

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

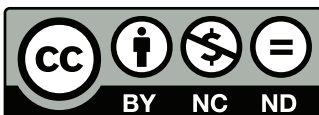
Der Fachbereich Rechtswissenschaft
der Friedrich-Alexander-Universität Erlangen-Nürnberg hat diese Arbeit
im Jahre 2024 als Dissertation angenommen.

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

Dieses Werk wurde auf Basis der Open Access-Lizenz CC BY-NC-ND 4.0
(s. <https://creativecommons.org/licenses/by-nc-nd/4.0/>) veröffentlicht. Die E-Book-
Version ist unter <https://doi.org/10.3790/978-3-428-59431-3> abrufbar.



Alle Rechte vorbehalten
© 2025 Nicole Scheler

Erschienen bei: Duncker & Humblot GmbH, Berlin
Satz: L101 Mediengestaltung, Fürstenwalde
Druck: CPI books GmbH, Leck
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

1. Teil

Einführung 19

- A. Skizzierung der Forschungsfragen 21
- B. Gang der Untersuchung 26

2. Teil

Grundlegendes zum IT-Sachverständigenbeweis im deutschen Strafverfahren 29

- A. Die Dringlichkeit der Diskussion um das Thema des IT-Sachverständigenbeweises 29
- B. Die deutsche StPO und der Sachverständigenbeweis 52

3. Teil

Die Beschaffung des Tatsachenstoffes: Die forensische Informatik 221

- A. Die forensische Wissenschaft 223
- B. Die forensische Informatik (als Teil der klassischen Forensiken) 229
- C. Zusammenfassung „Die Beschaffung des Tatsachenstoffes: Die forensische Informatik“ 293

4. Teil

Die Beweismwürdigung des IT-Sachverständigenbeweises 295

- A. Grundlage der tatrichterlichen Überzeugung 301
- B. Die Würdigung von IT-Sachverständigenaussagen 343
- C. Vagheiten in der Person des Richters 362
- D. Ideen für eine Verbesserung 368

*5. Teil***Zusammenfassung** 374

- A. Passt die tatsächlich ausgeführte Praxis der IT-Sachverständigen (noch) unter die Strafverfahrensvorschriften? 374
- 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? ... 377
- C. Wie sieht eine revisionssichere Beweiswürdigung des IT-Sachverständigenbeweises aus? 378

*6. Teil***Ein Ausblick** 381**Literaturverzeichnis** 384**Stichwortverzeichnis** 412

Inhaltsverzeichnis

1. Teil

Einführung	19
A. Skizzierung der Forschungsfragen	21
B. Gang der Untersuchung	26

2. Teil

Grundlegendes zum IT-Sachverständigenbeweis im deutschen Strafverfahren	29
A. Die Dringlichkeit der Diskussion um das Thema des IT-Sachverständigenbeweises	29
I. Digitale Beweismittel	31
II. Zahlen und Praxisbeispiele	32
III. Die Besonderheit der forensischen Informatik	35
1. Die Abgekoppeltheit von der physischen Welt	36
2. Die Universalität	39
IV. Der IT-Sachverständige als bestmögliches und sachnächstes Beweismittel	40
V. Die Lücke im wissenschaftlichen Diskurs zum IT-Sachverständigenbeweis	48
VI. Zusammenfassung „Dringlichkeit der Diskussion um das Thema des IT-Sachverständigenbeweises“	51
B. Die deutsche StPO und der Sachverständigenbeweis	52
I. Die Wahrheitsfindung im Strafverfahren	52
1. Der Wahrheitsbegriff	53
2. Der Umfang der Wahrheitserforschung i. S. d. § 244 Abs. 2 StPO	61
3. Die Rationalisierung des Wahrheitsfindungsprozesses	65
II. Der IT-Sachverständige im Strafverfahren	67
1. Der Begriff des „Sachverständigen“	67
2. Auftrag und Auswahl	70
a) Die Grenzen der eigenen Sachkunde des Auftraggebers	72
b) Die möglichen Auftraggeber	81
c) Die Auswahl	86

aa)	Der Sachverständigenpool	86
bb)	Die besondere Sachkunde	90
cc)	Die persönliche Eignung	95
dd)	Die Pflicht zur Objektivität, vgl. § 79 Abs. 2 StPO	96
ee)	Urteilsverzerrungen („bias“)	97
d)	Die Ernennung (Form der Bestellung)	101
e)	Der Begutachtungszwang	104
f)	Die Übertragung des Auftrags auf andere (Hilfs-)Personen	107
3.	Art und Umfang der Gutachtenerstattung	111
a)	Die Art der Gutachtenerstattung	111
b)	Der Umfang der Gutachtenerstattung anhand des Beweisthemas	112
aa)	Das Beweisthema als Tatsachenbehauptung	112
bb)	Die Trennung zwischen Rechts- und sonstigen Tatsachenbehauptungen	113
cc)	Die verschiedenen Tatsachentypen im Rahmen der Gutachtenerstattung	116
c)	Die Formulierung des Beweisthemas im Untersuchungsauftrag .	119
aa)	Das Problem der Kommunikation und Übersetzung	122
bb)	Das Problem des „Primens“	126
cc)	Fazit	127
d)	Die verschiedenen Aussagekategorien des Sachverständigenbeweises	127
aa)	Die erste Kategorie: Die Mitteilung von abstrakten Erfahrungssätzen	129
bb)	Die zweite Kategorie: Das Ziehen von Schlussfolgerungen aus konkreten Tatsachen des Prozesses mithilfe von Sachkunde	131
cc)	Die dritte Kategorie: Die Ermittlung konkreter Tatsachen, zu deren Wahrnehmung bzw. Feststellung besondere Sachkunde benötigt wird	134
dd)	Die Vornahme bloßer Verrichtungen	136
ee)	Fazit	138
III.	Die Abgrenzung zu anderen Prozessrollen	138
1.	Die Abgrenzung zu Richterinnen	140
2.	Die Abgrenzung zu (sachverständigen) Zeugen	141
a)	Die Rolle des (sachverständigen) Zeugen im Strafverfahren ...	142
b)	Die Abgrenzung zu Ermittlungspersonen	144
c)	Die Abgrenzung zum Augenscheinsgehilfen	146
d)	Unterschiedliche Rechte- und Pflichtenkataloge	148
3.	Abgrenzungskriterien	152
4.	Fazit	158
IV.	Der Versuch einer Kategorisierung und Bewertung der IT-Sachverständigentätigkeit aus juristischer Perspektive	158

1. Aus Sicht der Strafverteidiger	159
2. Eine Stellungnahme	162
3. Aus Sicht der Strafrichterinnen	163
a) Leitlinien zur Bestimmung der Sachverständigentätigkeit	163
b) OLG Schleswig, Beschluss vom 10.1.2017 – 2 Ws 441/16	164
c) LG Hamburg, Beschluss vom 7.8.2019 – 631 Qs 27/19	167
d) OLG Saarbrücken, Beschluss vom 20.9.2018 – 1 Ws 104/18 ...	169
e) Weitere Rechtsprechungsentwicklung	170
4. Eine Stellungnahme	170
V. Einflussmöglichkeiten der Verfahrensbeteiligten auf den bestellten Sachverständigen	171
1. Die dominierende Stellung der Staatsanwaltschaft im Ermittlungsverfahren	172
2. Ausgleichsmechanismen	176
a) Antragsrechte der Verfahrensbeteiligten	176
b) Die Einsicht in das schriftliche Gutachten und in die Arbeitsunterlagen	180
aa) Die Einsicht in das Sachverständigengutachten nach § 147 StPO	182
bb) Die Einsicht in die Arbeitsunterlagen nach § 147 StPO bzw. unter Berücksichtigung des Rechts auf ein faires Verfahren	183
cc) Fazit	188
c) Die Ablehnung des IT-Sachverständigen	189
aa) Ablehnungsrecht nach § 74 Abs. 1 S. 1 StPO i.V.m. § 22 Nr. 4 Var. 1 und 2 StPO	191
bb) Ablehnungsrecht nach § 74 Abs. 1 S. 1 StPO i.V.m. § 24 StPO	194
cc) Der abgelehnte Sachverständige	196
d) Fazit	201
VI. Die Grenzen der Sachverständigentätigkeit	201
1. Grenzen durch den Rahmen des Auftrags	203
2. Keine eigenen Ermittlungen	203
3. Die rechtsstaatliche Bindung bei der Durchführung des Gutachtenauftrags	205
4. Konsequenzen und weitere Sanktionen gegen den IT-Sachverständigen	210
VII. Die Leitung des Sachverständigen, § 78 StPO	211
1. Die Informationsbasis für die Sachverständigentätigkeit	213
2. Achtung der Weisungsfreiheit des Sachverständigen	216
3. Vorrang der Methodik mit bekannter Funktionalität	217
4. Checklisten	218
VIII. Zusammenfassung „Die deutsche StPO und der Sachverständigenbeweis“	219

3. Teil

Die Beschaffung des Tatsachenstoffes:	
Die forensische Informatik	221
A. Die forensische Wissenschaft	223
I. Die wissenschaftliche Methode	224
II. Der Grundsatz der Nachvollziehbarkeit und Transparenz der Forensik	227
B. Die forensische Informatik (als Teil der klassischen Forensiken)	229
I. Definition der „forensischen Informatik“ und ihre Aufgaben	230
II. Digitale Spuren im forensischen Prozess	232
1. Information und Träger	233
2. Die Entstehung digitaler Spuren	235
3. Eigenschaften digitaler Spuren	237
a) Flüchtigkeit	237
b) Technische Vermeidbarkeit	238
c) Manipulierbarkeit	239
d) Kopierbarkeit	241
e) Semantik	242
f) Big data	244
g) Verschlüsselungstechnologien	245
4. Fazit	246
III. Der forensische Prozess („the journey from data to evidence“)	246
1. Die Sicherung digitaler Spuren	248
a) Isolation des Beweismittels	249
b) Abstraktionsschichten	250
c) Fazit	252
2. Die Analyse digitaler Spuren	252
a) Ein Beispiel für den Ablauf einer Datenträger-Analyse	254
b) Datenanalyse-Methoden	257
aa) Deterministische Methoden	257
bb) Statistische Methoden	258
cc) Machine learning-Methoden	259
c) Folgen für das Beweisrecht	260
3. Die Rekonstruktion des Tathergangs mit Assoziation mithilfe digitaler Spuren	260
a) Die Quantifizierung der Irrtumswahrscheinlichkeit	261
b) Identifizierung/Klassifizierung/Individualisierung/Assoziation	263
c) Beispiele (USB/Browser)	265
d) Verwendung von Wahrscheinlichkeiten	267
e) Fazit	271
4. Die Präsentation	272
5. Die Standards der forensischen Informatik	277

a) Die Integrität und Authentizität von digitalen Spuren	281
aa) Die Integrität digitaler Spuren	282
bb) Die Authentizität digitaler Spuren	282
cc) Die zugrundeliegenden Annahmen	283
dd) Organisatorische und technische Maßnahmen	284
b) Die (korrekte) Verwendung von wissenschaftlich verifizierten Methoden	285
c) Erforderliche Sachkunde des Forensikers	285
d) Die Wiederholbarkeit und Reproduzierbarkeit der Ergebnisse . .	286
e) Die Mitteilung über mögliche und nicht mögliche Schlussfolge- rungen und Fehlerquellen	286
f) Die Dokumentation	287
aa) Exkurs: Die Zeitstempel	288
bb) Exkurs: Chain of custody	289
g) Einhaltung der verfahrensrechtlichen Grenzen	290
h) Die Bedeutung für das Beweisrecht	290
IV. Zusammenfassung „Die forensische Informatik (als Teil der klassi- schen Forensiken)“	291
C. Zusammenfassung „Die Beschaffung des Tatsachenstoffes: Die forensische Informatik“	293

4. Teil

Die Beweismwürdigung des IT-Sachverständigenbeweises	295
A. Grundlage der tatrichterlichen Überzeugung	301
I. Das Beweismaß der tatrichterlichen Überzeugung	302
II. Die persönliche Gewissheit	303
III. Die Regeln der praktischen Rationalität	305
1. Vollständige Beweismwürdigung	305
2. Allgemeine Regeln des schlussfolgernden Denkens	306
3. Auswirkungen der Einhaltung der forensischen Standards	307
4. Die objektiven Elemente zur Bestimmung der persönlichen Gewiss- heit	310
a) Die Nähe der Tatsachen zum Sachverhalt	311
b) Der Beweiswert des Indizes	311
aa) Ein Beispielfall	312
bb) Die Fragentrias in Bezug auf das Belastungs- oder Entlas- tungsindiz	313
cc) Die Beweiskraft des Indizes	315
(1) Die Zuverlässigkeit der zugrundeliegenden Richtig- keitswahrscheinlichkeit	317
(2) Die Zuverlässigkeitsskala	318

(a)	Gesicherte wissenschaftliche Erkenntnis	319
(b)	Standardisierte Verfahren	321
(c)	Neue wissenschaftliche Erkenntnisse und Untersuchungsmethoden	327
(d)	Wissenschaftliche Erkenntnis mit wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit	327
(e)	Sonstige Erfahrungssätze	330
(f)	Die Folgen von Blackbox-Tools für die Beweiswürdigung	332
(3)	Fazit und Ideen zur Verbesserung	335
dd)	Die Belastungswahrscheinlichkeit	337
c)	Zwischenergebnis	339
5.	Darstellung in den Urteilsgründen, § 267 StPO	340
IV.	Zusammenfassung „Grundlagen tatrichterlicher Überzeugung“	342
B.	Die Würdigung von IT-Sachverständigenaussagen	343
I.	Die Würdigung trotz mangelnder Sachkunde des Richters	346
II.	Die Würdigung des untersuchten Sachverhalts des Sachverständigen (1. Schritt)	348
1.	Erste Kategorie (Erfahrungssätze)	349
a)	Ungeprüfte Übernahme der Bedingungsverhältnisse und Wahrscheinlichkeitsrelationen?	350
b)	Tiefenstruktur des Erfahrungssatzes	351
2.	Zweite Kategorie (Befundbewertung)	352
a)	Falsche Einschätzungen des Erfahrungssatzes	352
b)	Trennung zwischen Rechts- und sonstigen Tatsachen	355
3.	Dritte Kategorie (Befundgewinnung/Ergebnisse von Datenverarbeitungsvorgängen)	357
III.	Die Würdigung der Person des Sachverständigen (2. Schritt)	358
1.	Kriterien für die Vertrauenswürdigkeit von Aussagepersonen (Die Drei Faktoren)	359
2.	Qualifikation des IT-Sachverständigen	360
3.	Fazit	362
C.	Vagheiten in der Person des Richters	362
I.	Fehler im Vorgang der Beweisbewertung	363
II.	Feststellbarkeit von Fehlern innerhalb des Vorgangs der Überzeugungsbildung	367
D.	Ideen für eine Verbesserung	368

Inhaltsverzeichnis	17
--------------------	----

5. Teil

Zusammenfassung	374
------------------------	-----

A. Passt die tatsächlich ausgeführte Praxis der IT-Sachverständigen (noch) unter die Strafverfahrensvorschriften?	374
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? ...	377
C. Wie sieht eine revisionssichere Beweiswürdigung des IT-Sachverständigenbeweises aus?	378

6. Teil

Ein Ausblick	381
---------------------	-----

Literaturverzeichnis	384
-----------------------------------	-----

Stichwortverzeichnis	412
-----------------------------------	-----

Abbildungsverzeichnis

Abbildung 1:	„Die objektive Stärke der tatrichterlichen Überzeugung i. S. d. § 261 StPO“	67
Abbildung 2:	„Ping-Pong Spiel“	121
Abbildung 3:	„Prozess des Auftrags“	124
Abbildung 4:	„Die verschiedenen Aussagekategorien“	128
Abbildung 5:	„Abgrenzung zwischen (sachverständigen) Zeugen und den Sachverständigen“	157
Abbildung 6:	„Möglicher Ablauf einer IT-forensischen Untersuchung“	222
Abbildung 7:	„Die wissenschaftliche Methode“	225
Abbildung 8:	„Der digitale Tatort“	236
Abbildung 9:	„Der forensische Prozess“	247
Abbildung 10:	„Die Abstraktionsschichten von Datenträgern“	250
Abbildung 11:	„Zuverlässigkeitsskala“	317

1. Teil

Einführung

IT ruft bei den Menschen¹ 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 „AI 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 Richterinnen 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 ausreichen. 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 Anrufrufdatenaufzeichnungen⁷, E-Mails und Social-Media Beiträgen⁸ oder Bildern von Google Earth und YouTube-Videos⁹ 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.*, Urte. 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.*, Urte. 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*, Urte. 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].