 4.0 – Innovationen aus den rechtswissenschaftlichen Laboren, S. 717 – 731

Mysegades, Jan: DNA-Auswertung in der Black Box? – Gerichtliche Beweisführung durch statistische Computerprogramme, CR 2018, S. 225 – 231

Mysegades, Jan: Software als Beweiswerkzeug – Gerichtliche Sachverhaltsfeststellung mittels nicht nachvollziehbarer Software in Gegenwart und Zukunft, Trier 2002 (zit.: *Mysegades*, Software als Beweiswerkzeug)

Nelles, Ursula: Der Einfluss der Verteidigung im Ermittlungsverfahren, StV 1986, S. 74 ff.

Neuhaus, Ralf/*Artkämper*, Heiko: Kriminaltechnik und Beweisführung im Strafverfahren, München 2014 (zit.: *Neuhaus/Artkämper*, Kriminaltechnik und Beweisführung im Strafverfahren)

Neumann, Cedric/*Kaye*, David/*Jackson*, Graham/*Reyna*, Valerie/*Ranadive*, Anjali: Presenting Quantitative and Qualitative Information on Forensic Science Evidence in the Courtroom, Chance 29 (2016), S. 37 ff.

Neumann, Ulfrid: Sebastian Seel: Wahrheit im Strafprozess, JZ 1/2022, S. 30 ff.

Niese, Werner: Zur Frage der freien richterlichen Überzeugung (zum Urteil des BGH v. 21.5.1953 – 3 StR 9/53), GA, 1954, S. 152 ff.

Nikisch, Arthur: Zivilprozessrecht, 2. Auflage, Tübingen 1952

Nink, David: Justiz und Algorithmen – Über die Schwächen menschlicher Entscheidungsfindung und die Möglichkeiten neuer Technologien in der Rechtsprechung, Berlin 2021

Nix, Christoph: Ablehnung des polizeilichen Sachverständigen, Kriminalistik 1994, S. 83 ff.

Nurek, Mateusz/*Michalski*, Radoslaw: Combining Machine Learning and Social Network Analysis to Reveal the Organizational Structures, Appl. Sci. 2020, Vol. 10 No. 5, S. 1699 ff.

Ostermeyer, Helmut: Die bestrafte Gesellschaft: Ursachen u. Folgen eines falschen Rechts, München 1975

Otte, Karina: Rechtsgrundlagen der Glaubwürdigkeitsbegutachtung von Zeugen im Strafprozess, Münster und Hamburg 2002

Ottmann, Jenny/*Breitinger*, Frank/*Freiling*, Felix: „Defining Atomicity (and Integrity) for Snapshots of Storage in Forensic Computing." Proceedings of the Digital Forensics Research Conference Europe (DFRWS EU) 2022, Oxford 2022

Ottmann, Jenny/*Pollach*, Johannes/*Scheler*, Nicole/*Schneider*, Janine/*Rückert*, Christian/*Freiling*, Felix: Zur Blackbox-Problematik im Bereich der Mobilfunkforensik, DuD 2021, S. 546 ff.

Overill, Richard/*Silomon*, Jantje: Uncertainty Bounds for Digital Forensic Evidence and Hypotheses, in: ARES 2012, S. 590 ff.

Overill, Richard/*Silomon*, Jantje/*Chow*, Kam-Pui: A Complexity Based Model for Quantifying Forensic Evidential Probabilities, in: ARES 2010, S. 671 ff.

Overill, Richard/*Silomon*, Jantje/*Chow*, Kam-Pui: Quantification of digital hypotheses using probability theory, in: SADFE 2013, S. 1 ff.

Page, Helen/*Horsman*, Graeme/*Sarna*, Anna/*Foster*, Julienne: A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn, Science & Justice (2019) Vol. 59, S. 83 ff.

Paul, Werner: Die Bedeutung des kriminalpolizeilichen EDV-Sachverständigen aus polizeilicher Sicht, CR 1986, S. 173 ff.

Pause, Eckhard: Der „unabhängige Sachverständige", NJW 1985, S. 2576 ff.

Pawlak, Klaus: Ablehnung des Sachverständigen im Strafverfahren wegen Befangenheit? Eine Untersuchung zur Berechtigung des § 74 StPO, Juristische Schriftenreihe Band 6, Hamburg 1998 (zit.: *Pawlak*, Ablehnung des Sachverständigen)

Perron, Walter: Das Beweisantragsrecht des Beschuldigten im deutschen Strafprozess, Berlin 1995

Peters, Karl: Die prozessrechtliche Stellung des psychologischen Sachverständigen, in: Gottschaldt, K./Lersch, Ph./Sander, F./Thomae, H.: Handbuch der Psychologie, Bd. 11 „Forensische Psychologie", hrsg. v. U. Undeutsch, Göttingen 1967, S. 768 (zit.: *Peters*, Psychologischer Sachverständiger)

Peters, Karl: Fehlerquellen im Strafprozess, Eine Untersuchung der Wiederaufnahmeverfahren in der Bundesrepublik Deutschland, Bd. 1, Einführung und Dokumentation, Karlsruhe 1970; Bd. 2 Systematische Untersuchungen und Folgerungen, Karlsruhe 1972, Bd. 3 Wiederaufnahmerecht, Karlsruhe 1974 (zit.: *Peters*, Fehlerquellen)

Peters, Karl: Fehlerquellen und Rechtsanwendung im Strafprozeß, in: Hirsch, Hans Joachim/Kaiser, Günther/Marquardt, Helmut (Hrsg.): Gedächtnisschrift für Hilde Kaufmann, Berlin/New York 1986, S. 913 – 927

Peters, Karl: Strafprozess, 4. Auflage Heidelberg 1985

Pfeiffer, Gerd: Strafprozessordnung, 5. Auflage, München 2005

Pieper, Helmut: Richter und Sachverständiger im Zivilprozessrecht, ZZP 84 (1971), S. 1 ff.

Plewig, Hans-Joachim: Funktion und Rolle des Sachverständigen aus der Sicht des Strafrichters, Hamburg 1983 (zit.: *Plewig*, Funktion und Rolle des Sachverständigen)

Pollähne, Helmut, Kriminalprognostik – Untersuchungen im Spannungsfeld zwischen Sicherheitsrecht und Rechtssicherheit, Berlin 2011

Poppen, Enno: Die Geschichte des Sachverständigenbeweises im Strafprozess des deutschsprachigen Raumes, Göttingen 1984. (zit.: *Poppen*, Die Geschichte des Sachverständigenbeweises)

Popper, Karl Raimund: Logik der Forschung, 10. Aufl. Tübingen 1994

Popper, Karl Raimund: Conjectures and Refutations: The Growth of Scientific Knowledge (Vermutungen und Widerlegungen), 1962

Povar, Digambar/*Bhadran*, Vishnu: Forensic Data Carving, in: Baggili, Ibrahim (Hrsg.), ICDF2C 2010: Digital Forensics and Cybercrime, S. 137 ff.

Puppe, Ingeborg: Anmerkung zu BGH v. 2.8.1995 – Az. 2 StR 221/94, JZ 1996, S. 318 – 320

Putnam, Hilary: Representation and Reality, Cambridge (Mass.) 1988

Ranft, Otfried: Strafprozessrecht, 3. Auflage, Stuttgart 2005

Rasch, Wilfried/*Jungfer*, Gerhard: Die Ladung des psychiatrisch-psychologischen Sachverständigen nach § 220 StPO – Ein Disput, StV 1999, S. 513 ff.

Rauch, Hans-Joachim: Auswahl und Leitung des Sachverständigen im Strafprozess, Bemerkungen zu Sarstedt in NJW 1968, 177, NJW 1968, S. 1173 ff.

Regan, James: The Forensic Potential of Flash Memory, Diplomarbeit, Monterey CA 2009

Rengier, Rudolf: Die Zeugnisverweigerungsrechte im geltenden und künftigen Strafverfahrensrecht – Grundlagen, Reformfragen und Stellung im System der Beweisverbote und im Revisionsrecht, Paderborn 1979 (zit.: *Rengier*, Zeugnisverweigerungsrechte)

Rieß, Peter: Zur Revisibilität der freien richterlichen Überzeugung, GA 1978, S. 257 ff.

Risse, Jörg: Der Homo iuridicus – ein gefährliches Trugbild, Wie Heuristiken richterliche Entscheidungen beeinflussen, NJW 2018, S. 2848 ff.

Rodenbeck, Julian: Lügendetektor 2.0 – Der Einsatz von Künstlicher Intelligenz zur Aufdeckung bewusst unwahrer Aussagen im Strafverfahren, StV 2020, S. 479 ff.

Rogall, Klaus: Behördengutachten im Strafverfahren, in: Festschrift für Karl-Heinz Gössel, Heidelberg 2002, S. 511 ff.

Rogall, Klaus: Die Beschuldigtenstellung im Strafverfahren. Objektivismus und Subjektivismus bei der Statusbegründung, in: Festschrift für Wolfgang Frisch, Berlin 2013, S. 1199 ff.

Rogall, Klaus: Gegenwärtiger Stand und Entwicklungstendenzen der Lehre von den strafprozessualen Beweisverboten, ZStW 91 (1979), S. 1 ff.

Roider, Jasmin: Der Einfluss von Sachverständigen – eine emprische Untersuchung am Beispiel der Strafgesetzgebung, Berlin 2023

Rollberg, Christoph: Algorithmen in der Justiz – Rechtsfragen zum Einsatz von Legal Tech im Zivilprozess, in: Broemel, Roland/Lüdemann, Jörn/Podszun, Rupprecht/Schweitzer, Heike (Hrsg.): Recht und Digitalisierung, Bd. 2, Baden-Baden 2020

Rosenberg, Leo/*Schwab*, Karl Heinz/*Gottwald*, Peter: Zivilprozessrecht, 17. Auflage, München 2010, S. 730 ff.

Roxin, Claus/*Schünemann*, Bernd: Strafverfahrensrecht, 27. Auflage, München 2012 (zit.: *Roxin/Schünemann*, Strafverfahrensrecht)

Rudolph, Kurt: Das Zusammenwirken des Richters und des Sachverständigen, Die Justiz 1969, S. 24 ff.

Rückert, Christian: Digitale Daten als Beweismittel im Strafverfahren, Tübingen 2023 (zit.: *Rückert*, Digitale Daten als Beweismittel im Strafverfahren)

Rückert, Christian: Herausforderungen der Digitalisierung für das Strafverfahren, in: Hoven, Elisa/Kudlich, Hans (Hrsg.), Digitalisierung und Strafverfahren, Baden-Baden 2020, S. 71 ff.

Rückert, Christian: Mit künstlicher Intelligenz auf Verbrecherjagd: Einsatz von Gesichtserkennungstechnologie zur Aufklärung der „Kapitolverbrechen", VerfBlog, 2021/1/22

Rückert, Christian/*Meyer-Wegener*, Klaus/*Safferling*, Christoph/*Freiling*, Felix: Messengerdienst-Nachrichten als Beweismittel im Strafverfahren – am Beispiel der Auswertung von WhatsApp-Chats, JR 2023, S. 366 – 378

Rückert, Christian/*Scheler*, Nicole: Erlanger Cyber^2 Crime Tag 2021: Internationale Strafverfolgung von Cybercrime Delikten, KriPoZ 2022, S. 227 ff.

Rückert, Christian/*Wüst*, Marlene: Erlanger Cyber^2 Crime Tag 2020: IT-Forensik und Strafprozessrecht, KriPoZ 2021, S. 64 ff.

Rüping, Hinrich: Das Strafverfahren, 3. Auflage, München 1997

Safferling, Christoph: Audiatur et altera pars – die prozessuale Waffengleichheit als Prozessprinzip? Qui statuit aliquid parte inaudita altera, Aequum liquet statuerit haud aequs fuit., NStZ 2004, S. 181 ff.

Safferling, Christoph/*Rückert*, Christian: Europäische Grund- und Menschenrechte im Strafverfahren – ein Paradigmenwechsel?, NJW 2021, S. 287 ff.

Sagana, Anna: The downward spiral of biases in criminal investigations: From eyewitnesses to forensic experts and judges, in: Barton/Dubelaar/Kölbel/Lindemann (Hrsg.), Vom hochgemuten, voreiligen Griff nach der Wahrheit – Fehlurteile im Strafprozess, S. 133 ff.

Sakshi/Malik Aruna/*Sharma*, Ajay K.: Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things, Journal of Information Security and Applications 2023 Vol. 77, 103579 ff.

Salditt, Franz: Intelligent Agents – Verdacht unter der Herrschaft computergestützter Technologien, in: Fischer, Thomas, Hoven, Elisa (Hrsg.), Verdacht, Baden-Baden 2016, S. 199 ff.

Sarstedt, Werner: Auswahl und Leitung des Sachverständigen im Strafprozess, NJW 1968, S. 177 ff.

Sarstedt, Werner: Fragen des Sachverständigenbeweises zur Zurechnungsfähigkeit, in: Festschrift für Erich Schmidt-Leichner zum 65. Geburtstag, München 1977, S. 171 ff.

Sarstedt, Werner/*Hamm*, Rainer: Die Revision in Strafsachen, 5. Auflage, Berlin 1983

Sass, Wolfgang: Der „Mangel-Beweis" durch Sachverständige und die Symptomtheorie des BGH, DS 2010, S. 132 ff.

Satzger, Helmut/*Schluckebier*, Wilhelm/*Widmaier*, Gunter (Hrsg.), Strafprozessordnung mit GVG und EMRK: StPO – Kommentar, 4. Auflage, Köln 2020

Sauer, Wilhelm: Allgemeine Prozesslehre, Berlin 1951

Savic, Laura Iva: Beweisführung mit digitalen Medien im Strafprozess. Im Vergleich und unter Berücksichtigung der ZPO und VwGO (sowie weiterer Rechtsvorschriften) in: Buschmann, Almuth/Gläß, Anne-Christin/Gonska, Hans-Henning/Philipp, Markus/Zimmermann, Ralph (Hrsg.), Digitalisierung der gerichtlichen Verfahren und das Prozessrecht, Berlin 2018, S. 71 ff.

Savic, Laura Iva: Die digitale Dimension des Strafprozessrechts – Zur Doppelnatur digitaler Beweise, Berlin 2020

Schäfer, Gerhard: Die Praxis des Strafverfahrens, 6. Auflage, Stuttgart 2000

Schäfer, Gerhard: Freie Beweiswürdigung und revisionsrechtliche Kontrolle, StV 1995, S. 147 ff.

Schäfer, Helmut: Der Computer im Strafverfahren, wistra 1989, S. 8 ff.

Schikora, Gregor: Einsichtnahme in die Handakte von Sachverständigen durch Gerichte und Parteien, MDR 2002, S. 1033 ff.

Schirhakl, Thomas: Der Sachverständigenbeweis im neuen Strafprozessrecht – Ausgewählte Fragen zum neuen Ermittlungsverfahren und zur Rolle des Sachverständigen in der „StPO neu", Sachverständige Heft 3/2009, S. 146 ff.

Schlüchter, Ellen: Das Strafverfahren, 2. Auflage, München 1983

Schmidhäuser, Eberhard: Zeuge, Sachverständiger und Augenscheinsgehilfe, ZZP 72 (1959), S. 365 ff.

Schmidhäuser, Eberhard: Über die Praxis der Gerichte, die richterliche Verantwortung in der Strafrechtsanwendung zu verschleiern, in: Grundfragen der gesamten Strafrechtswissenschaft, Festschrift für Heinrich Henkel zum 70. Geburtstag, Berlin 1974, S. 229 ff.

Schmidt, Eberhard: Der Arzt als Sachverständiger im Strafprozess, Hefte zur Unfallkunde, Versicherungs- und Versorgungsmedizin, XX. Tagung am 17. Und 18.5.1956 in Heidelberg, hrsg. v. Herget, R., Berlin 1957, S. 162 (zit.: *Eb. Schmidt*, Arzt als Sachverständiger)

Schmidt, Eberhard: Gehört der Sachverständige auf die Richterbank? Ein Beitrag zur Problematik des Sachverständigenbeweises, JZ 1961, S. 585 ff.

Schmidt, Eberhard: Lehrkommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz, Teil I, Göttingen 1952 (zit.: *Eb. Schmidt*, I); Teil II, Göttingen 1957 (zit.: *Eb. Schmidt*, II).

Schmidt, Eberhard: Nachträge und Ergänzungen zu Teil II, Nachtragsband I, Göttingen 1967 (zit.: *Eb. Schmidt*, Nachtragsband I)

Schmidt, Eberhard: Richter und Sachverständige in ihrem Zusammenwirken bei kriminologischen Problemen, in: Psychopathologie heute, Festschrift für Kurt Schneider zum 75. Geburtstag, Stuttgart 1962, S. 258 ff.

Schneider, Ernst: Vollständige Lehre vom Beweise in bürgerlichen Rechtssachen: Aus vernunftsmäßigen Grundbegriffen mit Rücksicht auf die Positivgesetze, abgeleitet und systematisch dargestellt, Gießen 1803 (zit.: *Schneider*, Lehre vom Beweise)

Schneider, Frédéric: Auswirkungen der Digitalisierung auf das Ermittlungsverfahren, ZIS 2020, S. 79 ff.

Schneider, Hans-Joachim: Beweisverwertungsverbot der Zeugnisverweigerung eines Angehörigen gegen den Angeklagten, JuS 1970, S. 271 ff.

Schneider, Hartmut: Bezeichnung konkreter Beweistatsachen bei Beweisanträgen auf Einholung eines Sachverständigengutachtens, NStZ 2023, S. 65 ff.

Schneider, Janine/*Eichhorn*, Maximilian/*Freiling*, Felix: Ambiguous file system partitions, Forensic Science International: Digital Investigation 2022

Schneider, Janine/*Wolf*, Julian/*Freiling*, Felix: Tampering with Digital Evidence is Hard: The Case of Main Memory Images, Forensic Science International: Digital Investigation (2020) Vol. 32, S. 1 ff.

Schnellbach, Dietrich: Sachverständigengutachten kollegialer Fachbehörden im Prozess (unter besonderer Berücksichtigung des österreichischen Rechts), Marburg 1964

Schreiber, Hans-Ludwig: Zur Rolle des psychiatrisch-psychologischen Sachverständigen im Strafverfahren, in: Festschrift für Rudolf Wassermann, Neuwied 1985, S. 1007 ff.

Schröder, Horst: Die kriminalpolitischen Aufgaben der Strafrechtsreform, Referat zum 43. Deutschen Juristentag, in: Verhandlungen des 43. Deutschen Juristentages, Bd. 2 (Sitzungsberichte) Teil E, Tübingen 1962, S. 3 ff.

Schulz, Joachim: Die Austauschbarkeit von Beweismitteln oder die Folge apokrypher Beweismittel, StV 1983, S. 341 ff.

Schünemann, Bernd: Kognition, Einstellung und Vorurteil bei der Rechtsfindung, in: Lampe, E.-J. (Hrsg.), Beiträge zur Rechtsanthropologie ARSP Beiheft 22 (1985), S. 68 ff.

Schünemann, Bernd: Risse im Fundament, Flammen im Gebälk: Die Strafprozessordnung nach 130 Jahren, ZIS 2009, S. 484 ff.

Schünemann, Bernd: Zur Reform der Hauptverhandlung im Strafprozeß, GA 1978, S. 172 ff.

Schum, David: The Evidential Foundations of Probabilistic Reasoning, 2001

Schwartz, Tobias/*Faber*, Sabrina: Die Durchsicht elektronischer Speichermedien in Steuer- und Wirtschaftsstrafverfahren – „IT-Durchsuchung“ (Teil 2), ZWH 2023, S. 123 – 127

Schwarz, Jürgen/*Wille*, Reinhard: § 51 StGB – gestern, heute und morgen, NJW 1971, S. 1061 ff.

Schwinge, Erich: Grundlagen des Revisionsrechts, 2. Aufl., Bonn 1960

Seel, Sebastian: Wahrheit im Strafprozess, Berlin 2021 (zit.: *Seel*, Wahrheit im Strafprozess)

Senge, Lothar: Strafverfahrensänderungsgesetz – DNA-Analyse, NJW 1997, S. 2411 ff.

Seyler, Wendelin: Das Behördengutachten im Strafprozess, GA 1989, S. 547 ff.

Sheppard, K/*Fieldhouse*, S. J./*Casella*, J. P.: Experiences of evidence presentation in court: an insight into the practice of crime scene examiners in England, Wales and Australia, Egyptian Journal of Forensic Sciences, 2020, https://doi.org/10.1186/s41935-020-00184-5

Sieber, Ulrich: Straftaten und Strafverfolgung im Internet – Gutachten C zum 69. Deutschen Juristentag, München 2012

Sieverts, Rudolf: Fachpsychologische Aufgaben innerhalb einer modernen Strafrechtspflege, in: Blau, G./Müller-Luckmann, E.: Gerichtliche Psychologie, Aufgabe und Stellung des Psychologen in der Rechtspflege, Berlin 1962, S. 91 ff. (zit.: *Sieverts*, Fachpsychologische Aufgaben)

Singelnstein, Tobias: Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, NStZ 2018, S. 1 – 9

Soll, Jack/*Milkman*, Katherine/*Payne*, John: A User's Guide to Debiasing, in: Keren, Gideon/Wu, George: The Wiley Blackwell Handbook of Judgment and Decision Making, 2015

Stamp, Frauke: Die Wahrheit im Strafverfahren. Eine Untersuchung zur prozessualen Wahrheit unter besonderer Berücksichtigung der Perspektive des erkennenden Gerichts in der Hauptverhandlung, Baden-Baden 1998 (zit.: *Stamp*, Die Wahrheit im Strafverfahren)

Stein, Friedrich: Das private Wissen des Richters, Leipzig 1893

Stinshoff, Frederike: Die operative Fallanalyse im Strafverfahren. Ein Beitrag zur Dogmatik der persönlichen Beweismittel, Frankfurt am Main 2017 (zit.: *Stinshoff*, Operative Fallanalyse)

Stoykova, Radina: Digital evidence: Unaddressed threats to fairness and the presumption of innocence: Computer Law & Security Review 2021 Vol. 42, S. 105575 ff.

Stoykova, Radina/*Andersen*, Stig/*Franke*, Katrin: Reliability assessment of digital forensic investigations in the Norwegian police, Forensic Science International Digital Investigation (2022), S. 301351 ff.

Stoykova, Radina/*Franke*, Katrin: Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations: Forensic Science International: Digital Investigation, 2023 Vol. 45, S. 301554 ff.

Strippelmann, Friedrich: Die Sachverständigen im gerichtlichen und außergerichtlichen Verfahren, Cassel 1858

Stuckenberg, Carl-Friedrich: Untersuchungen zur Unschuldsvermutung, Berlin 1998

Stüttgen, Johannes/*Dewald*, Andreas/*Freiling*, Felix: Selective Imaging Revisited, in: Sidar, Gi (Hrsg.): Proceedings of the 7th Intern. Conference on IT Security Incident Management § IT Forensics 2013

Sunde, Nina: Forensic Science International: Digital Investigation 40 (2022), Nr. 301317 ff.

Sunde, Nina: Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation, Masterarbeit der NTNU (Norwegian University of Science and Technology, Oslo 2017 (zit.: *Sunde*, Non-technical Sources of Errors)

Sunde, Nina: Unpacking the evidence elasticity of digital traces, Cogent Social Sciences (2022) Vol. 8

Sunde, Nina: What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices, Science & Justice 61 (2021), S. 586 ff.

Sunde, Nina/*Dror*, Etiel: Cognitive and Human Factors in Digital Forensics: Problems, Challenges, and the Way Forward, Digital Investigation (2019) Vol. 29, S. 101 ff.

Sunde, Nina/*Horsman*, Graeme: Part 1: The need for peer review in digital forensics, Forensic Science International: Digital Investigation 35 (2020), Nr. 301062 ff.

Sunde, Nina/*Sunde*, Inger Marie: Conceptualizing an AI-based Police Robot for Preventing Online Child Sexual Exploitation and Abuse – Part 2: Legal Analysis of PrevBOT, Nordic Journal of Studies in Policing (2022), S. 1 ff.

Systematischer Kommentar zur Strafprozessordnung, Wolter, Jürgen (Hrsg.), Band I: §§ 1 – 93, 5. Auflage, Köln 2018

Systematischer Kommentar zur Strafprozessordnung, Wolter, Jürgen (Hrsg.), Band IV: §§ 198 – 246, 5. Auflage, Köln 2015

Systematischer Kommentar zur Strafprozessordnung, Wolter, Jürgen (Hrsg.), Band V: §§ 246a – 295, 5. Auflage, Köln 2016

Systematischer Kommentar zur Strafprozessordnung, Wolter, Jürgen (Hrsg.), Band VIII: §§ 374 – 500, 5. Auflage, Köln 2020

Thaler, Richard/*Sunstein*, Cass: Nudge – Wie man kluge Entscheidungen anstößt, 16. Auflage, Berlin 2020

Thiel, Christian/*Thiel*, Christoph/*Fiedler*, Arno: Verlässliche Personenidentifizierung mittels Techniken der Künstlichen Intelligenz, DuD 2021, S. 462 ff.

Thomae, Hans: Prinzipien und Formen der Gestaltung psychologischer Gutachten, in: Gottschalk, K/Lersch, Ph./Sander, F./Thomae H.: Handbuch der Psychologie, Bd. 11 „Forensische Psychologie“, hrsg. v. U. Undeutsch, Göttingen 1967, S. 237 ff.

Toepel, Friedrich: Grundstrukturen des Sachverständigenbeweises im Strafprozessrecht, Veröffentlichungen zum Verfahrensrecht, Bd. 27, Tübingen 2002 (zit.: *Toepel*, Grundstrukturen des Sachverständigenbeweises)

Tondorf, Günter/*Tondorf*, Babette: Psychologische und psychiatrische Sachverständige im Strafverfahren, 3. Auflage, Heidelberg 2011

Tondorf, Günter/*Waider*, Heribert: Der Sachverständige, ein „Gehilfe“ auch des Strafverteidigers? StV 1997, S. 493 ff.

Trapp, Jana/*Gallmetzer*, Alena/*Safferling*, Christoph: StPO-Planspiel: Strafprozessrecht für Studierende und Lehrende zum Anfassen, Erfahrungsbericht JA 10/2020

Tröndle, Herbert: Der Sachverständigenbeweis, JZ 1969, S. 374 ff.

Trück, Thomas: Die Rechtsprechung des BGH zur Ablehnung von Beweisanträgen auf Vernehmung eines Sachverständigen, NStZ 2007, S. 377 ff.

Ulrich, Jürgen: Der Gerichtliche Sachverständige, 12. Auflage, Köln 2007

Valerius, Brian: „Legal Tech" im Strafverfahren? ZStW 133 (2021), S. 152 – 168

Vennemann, Marielle/*Oppelt*, Claus/*Grethe*, Stefanie/*Anslinger*, Katja/*Schneider*, Harald/*Schneider*, Peter M.: Möglichkeiten und Grenzen der forensischen DNA-Analyse unter dem Gesichtspunkt verschiedener Szenarien zur Spurenentstehung – Eine Stellungnahme der gemeinsamen Spurenkommission der rechtsmedizinischen und kriminaltechnischen Institute, NStZ 2022, S. 72 ff.

Venzlaff, Ulrich: Methodische und praktische Probleme der forensisch-psychiatrischen Begutachtung, in: Venzlaff, Ulrich/Foerster, Klaus: Psychiatrische Begutachtung, 3. Auflage, München 2000, S. 67 ff.

Vogel, Sebastian/*Volkmann*, Viktor: Die Sachverständigenauswahl und -beauftragung in Medizinstrafverfahren – Gute Gutachten durch gute Gutachter, GesR 2021, S. 753 ff.

Volk, Klaus/*Engländer*, Armin: Grundkurs StPO, 8. Auflage, München 2013

Volkmann, Viktor/*Vogel*, Sebastian: Die Besorgnis der Befangenheit gegenüber der Staatsanwaltschaft, StV 2021, S. 537 ff.

Vyhnálek, Sascha: Die Abgrenzung von Sachverständigen und Zeugen im Strafverfahren, Kiel 1997

Wabnitz, Heinz-Bernd/*Janovsky*, Thomas/*Schmitt*, Lothar (Hrsg.): Handbuch Wirtschafts- und Steuerstrafrecht, 5. Auflage, München 2020

Wacher Lentz, Lene/*Sunde*, Nina: The use of historical call data records as evidence in the criminal justice system – lessons learned from the Danish telecom scandal, Digital Evidence and Electronic Signature Law Review (2021) Vol 18, S. 1 ff.

Wackernagel, Udo/*Graßie*, Christian: Die Beauftragung von IT-Forensikern im Ermittlungsverfahren: Zulässige Sachverständigenbeauftragung oder unzulässiges Outsourcing originärer Ermittlungstätigkeit?, NStZ 2021, S. 1 ff.

Walter, Dietmar: Sachverständigenbeweis zur Schuldfähigkeit uns strafrechtliche Überzeugungsbildung, Berlin 1978 (zit.: *Walter*, Sachverständigenbeweis)

Walter, Gerhard: Freie Beweiswürdigung, Tübingen 1979

Warken, Claudia: Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 2, Beweisverwertung im Zeitalter der digitalen Cloud und datenspezifische Regelungen in der StPO, NZWiSt 2017, S. 329 – 338

Wasserburg, Klaus: Anmerkung zu BGH StV 1989, S. 331 ff.

Wasserburg, Klaus: Das Einsichtsrecht des Anwalts in die kriminalpolizeilichen Spurenakten, NJW 1980, S. 2440 ff.

Wassermann, Rudolf (Hrsg.): Reihe Alternativkommentare, Kommentare zur Strafprozessordnung in drei Bänden. Bd. 1 (Einl – § 93) 1988, Bd. 2 Teilbd. 1 (§§ 94 – 212 b) 1992, Teilbd. 2 (§§ 213 – 275) 1993, Bd. 3 (§§ 276 – 477) 1996

Weber, Max: Gesammelte politische Schriften, 3. Auflage, Tübingen 1971

Weichert, Thilo: Big Data und Datenschutz – Chancenund Risiken einer neuen Form der Datenanalyse, ZD 2013, S. 251 – 259

Wellmann, Carl: Der Sachverständige in der Praxis, 6. Auflage, Düsseldorf, 1997

Wenskat, Wolfgang: Der richterliche Augenschein im deutschen Strafprozess, Frankfurt a. M. 1988

Wenzel, Henning: Rechtliche Grundlagen der IT-Forensik NZWiSt 2016, S. 85 ff.

Werner, Wibke: Schutz durch das Grundgesetz im Zeitalter der Digitalisierung, NJOZ 2019, S. 1041 ff.

Wess, Norbert/*Rohregger*, Michael: Der Sachverständige im Strafverfahren – Jüngste Entwicklungen in der Rechtsprechung des OGH, JSt 2014/3, S. 200 ff.

Wetterich, Paul: Der psychiatrische und psychologische Sachverständige im Strafverfahren – aus der Sicht des Strafrechtspraktikers – in: Kriminologische Gegenwartsfragen, Heft 12, Kriminologie und Strafverfahren, Neuere Ergebnisse zur Dunkelfeldforschung in Deutschland, Bericht über die XVIII. Tagung der Gesellschaft für die gesamte Kriminologie vom 9. Bis 12.10.1975 in Freiburg, hrsg. Göppinger, H./ Kaiser, G., Stuttgart 1976, S. 99 ff.

Wetzell, Georg Wilhelm: System des ordentlichen Civilprocesses, 3. Auflage, Leipzig 1878

Wie, Michael/*Grupp*, Laura/*Spada*, Frederick/*Swanson*, Steven: Reliably Erasing Data from Flashbased Solid State Drives, in: USENIX 2011

Wiegmann, Barbara: Ablehnung von Mitarbeitern der Strafverfolgungsbehörden als Sachverständige (§ 74 StPO), StV 1996, S. 570 ff.

Wigmore, Henry: Science of Judicial Proof, Brown 1937

Wimmer, August: Überzeugung, Wahrscheinlichkeit und Zweifel, DRZ 1950, S. 192 ff.

Witter, Hermann: Die Beurteilung Erwachsener im Strafrecht, in: Göppinger, H./Witter, H., Handbuch der forensischen Psychiatrie, Bd. 2, Teil C „Die forensischen Aufgaben der Psychiatrie“, Berlin 1972, S. 966 ff.

Witter, Hermann: Grundriss der gerichtlichen Psychologie und Psychiatrie, Berlin 1970

Wohlers, Wolfgang: Entstehung und Funktion der Staatsanwaltschaft, – Ein Beitrag zu den rechtshistorischen und strukturellen Grundlagen des reformierten Strafverfahrens, Berlin 1994

Wolf, Thomas: Der Sachverständige im Wirtschaftstrafverfahren, ZWH 2012, S. 125 ff.

Wolfslast, Gabriele: Die Gutachtenpraxis des Gerichtsärztlichen Ausschusses für NRW, dargestellt am Beispiel der beanstandeten Gutachten des Jahres 1976, MKrim 1979, S. 79 ff.

Wolschke, Heinz Günther: Leitgesichtspunkte zur Sachverständigenbeziehung im Strafprozess, Diss. Freiburg 1973

Wolter, Jürgen: Datenschutz und Strafprozess – Zum Verhältnis von Polizeirecht und Strafprozessrecht, ZStW 107 (1995), S. 793 ff.

Wüst, Herbert: Richter und psychologischer Sachverständiger im Strafprozess, Diss. München 1968

Zachariae, Heinrich: Handbuch des deutschen Strafprocesses, Bd. 1, Göttingen 1860; Bd. 2, Göttingen 1868 (zit.: *Zachariae*, II)

Zapf, Patricia/*Dror*, Itiel: Understanding and mitigating bias in forensic evaluation: Lessons from forensic science, International Journal of Forensic Mental Health (2017), S. 227 ff.

Zimmermann, Christian/*Spreitzenbart*, Michael/*Schmitt*, Sven/*Freiling*, Felix: Forensic Analysis of YAFFS2 in: GI Sicherheit (2012)

Zimmermann, Peter: Sachverständigenpflichten, DS 2006, S. 304 ff.

Zopfs, Jan: Der Grundsatz „in dubio pro reo", Baden-Baden 1999

Zuckerman, A.A. S.: The Principles of Criminal Evidence, Oxford 1989

Zweig, Katharina: Ein Algorithmus hat kein Taktgefühl – Wo künstliche Intelligenz sich irrt, warum uns das betrifft und was wir dagegen tun können, München 2019

Zwiehoff, Gabriele: Das Recht auf einen Sachverständigen, Baden-Baden 2000

Stichwortverzeichnis