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

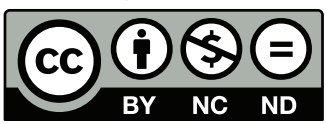
Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) –
Projektnummer 393541319

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: 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

Inhaltsverzeichnis

3. Teil

Die Beschaffung des Tatsachenstoffes: Die forensische Informatik 221

5. Teil

6. Teil

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].