MASTER KRIMINOLOGIE KRIMINALISTIK UND POLIZEIWISSENSCHAFT

MAKRIM

RUHR UNIVERSITÄT BOCHUM

RUB

MAKrim XV (2019)

Masterarbeit

zur Erlangung des akademischen Grades

Master of Criminology, Criminalistics and Police Science (M.A.)

Digitale Spuren - Herausforderungen und Risiken für die polizeiliche Ermittlungsarbeit

– Eine Analyse und kritische Reflexion in Zeiten ubiquitärer Digitalisierung –

Erstbetreuung: LKD Dr. Holger Plank

Zweitgutachter: Henrik Englberger

Vorgelegt von:

Andre Fiedler

Matrikelnummer 108118203223

E-Mail: andre@balticnetwork.de

Kurzzusammenfassung

Diese Arbeit befasst sich mit den Risiken und Herausforderungen, aber auch mit den Chancen der im Zuge der digitalen Transformation[1] in nahezu jedem Deliktsbereich und in verschiedensten Formen auftretenden digitalen Spuren im Kontext polizeilicher Ermittlungsarbeit. Da sich durch neue Generationen digitaler Technologien auch kontinuierlich die Art und Anzahl digitaler Spuren erhöht, beeinflussen diese die polizeiliche Ermittlungsarbeit zunehmend. Nach einer kurzen Einführung in die Thematik der Spuren im Allgemeinen wird grundlegend die Problematik beleuchtet, welche Besonderheiten digitale Spuren aufweisen und welche Arten den Alltag polizeilicher Ermittlungsarbeit betreffen. Als Synthese hieraus ergibt sich bereits die Erkenntnis, dass digitale Spuren nicht wie ihre analogen Pendants ihren Schwerpunkt im rein kriminaltechnischen Kontext haben, sondern die polizeiliche Ermittlungsarbeit in einem viel breiteren Spektrum durchziehen. Aus dieser Erkenntnis heraus ergeben sich die zentralen Hypothesen und Forschungsfragen. Diese Arbeit untersucht zum einen, welche Kompetenzanforderungen digitale Spuren an die polizeiliche Ermittlungsarbeit stellen und zum anderen, ob die Institution Polizei diesen Anforderungen personell und strukturell gewachsen ist. In diesem Zusammenhang wird auch erörtert, ob und wie Essenzen aus bereits bewährten Lösungsansätzen außerhalb der Polizei für eine zukunftsfähige Ermittlungsarbeit gewonnen werden können.

Schlüsselbegriffe:

Kriminalistik, Digitalisierung, digitale Transformation, digitale Spuren, digitale Ermittlungen, Computerforensik, Internet of Things, IoT, VUKA, Polizei, Polizeiausbildung, IT-Forensik

[1] Die digitale Transformation bezeichnet den gesamtgesellschaftlichen Wandel, welcher durch die zunehmende digitale Durchdringung der Lebens- und Arbeitswelt begründet ist. Dahm und Walther beispielsweise sehen in der digitalen Transformation die Digitalisierung und Abstimmung unterschiedlichster Prozesse aufeinander, um Kunden möglichst individuelle und auf sie zugeschnittene Erlebnisse bieten zu können (vgl. Dahm und Walther, 2019). Krcmar definiert die digitale Transformation gar als unausweichlich, unumkehrbar, ungeheuer schnell voran schreitend und unsicher im Detail (vgl. Krcmar, 2018).

Abkürzungsverzeichnis

ACPO	Association of Chief Police Officers
BIOS	Basic Input/Output System
BKA	Bundeskriminalamt
BMBF	Bundesministeriums für Bildung und Forschung
BtM	Betäubungsmittel
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CaaS	Crime-as-a-Service
CCK	Cybercrime-Konvention
CMOS	Complementary Metal Oxid Semiconductor
DNA	Desoxyribonukleinsäure (Englisch: deoxyribonucleic acid)
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FHöVPR	Fachhochschule für öffentliche Verwaltung Polizei und Rechtspflege des Landes Mecklenburg-Vorpommern
FAU	Friedrich-Alexander-Universität Erlangen-Nürnberg
FHVD	Fachhochschule für Verwaltung und Dienstleistung
Fn.	Fußnote
gem.	gemäß
GG	Grundgesetz
HfPV	Hessische Hochschule für Polizei und Verwaltung
HSPV NRW	Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
i. d. R.	in der Regel
IoT	Internet der Dinge [Englisch: Internet of Things]
ISO	International Standardization Organisation
IT	Informationstechnologie

IuK	Information und Kommunikation
KI	Künstliche Intelligenz
LKA	Landeskriminalamt
MIC	Machine Identification Code
Mrd.	Milliarden
NIJ	National Intitute of Justice
NIST	National Institute of Standards and Technology
NRW	Nordrhein-Westfalen
OPAC	Online Public Access Catalogue
OSI	Open System Interconnection
OSINT	Open Source Intelligence
PaaS	Platform as a Service
PDV	Polizeidienstvorschrift
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PWC	PricewaterhouseCoopers
RAM	Random-Access Memory
RFC	Request for Comments
Rn.	Randnummer
RUB	Ruhr-Universität Bochum
SaaS	Software as a Service
sog.	sogenannte | sogenannter | sogenanntes
StPO	Strafprozessordnung
u. a.	unter andere[m,n]
u. U.	unter Umständen
VS-NfD	Verschlusssachen - Nur für den Dienstgebrauch
WLAN	Wireless Local Area Network
VUKA	Volatilität, Unsicherheit, Komplexität und Mehrdeutigkeit
z. T.	zum Teil

Genderhinweis

In der vorliegenden Arbeit werden geschlechtsneutrale Formulierungen bevorzugt. Textpassagen, an denen aus sprachästhetischen Gründen die männliche Form (generisches Maskulinum) gewählt wurde, gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter, sollen als neutral verstanden werden und beinhalten keinerlei Wertung.

Inhaltsverzeichnis

1 Einleitung **1**

1.1 Motivation und Zielsetzung 1
1.2 Hypothesen und Forschungsfragen 4
1.3 Methodik 6
1.4 Aufbau der Arbeit 7

2 Begriffsbestimmungen **8**

2.1 Spurenbegriffe 9
2.2 Spureninformation und Spurenträger 10
2.3 Entstehung und Übertragung von Spuren 11
2.4 Spurenkategorien 12
2.5 Assoziation einer Spur 15

3 Digitale Spuren **17**

3.1 Definition 18
3.2 Besonderheiten digitaler Spuren 20
3.2.1 Entstehung digitaler Spuren 21
3.2.2 Abstraktionsschichten 23
3.2.3 Information und Träger digitaler Spuren 25
3.3 Eigenschaften digitaler Spuren 27
3.3.1 Flüchtigkeit 27
3.3.2 Kopierbarkeit 28
3.3.3 Manipulierbarkeit 29
3.3.4 Integrität und Authentizität digitaler Spuren 30
3.4 Kategorien digitaler Spuren 33
3.4.1 Persistente digitale Spuren 35
3.4.2 Semipersistente digitale Spuren 37
3.4.3 Transiente digitale Spuren 39
3.4.4 Remote- bzw. Onlinespuren 41
3.5 Zusammenspiel digitale Spuren / Ermittlungsarbeit 48
3.6 Zwischenfazit 50

4 Chancen und Herausforderungen digitaler Spuren 52
4.1 Integration digitaler Spuren in den Kontext polizeilicher Ermittlungshandlungen 53
4.1.1 Sicherungs- und Auswertungsangriff 57
4.1.2 Durchsuchung 59
4.1.3 Von der digitalen Spur zur digitalen Ermittlung 63
4.1.4 Einbindung externer Dienstleister 64
4.1.5 Zwischenfazit 66
4.2 Erforderliche Qualifikationen und digitale Kompetenz 67
4.2.1 Kompetenzbegriff 67
4.2.2 Digital-Forensik und Digitale Ermittlungen 68
4.2.3 Anforderungen an Kompetenz und Qualifikation 70
4.3 Status Quo und notwendige Konsequenzen 71
4.3.1 Digitale Kompetenzen von Kriminalist*innen 72
4.3.2 derzeitige Personal(gewinnungs)strategien 73
4.3.3 Weiterentwicklung der Aus- und Fortbildung 75
4.3.4 Rekrutierung von Spezialisten 78
4.3.5 Flexibilisierung des Anforderungsprofils bzw. Wandel des Berufsbildes 79
4.3.6 Institutionelle Anpassungen 81

5 Schlussbetrachtung und Ausblick 84

6 Literatur 89

1 Einleitung

1.1 Motivation und Zielsetzung

Nahezu alle Lebens- und Arbeitsbereiche sind in der heutigen Zeit von der Digitalisierung, also der Umwandlung analoger Inhalte und Prozesse in eine digitale Form, betroffen bzw. in großem Maße von ihr durchsetzt. Dies verdeutlicht sich im Privaten am Beispiel von Urlaubsfotos, welche in noch nicht allzu fernen Zeiten nach dem Entwickeln[2] im Kollegenkreis gezeigt oder gar zusammen mit Freunden auf Dia-Abenden[3] geschaut wurden, heute jedoch fast ausschließlich mit Digitalkameras und Smartphones aufgenommen und in sozialen Netzwerken hochgeladen werden. Eine Bildnachricht mit Urlaubsgrüßen per Messenger ersetzt die Urlaubspostkarte, während man gleichzeitig von jedem Punkt der Erde aus mit dem Smartphone die Temperatur des Kühlschranks überwachen und die Versorgung der Zimmerpflanzen mit Wasser steuern kann. In der Arbeitswelt wiederum bringt die Digitalisierung vor allem eine Vernetzung aller Prozesse mit sich – ein beliebtes Schlagwort ist hier die sogenannte „Industrie 4.0“[4]. Das Bezahlen mit dem Smartphone oder den sogenannten Kryptowährungen[5] erlangt eine weiter wachsende Akzeptanz, große Dienstleister testen die automatisierte Auslieferung von Waren und Sendungen per Drohne. Schlussendlich zeigt sich die jüngste Entwicklung in einer unzähligen Menge smarter Geräte[6] und dem sogenannten „Internet der Dinge [Englisch: Internet of Things] (IoT)“[7]. Zweifelsohne ist die Durchdringung des

[2] Die klassische analoge Fotografie umfasst eine Reihe physikalischer und chemischer Prozesse. Diese Prozesse, welche nach der Belichtung des Films zur Sichtbarmachung des Bildes stattfinden, werden als „Entwickeln“ bezeichnet.

[3] Diapositivfilm, kurz „Dia“ (von altgriechisch *dia* - deutsch ‚durch‘) genannt, ist ein lichtdurchlässiger Film, der zur Projektion genutzt wird.

[4] Industrie 4.0, oft auch die „vierte industrielle Revolution“ genannt, bezeichnet die intelligente Vernetzung von Maschinen und Abläufen in der Industrie mit Hilfe von Informations- und Kommunikationstechnologie. Die zentrale Instanz ist also nicht der Computer, sondern das Internet – durch die weltweite Vernetzung über Unternehmens- und Ländergrenzen hinweg gewinnt die Digitalisierung der Produktion eine neue Qualität (vgl. Voigt u. a., 2018, S. 333).

[5] Kryptowährungen sind digitale Währungen, welche wie herkömmliche Währungen getauscht und gehandelt werden können. Sie befinden sich jedoch außerhalb der Kontrolle finanzieller Institutionen und Regierungen.

[6] Als smarte Geräte oder auch Smart Devices werden Geräte bezeichnet, welche mit anderen Geräten über verschiedene Funkprotokolle verbunden sind. Beispiele hierfür sind Smartphones, Smartwatches oder auch Smartmeter (Stromzähler).

[7] Eine allgemeingültige Definition des IoT existiert nicht. Es bezeichnet u. a. ein System miteinander vernetzter, oftmals autark arbeitender elektronischer Geräte, mit denen sich Anwendungen automatisieren lassen. IoT umschreibt somit keine

Alltags durch den genannten technischen Fortschritt zu begrüßen, sie birgt aber auch unweigerlich Gefahren. So wächst mit der zunehmenden Technisierung auch die Menge an Daten, welche weder in ihrer Struktur noch in ihrer Art und dem Ort ihrer Speicherung für den einzelnen überschaubar ist. Nicht zuletzt steigt mit der Menge der Daten und ihrer permanenten Verfügbarkeit auch das Risiko des Missbrauchs.

Bis vor wenigen Jahren war das Aufkommen digitaler Spuren in der polizeilichen Ermittlungsarbeit überschaubar und durch überwiegend lokal und unverschlüsselt gespeicherte Daten gekennzeichnet. Es genügte, betreffende Geräte, auf denen ermittlungsrelevante Daten vermutet wurden, sicherzustellen und deren Datenträger mittels Post-Mortem-Analyse[8] der Gewinnung und Untersuchung von gelöschten, umbenannten oder versteckten Daten zu unterziehen. Das Aufkommen dieser Art von Spuren hat sich mit zunehmender Digitalisierung der Lebens- und Arbeitswelt in Form ihrer Qualität und vor allem ihrer Quantität grundlegend gewandelt. Feste und mobile Endgeräte mit permanenter Internet-Konnektivität, global verteilte (Cloud-)Speicher, Smart-Home im Kleinen und global vernetzte Firmen mit weltweit verteilten Standorten im Großen – sie alle speichern und verarbeiten Daten (nahezu durchgängig und sicher verschlüsselt) in immer umfangreicher werdender Menge. Gehen hiermit zwangsläufig technische Probleme einher, so ist oftmals auch die rechtliche Problematik eine zunehmende Hürde. Wo und in welcher Form sind digitale Spuren auffindbar? Ist die Beschlagnahme von im Ausland gespeicherten Daten durch die deutsche Strafprozessordnung sichergestellt? Dürfen (passwort-)geschützte Daten auf Cloudspeichern, in Postfächern oder Messenger-Diensten, für die betroffene Endgeräte die Zugriffsschlüssel darstellen, sichergestellt bzw. beschlagnahmt werden? Wie kann bei stetig anwachsenden Datenmengen auch in Zukunft eine effiziente Sicherung, Selektion und Auswertung erfolgen, d.h., inwiefern kann u. a. durch flächendeckende Nutzung von Automatisierung und künstlicher Intelligenz die zwangsläufig notwendige Ökonomisierung digitaler Ermittlungen erreicht werden?

in sich geschlossene Technologie, sondern vielmehr die Zusammenführung zahlreicher Technologien aus unterschiedlichen Feldern zu einem an der Anwendung orientierten Gesamtsystem (vgl. Hoch, 2019).

8 Bei der Post-Mortem- oder auch Offline-Analyse genannten Methode wird von Datenträgern mittels spezieller Software ein forensisches Duplikat (bitgenaue 1:1-Kopie) der nichtflüchtigen Daten vorgenommen. Sie kommt immer dann zum Einsatz, wenn die flüchtigen Daten (z. B. aus dem Arbeitsspeicher) nicht mehr gesichert werden können oder nicht relevant sind (vgl. Dolle, 2009, S. 186 ff.).

„Digitale Spuren machen im Zeitalter der digitalen Geräte bzw. der digitalen Kommunikation einen nicht unwesentlichen Anteil aller Ermittlungsansätze aus – oftmals sind sie sogar die einzigen Ermittlungsansätze. Diese Thematik wird künftig weiter an Bedeutung gewinnen, da immer mehr Menschen mit immer mehr Geräten immer mehr digital kommunizieren werden“ (Hahn, 2017, S. 4). Die beschriebene kontinuierlich fortschreitende Digitalisierung mit ihren neuen Herausforderungen und Möglichkeiten erfasst also die polizeiliche bzw. kriminalistische Arbeit in großer Breite, denn Systeme und Geräte sind nicht nur potentielle Spurenträger und Hinweisgeber, sondern oftmals selbst Ziel krimineller Handlungen. Die innerhalb dieses Kontextes entstehenden digitalen Spuren halten flächendeckend Einzug in die polizeiliche Ermittlungsarbeit und bestimmen zunehmend – und das macht sie so besonders – die Arbeit aller Polizist*innen und nicht nur einiger weniger Spezialist*innen. Im Gegensatz zu klassischen analogen Spuren, der Daktyloskopie[9] oder der DNA-Analytik, sind digitale Spuren nicht-körperlich bzw. virtuell und somit nicht unmittelbar wahrnehmbar. „Anders als ihre analogen Pendants müssen digitale Daten [. . .] einen oder mehrere Zwischenschritte durchlaufen, um überhaupt nutzbar zu sein“ (Momsen, 2015, S. 74). Neben den bereits oben erwähnten, oftmals nicht eindeutigen rechtlichen Rahmenbedingungen ergeben sich aus diesen Besonderheiten digitaler Spuren Fragen nach deren Wert und Qualität als Beweismittel sowie der damit verbundenen Reichweite zu führender Beweise (vgl. ebd., S. 72). Die Sicht- bzw. Nutzbarmachung digitaler Spuren und somit in gewisser Weise die „Manipulation“ bzw. „Herstellung“ eines Beweismittels ist ein äußerst kritischer Umstand und einzigartig für digitale Spuren. Dies bedarf, insbesondere bei der Sicherung und Aufbereitung flüchtiger und zeitlich begrenzt zur Verfügung stehender Daten, einer besonderen Sorgfaltspflicht in Bezug auf die Durchführung und Dokumentation der (digitalen) Spurensicherung zum Nachweis ihrer Authentizität.

Zweifelsohne gibt es die Notwendigkeit der technischen Erforschung, Erkennung und Sicherstellung digitaler Spuren. Dies ist Aufgabe der IT-Forensik bzw. der forensischen Informatik, deren Fachgebiet sich einer zunehmenden Popularität erfreut, was sich u. a. an der wachsenden Zahl IT-forensischer Studiengänge erkennen lässt[10]. Die forensische Informatik ist in der Wissenschaft

[9] Die Daktyloskopie ist ein kriminalistisches Verfahren zur Personenidentifizierung anhand der Papillarleistenabbilder (auch Papillarlinien genannt) von Fingern, Handflächen und in seltenen Fällen auch von Fußsohlen (vgl. Zirk und Vordermaier, 1998, S. 183 ff.).

[10] Der erste deutschen Master-Studiengang in digitaler Forensik wird seit dem Wintersemester 2010/2011 in einem Kooperationsprojekt mit der Friedrich-Alexander-

fest etabliert. Die Ubiquität digitaler Spuren in nahezu allen Deliktsbereichen hat trotz alledem zur Folge, dass sich für die polizeiliche Ermittlungsarbeit einerseits Risiken in Bezug auf Kompetenzdefizite, andererseits aber auch neue, kreative Handlungs- und Beweismöglichkeiten ergeben. Ihre Relevanz wird u. a. anhand medialer Publikationen deutlich (vgl. Hahn, 2017; Arnold, 2015; Hoch, 2019; Tecklenborg und Stupperich, 2018). Digitale Spuren weisen einen immateriellen, häufig flüchtigen Charakter auf und sind mehr als andere (insb. klassische materielle) Spurenarten der Gefahr ausgesetzt, nicht entdeckt zu werden. Eine kritische, im Schwerpunkt kriminalistisch-polizeiwissenschaftlich ausgerichtete Reflexion im notwendigen Umgang mit digitalen Spuren im sicherheitsbehördlichen Kontext bildet den engeren Fokus dieser Masterarbeit.

1.2 Hypothesen und Forschungsfragen

Der Begriff der Spur bedeutete für die polizeiliche Ermittlungsarbeit lange Zeit ein physisches, unmittelbar wahrnehmbares Vorkommen ebendieser. Zurückzuführen ist dies auf die Beobachtung des französischen Forensikers Dr. Edmond Locard (1877-1966), dass kein Täter einen Tatort verlassen kann, ohne Spuren zu hinterlassen. Jede Berührung hinterlässt zwangsläufig eine Spur. Klassische (analoge) Spuren entstehen somit durch eine Übertragung von Materie (z. B. Blut- oder Schmauchspuren, DNA-Material) oder Mustern (z. B. Kratzspuren von Werkzeugen oder Fingerabdrücke). Die polizeiliche Ermittlungsarbeit umfasst die Entdeckung, Sicherung und anschließende kriminaltechnische (forensische) Untersuchung von Spuren. Oftmals werden durch sie relativ einfache Fragestellungen beantwortet („Fußabdruck A passt zu Schuh B“, „Das Projektil X wurde aus der Waffe Y abgefeuert“ oder auch „Das an der Kleidung des Opfers gefundene DNA-Material ist das des Täters“.). Polizeiliche Ermittlungsarbeit und kriminaltechnische Laboruntersuchungen können getrennt voneinander erfolgen. Überdies sind neben der Einführung der Daktyloskopie und der DNA-Analytik keine nennenswerten Veränderungsprozesse aufgetreten, welche die Aufhebung dieser strikten Trennung von Ermittlungsarbeit und kriminaltechnischer Untersuchung erforderte.

Universität Erlangen-Nürnberg (FAU) an der Hochschule Albstadt-Sigmaringen angeboten. Es existieren eine Vielzahl weiterer Bachelor- und Masterstudiengänge, u. a. an der Hochschule Mittweida, der Hochschule Wismar oder der Universität Potsdam.

Hypothese 1: Digitale Spuren wiederum unterscheiden sich durch ihre besonderen Eigenschaften wie Flüchtigkeit, Kopierbarkeit und Manipulierbarkeit deutlich von ihren analogen Pendants. Aufgrund der nach wie vor weit fortschreitenden Digitalisierung treten sie in immer umfangreicherer und vielfältigerer Form in Erscheinung, d.h., es besteht eine wachsende Schwierigkeit ihrer Erkennung und Sicherung.

Hypothese 2: Zusätzlich besitzen digitale Spuren oftmals nicht aus sich selbst heraus eine direkte Beweiskraft, sondern entfalten diese erst nach Selektion, Interpretation und Einordnung in das (mögliche) Gesamtgeschehen einer Tat. Hierdurch besteht ein deutlicher Unterschied zu den klassischen analogen Spuren, so dass die bereits genannte strikte Trennung von Ermittlungsarbeit und kriminaltechnischer Laboruntersuchung nicht dauerhaft aufrecht erhalten werden kann. Dies lässt sich anhand eines Beispiels untermauern: „Sind auf dem Asservat Hinweise auf Kryptowährungen vorhanden?“ Diese Frage lässt sich zweifelsohne mit „ja“ bzw. „nein“ beantworten, führt aber zu keinem direkten Erkenntnisgewinn, da erst Informationen zu möglichen Zahlungsströmen im Zusammenhang mit gefundenen Spuren von Kryptowährungen zu weiteren Erkenntnissen führt.

Hypothese 3: So lässt sich bereits an dieser Stelle erkennen, dass digitale im Gegensatz zu analogen Spuren die Ermittlungsarbeit vollumfänglich durchdringen. Hieraus folgend begründen digitale Spuren mehrheitlich nachfolgende digitale Ermittlungen, so dass eine hohe digitale Kompetenz in der Breite der polizeilichen Tätigkeiten unverzichtbar ist.

Die Arbeitshypothesen bekräftigend, stehen insbesondere die nachfolgenden beiden ergänzenden Forschungsfragen im Bearbeitungsschwerpunkt der Masterarbeit:

- Welche Anforderungen stellen digitale Spuren an die Kompetenz polizeilicher Ermittlungsarbeit?
- Ist die Polizei strukturell und vor allen Dingen personell den Herausforderungen digitaler Spuren gewachsen?

Diese Fragen bilden gewissermaßen den roten Faden und ermöglichen in ihrer Anlage eine erweiterte kritische Reflexion der Arbeitshypothesen.

1.3 Methodik

Die Untersuchung der Hypothesen und Fragestellungen der Masterarbeit erfolgt mittels gezielter Literaturauswertung. Hierzu werden wissenschaftliche Publikationen u. a. aus den Bereichen der Kriminologie, der Kriminalistik sowie der Cybercrime und IT-Forensik analysiert und eingeordnet. Dies umfasst auch Veröffentlichungen aus wissenschaftlichen Zeitschriften (Journals). Aus dem umfangreichen Bestand verschiedener Datenbanken (u. a. OPAC[11] der Ruhr-Universität Bochum (RUB), KrimDok[12] der Universität Tübingen, Online-Archive der Zeitschriften „Kriminalistik", „der kriminalist") werden sozial-, kriminal- und polizeiwissenschaftliche Publikationen zur Bearbeitung herangezogen. Überdies bietet ein großer Umfang vorhandener Publikationen aus dem Bereich der IT-Forensik die Möglichkeit der fachlich-technischen Einordnung digitaler Spuren in den polizeilichen Ermittlungsprozess. Hinsichtlich der Hypothese 3 und der begleitenden Frage notwendiger Cyberkompetenz wird begleitend einschlägige polizeiwissenschaftliche Literatur beigezogen. Speziell für Kapitel 4 erweitert sich das Literaturportfolio um wirtschaftswissenschaftliche Publikationen, da die digitale Transformation[13] unausweichlich und unumkehrbar ist, ungeheuer schnell voranschreitet, mit Unsicherheit behaftet ist und somit auch Industrie und Wirtschaft vor gewaltige Herausforderungen stellt (vgl. Krcmar, 2018) und sich aus der Erfahrung in diesem Umfeld bewährter Konzepte Essenzen bzw. Symbiosen für die (zukünftige) polizeiliche Ermittlungsarbeit ergeben können.

---

11 Der Online Public Access Catalogue (OPAC) ist ein oftmals auch über das Internet verfügbares Tool zur Literaturrecherche in Beständen öffentlicher und wissenschaftlicher Bibliotheken.

12 https://krimdok.uni-tuebingen.de: KrimDok ist ein bibliographisches Nachweissystem kriminologischer Literatur.

13 Die digitale Transformation ist lt. International Business Machines Corporation (IBM) die zweite Phase eines stattfindenden digitalen Reifeprozesses, welcher sich aus der Digitalisierung, der bezeichneten Digitalen Transformation sowie der digitalen Neuerfindung zusammensetzt (vgl. Dahm und Walther, 2019; IBM Institute for Business Value, 2016). Insbesondere durch die digitale Transformation erfolgt die Übertragung des Menschen und seiner Lebens- und Arbeitswelt auf eine digitale Ebene. Diese ist gekennzeichnet durch Digitale Daten, Vernetzung, Automatisierung und digitale (Kunden-)Beziehungen (vgl. Rossberger, 2019, S. 22 f.).

1.4 Aufbau der Arbeit

Um sich dem Inhalt der Arbeit thematisch anzunähern, erfolgt in Kapitel 2 eine kurze, dennoch grundsätzliche theoretische und begriffliche Einführung zum Thema (klassischer analoger bzw. körperlicher) Spuren. Die mit ihnen in unmittelbarem Zusammenhang stehende Spurenkunde bildet den allgemeinen Teil der Kriminaltechnik und ist beweistechnisch außerordentlich wichtig und nach wie vor als Kernstück der modernen naturwissenschaftlichen Kriminalistik anzusehen (vgl. Zirk und Vordermaier, 1998, S. 13 f.). Auf dieser Vorbetrachtung aufbauend erfolgt in Kapitel 3 die Überleitung zu digitalen Spuren. Dieses Kapitel wird aufzeigen, welche Kongruenz zu klassischen Spuren besteht und in welcher Hinsicht sich digitale Spuren abgrenzen. Des Weiteren wird eine Klassifizierung digitaler Spuren erfolgen. Hierbei wird aufgezeigt, dass zwischen der Art und dem Ursprung einer digitalen Spur (Spurenträger), ihrer Kopierbarkeit, Flüchtigkeit und ihrer daraus resultierenden Beweiskraft ein unmittelbarer Zusammenhang besteht. Anhand dieser Klassifizierungen lassen sich die gegenwärtigen und zukünftigen Risiken und Herausforderungen ableiten und bieten einen Übergang zu Kapitel 4 und den beiden zentralen Forschungsfragen dieser Arbeit. Unter Nutzung der in Kapitel 3 gewonnenen Erkenntnisse erfolgt die Analyse, wie Einbindung digitaler Spuren in den Kontext kriminalpolizeilicher Ermittlungshandlungen erfolgen kann, denn hieraus ergeben sich die Antworten auf die erste Forschungsfrage, welche Anforderungen an die Kompetenz polizeilicher Ermittlungsarbeit bestehen[14]. Im Anschluss wird beleuchtet, ob die polizeiliche Ermittlungsarbeit diesen Herausforderungen sowie Risiken adäquat begegnet und welche Handlungsnotwendigkeiten (institutionell sowie personell) bestehen. Es wird in Kapitel 4 zudem ein „Blick über den Tellerrand hinaus geworfen“, denn das Thema Digitalisierung bzw. digitale Transformation[15] und die mit ihr einhergehende Innovationsgeschwindigkeit in sog. VUKA[16]-Umgebungen betrifft nicht nur die Strafverfolgungsbehörden, sondern ebenso Industrie und Wirtschaft.

---

14 siehe Abschnitt 1.2

15 siehe Fn. 13

16 Volatilität, Unsicherheit, Komplexität und Mehrdeutigkeit (VUKA) fasst die Herausforderungen zusammen, denen sich Unternehmen (und ebenso staatliche Institutionen) stellen müssen, um in einer zunehmend digitalisierten Welt bestehen zu können. Neue Technologien werden immer schneller entwickelt, was zur Folge hat, dass bewährtes Wissen und Erfahrung zunehmend endlicher wird. Lineares Denken und lineare Lösungen sind in dieser dynamischen, sich schnell verändernden Umgebung mehr Problem als Lösung zur Bewältigung (vgl. Lévesque und Vonhof, 2018; Bennett und Lemoine, 2014).

2 Begriffsbestimmungen

Für eine erste Annäherung und zur grundlegenden Einführung in die Thematik wird in diesem Kapitel ein grundsätzlicher, wenn auch kurzer Überblick zu den klassischen (physischen) Spuren gegeben. Der Umfang dieser Arbeit reicht selbstverständlich nicht aus, um dieses Themenfeld tiefgreifend zu bearbeiten. Es werden umrisshaft die wichtigsten Teilaspekte klassischer Spuren erörtert, da sich auf diesem Grundverständnis aufbauend die Besonderheiten digitaler Spuren deutlicher erschließen lassen.

„Nach deutschem Recht ist es Aufgabe des Gerichts, darüber zu entscheiden, ob eine Straftat als bewiesen gilt und der Tatverdächtige auch tatsächlich schuldiger Täter ist. Dies geschieht mit den strafprozessualen Beweismitteln und unter Beachtung bestimmter Beweisgrundsätze“ (Clages, 2019a, S. 55). Die Strafprozessordnung (StPO) kennt folgende Beweismittel (vgl. Meyer-Goßner und Schmitt, 2018, Einl Rn. 49):

- Zeugen (§§ 48ff StPO)
- Sachverständige und Augenschein (§§ 72ff StPO)
- Urkunden und andere Schriftstücke (§§ 249ff StPO)
- Aussagen des Beschuldigten (§§ 136, 163a I, 243 III StPO)

Zeugen berichten über sinnlich wahrgenommene Tatsachen, welche durch sie erlebt und in ihren geistigen Besitzstand aufgenommen wurden. Sachverständige ermöglichen durch ihre Sachkunde auf einem speziellen Wissensgebiet die richtige Auswertung festgestellter Tatsachen, während der richterliche Augenschein gem. § 86 StPO die sinnliche Wahrnehmung von Beweismitteln durch den Richter umfasst (vgl. Clages, 2019a, S. 60 ff.). Der Urkundenbeweis „[. . .] dient der Ermittlung des gedanklichen Inhalts eines Schriftstückes [. . .]; es kommt mittelbar derjenige zu Wort, der eine Aussage in die Urkunde gelegt hat“ (Meyer-Goßner und Schmitt, 2018, Einl Rn. 49). Des Weiteren wird zwischen den Formen des direkten und indirekten Beweises sowie zwischen Personalbeweis und Sachbeweis unterschieden. Ein direkter Beweis ergibt sich unmittelbar aus der beweiserheblichen Tatsache, beispielsweise aus der Aussagen von Zeugen. Bei einem indirekten Beweis muss erst von einer mittelbaren Tatsache, dem sogenannten Indiz, auf eine unmittelbar entscheidungserhebliche Tatsache geschlossen werden. Er wird auch als

Indizienbeweis bezeichnet (vgl. Clages, 2019a, S. 68 f.). Der Mensch ist Beweismittel des Personalbeweises (Zeugen, Sachverständige, Beschuldigte), somit ist der Personalbeweis gleichzeitig ein direkter als auch subjektiver Beweis, da er von der individuellen Wahrnehmbarkeit und Reproduzierbarkeit sowie der Wahrhaftigkeit einer Aussage abhängt (vgl. ebd., S. 70 f.). Zu den Sachbeweisen zählen der Augenschein und die Urkunde. Beweisgegenstände und beweiserhebliche wahrnehmbare Sachgegebenheiten werden durch die Einnahme des Augenscheins zur Kenntnis genommen (vgl. Meyer-Goßner und Schmitt, 2018, Einl Fn. 49). Ein Sachbeweis spricht, losgelöst vom eigentlichen Tathergang, aus sich selbst und lässt somit Schlüsse auf diesen zu. Er ist im Gegensatz zum Personalbeweis objektiv und mit naturwissenschaftlichen Methoden überprüfbar (vgl. Clages, 2019a, S. 71 f.). Clages liefert folgende Definition zum Beweismittel des Augenscheins: „Beweismittel des Augenscheins sind Sachen oder Sachgegebenheiten jeder Art, ferner der lebende Mensch, auch seine Verhaltensweisen und seine Reaktionsfähigkeit, also alles, was mit menschlichen Sinnen wahrgenommen werden kann“ (ebd., S. 62).

2.1 Spurenbegriffe

Im Strafverfahren wird die Beweisführung hauptsächlich durch den Sachbeweis in Form (materieller) Spuren getragen (vgl. ebd., S. 71). Eine Spur in diesem Sinne ist „[. . .] jede sinnlich wahrnehmbare Veränderung [. . .], soweit sie durch die Tatbegehung verursacht wurde“ (Zirk und Vordermaier, 1998, S. 52). Spuren im kriminaltechnischen Sinn[17] sind weiterhin Gegenstände, die nach § 94 I StPO als Beweismittel für die Untersuchung von Bedeutung sein können. Gegenstände sind bewegliche Sachen jeder Art, also auch Datenträger und Computerausdrucke sowie digital gespeicherte Informationen, aber auch unbewegliche Sachen wie Grundstücke oder Grundstücksteile (vgl. Meyer-Goßner und Schmitt, 2018, § 94 Rn. 4). Spuren werden grundlegend in die folgenden drei Arten eingeteilt: Tatspuren, Trugspuren sowie fingierte Spuren. Bei Tatspuren handelt es sich um gegenständliche Veränderungen, die mit einer Tat im Zusammenhang stehen (Eindrücke, Abdrücke, Material-

[17] Auf eine Einordnung der Kriminaltechnik als Fachdisziplin der Kriminalistik im System der Kriminalwissenschaften verzichtet diese Arbeit bewusst, da der Umfang hierfür nicht ausreicht. Stellvertretend sei auf eine prägnante und gleichzeitig kritische Auseinandersetzung mit der Kriminalistik von Plank verwiesen (vgl. Plank, 2017, S. 139 ff.).

und Situationsspuren). Trugspuren wiederum sind gegenständliche Veränderungen, welche nur dem Anschein nach mit der Tat zusammenhängen, während fingierte Spuren zur Täuschung der Ermittlungshandlungen verursachte Veränderungen darstellen (vgl. Zirk und Vordermaier, 1998, S. 48). Des Weiteren erfolgt zusätzlich zu ihrer Art eine Einteilung von Spuren in die folgenden Kategorien[18]: Formspuren, Materialspuren, Gegenstandsspuren und Situationsspuren. Zu guter Letzt werden Spuren auch nach ihrer Größe oder ihrer Herkunft bzw. Entstehung kategorisiert. Die Größe ist entscheidend, ob eine Spur mit bloßem Auge sichtbar ist (Makrospur) oder nicht (Mikrospur). Mikrospuren können beispielsweise Staub, feinste Lackpartikel oder auch Körperzellen sein. Spuren, die einzig aufgrund ihrer mangelnden Sichtbarkeit des Materialauftrages nicht direkt erkennbar sind (z. B. Fingerabdrücke), entfallen nicht in die Kategorie der Mikrospuren, da sie nach Sichtbarmachung mit dem bloßen Auge zu erkennen sind (vgl. Kawelovski, 2018, S. 24 ff.). Kategorien von Spuren bzgl. ihrer Herkunft bzw. Entstehung sind beispielsweise „menschliche Ein- und Abdruckspuren, Schuh- und Reifenspuren, Werkzeugspuren, körperzellenhaltige Spuren, digitale Spuren, textile Faserspuren, Schusswaffenspuren, Brandspuren, Vegetationsspuren und sonstige Spurenarten wie Geruchsspuren, Schriftspuren, chemische Stoffe, Rauschgifte etc.“ (ebd., S. 26). Resultierend aus diesen unterschiedlichen Systemen der Einteilung kann eine einzelne Spur somit mehreren Spurenbegriffen zugeordnet werden. So ist eine sichtbare Blutspur vom Täter gleichzeitig Tatspur, Makrospur, Formspur sowie serologische Spur (vgl. ebd., S. 27).

2.2 Spureninformation und Spurenträger

In der klassischen Forensik bzw. Kriminaltechnik wird zwischen dem Träger und der Information einer Spur unterschieden. Beim Träger einer Spur handelt es sich ganz allgemein um diejenige Materie, welche die Bedeutung einer Spur, also das, was sie aussagt, trägt, so dass es sich bei der Information einer Spur um ebenjene Bedeutung handelt. Und obwohl Spurenträger und Spureninformation zwei getrennte Parameter einer Spur sind, so besteht doch eine starke Verbindung zwischen ihnen, denn die Existenz einer analogen (bzw. körperlichen) Spureninformation ist ohne einen komplementären Spurenträger nicht möglich (vgl. Dewald und F. C. Freiling, 2015, S. 13 f.). Hierfür

[18] siehe Abschnitt 2.4

kommen Personen und Gegenstände – mobil wie immobil – in Frage. Dass ein Spurenträger auch mehr als eine Spureninformation enthalten kann, zeigt nachfolgendes Beispiel. Bei einem durch den Täter ausgedruckten Erpresserschreiben gestaltet sich die Unterscheidung zwischen Spurenträger und Spureninformation recht intuitiv. Das Papier und die Tinte des Druckers sind Träger der Spur, während die geschriebenen Worte die Spureninformation enthalten. Aber es gibt mitunter noch eine weitere, wenn auch nicht unmittelbar sichtbare Information, welche durch Drucker verursacht wird: den Machine Identification Code (MIC). Dieser wird bei fast allen handelsüblichen Farblaserdruckern mit auf das Papier gebracht. Es handelt sich hierbei um ein Muster aus winzigen gelben Punkten (Tracking Dots), welche mit dem bloßen Auge so gut wie nicht zu erkennen sind. Dieses Muster gibt Auskunft über den Hersteller des Druckers, die Seriennummer sowie das Datum und die Zeit des Ausdrucks. Der MIC ist mehrfach über die gesamte Seite eines Ausdrucks verteilt und kann durch Einscannen desselben und anschließender Bearbeitung des Scans mit einem Grafikprogramm sichtbar gemacht werden. So enthält ein ausgedrucktes Erpresserschreiben also nicht nur die Information der geschriebenen Worte, sondern unter Umständen auch Informationen über den verwendeten Drucker und liefert damit vielleicht indirekt Hinweise zum Verfasser des Schreibens (vgl. Salim und Abdalla, 2019). Final kann man also von einen Informationsgehalt einer Spur sprechen, welcher die Gesamtheit alle in ihr gespeicherten oder aus ihr hervorgehenden Informationen darstellt (vgl. Howorka, 2013, S. 1284).

2.3 Entstehung und Übertragung von Spuren

Das Grundprinzip der Entstehung von Spuren geht auf den Franzosen Edmund Locard[19] zurück, welcher in einem seiner Werke (Locard, 1930) die Beobachtung beschrieb, dass jeglicher Kontakt auch eine Spur hinterlässt. Niemand könne eine Straftat begehen, ohne eine Spur zu hinterlassen. So hinterlässt der Täter oder das Opfer etwas am Tatort bzw. nimmt etwas mit, oder Täter und Opfer tauschen untereinander Spuren aus. Dieser Austausch erfolgt bei klassischen körperlichen Spuren in Form von Materie oder in Form von Mustern. Als Grundvoraussetzung für die Übertragung von Materie gilt das Prinzip der Zerteilbarkeit. Ein Austausch von Materie ist nur möglich,

[19] Dr. Edmond Locard (1877 - 1966) war Arzt und Direktor eines französischen Polizeilabors in Lyon. (vgl. Hochschule Wismar, 2020)

wenn die Zerteilung von Objekten erfolgt. Dies geschieht, wenn ausreichend Kraft auf ein Objekt ausgeübt wird. Die Bestandteile nach der Zerteilung enthalten zum einen Eigenschaften, welche durch den Zerteilungsprozess selbst erzeugt wurden (z. B. Bruchkanten) und zum anderen die physisch-chemischen Eigenschaften des Ausgangsobjektes (vgl. Inman und Rudin, 2000, S. 87). Für eine Übertragung von Materie sind nach Inman und Rudin drei Objekte und zusätzlich Energie notwendig: Das Ausgangsobjekt, ein Fragment des Ausgangsobjektes sowie ein Zielobjekt, auf welches das Fragment des Ausgangsobjektes mithilfe der bezeichneten Energie übertragen wird (vgl. ebd., S. 94). Typischerweise handelt es sich bei Spuren, welche auf diese Art und Weise entstanden sind, um physisch sehr kleine, oftmals mikroskopische Einheiten. Beispielhaft zu nennen sind hier Haare, Fasern, Farbe oder Hautpartikel. Auch Locard hielt diese Art von Spuren für äußerst wichtig, da das Bewusstsein für ihre Verursachung nach seinen Vorstellungen nicht sehr ausgeprägt war. Neben diesem sogenannten Mikrotransfer erfolgt aber auch die Übertragung von größeren physikalischen Einheiten. In diese auch Makrotransfer genannte Kategorie fallen alle unmittelbar wahrnehmbaren Spuren wie beispielsweise der abgerissene Teil eines Kleidungsstückes oder der Farbabrieb eines Tatwerkzeuges. Die bereits benannte Übertragung in Form von Mustern entsteht, wenn Merkmale eines Gegenstandes auf einem hierfür empfänglichen Medium erzeugt werden. Zu nennen sind hier Schuhabdrücke, Reifenspuren oder Kratzspuren eines Tatwerkzeugs. Es werden also Merkmale eines Objektes anstatt Teile seiner Materie übertragen (vgl. ebd., S. 96). Ganz gleich, ob eine Spur durch Übertragung von Materie oder durch Übertragung von Mustern entstanden ist, erfolgt in jedem Fall eine Übertragung von Informationen über die Quelle einer Spur. Diese zu kennen erlaubt die Entscheidung, welche Informationen von Bedeutung sein können. So können bei einem unvollständigen Fingerabdruck (Übertragung von Mustern) ebenfalls verwertbare DNA-Spuren (Übertragung von Materie) vorhanden sein (vgl. ebd., S. 98 ff.).

2.4 Spurenkategorien

Die Kategorisierung von materiellen Spuren geht auf Wigger zurück (vgl. Wigger, 1965, S. 8 f.) und hat sich als Standard in der Fachwelt verfestigt.

Demnach sind es die folgenden vier Kategorien, in welche materielle Spuren eingeteilt werden (wenngleich begriffliche Überschneidungen existieren):

- Formspuren
- Materialspuren
- Gegenstandsspuren
- Situationsspuren

Formspuren: „Formspuren sind die durch Einwirkung eines Spurenverursachers entstandenen Formveränderungen an einem Objekt“ (Pientka und Wolf, 2017, S. 123). Es erfolgt somit eine Übertragung von Mustern (siehe Abschnitt 2.3). Formspuren lassen sich in in weitere Unterarten einteilen, so z. B. in Abdruckspuren, Eindruckspuren und Passspuren (vgl. Kawelovski, 2018, S. 23 f.).

Materialspuren: Pientka und Wolf definieren Materialspuren nach Wirth (vgl. Wirth, 2010, S. 236) folgendermaßen: „Materialspuren sind Substanzen (fest, flüssig oder gasförmig), deren stoffliche Eigenschaften und Zusammensetzungen kriminalistische Schlüsse zulassen“ (Pientka und Wolf, 2017, S. 122). Sie entstehen durch Übertragung von Materie (siehe Abschnitt 2.3), und ihre Erscheinungsformen sind äußerst vielfältig. Materialspuren können vom Täter, Opfer oder auch von Tatwerkzeugen stammen.

Gegenstandsspuren: „So werden beweiserhebliche Gegenstände bezeichnet, die als solche oft nicht der kriminaltechnischen Untersuchung bedürfen. Allein ihr Vorhandensein bei einem Tatverdächtigen oder in einem bestimmten Raum führen zur Tatrekonstruktion“ (Zirk und Vordermaier, 1998, S. 60). Dies können z. B. ein verlorener Personalausweis, das Smartphone eines Täters am Tatort oder auch die Tatwaffe im Besitz des Täters sein. Nichtsdestotrotz kann ein beweiserheblicher Gegenstand (also eine Gegenstandsspur) auch Träger anderer Spuren sein (siehe Abschnitt 2.2). Beispielsweise sind neben der Tatwaffe selbst auch die auf ihr vorhandenen Fingerabdrücke (Formspuren) für die Tatrekonstruktion relevant.

Situationsspuren: „Hierunter ist die besondere Lage von Spuren oder Gegenständen zueinander oder zu deren Umgebung zu verstehen“ (ebd., S. 60). Neben dem reinen Vorhandensein oder Fehlen von Gegenständen zählen hierzu weitere Zustände, welche sinnlich wahrnehmbar sind, so z. B., ob es am Tatort warm oder kalt ist, ein besonderer Geruch wahrnehmbar ist, Fenster

offen oder geschlossen sind oder auch elektrische Geräte, welche sich im eingeschalteten Zustand befinden (vgl. Kawelovski, 2018, S. 20).

Anfänglich wurde versucht, die in wachsender Form aufkommenden digitalen (IT-)Systeme in einer sich zunehmend weiterentwickelnden Kriminaltechnik den materiellen Spuren zuzuordnen (vgl. Zirk und Vordermaier, 1998, S. 59). Diese Einordnung war zumindest in einer Zeit rein lokal genutzter und nicht vernetzter Computersysteme folgerichtig, da aus kriminaltechnischer Perspektive eine digitale Spur immer das unmittelbare Vorhandensein einer ihr zugrunde liegenden materiellen (physischen) Spur bedingt (beispielsweise die Magnetisierung einer Festplatte oder elektromagnetische Signale auf Datenleitungen). Dies ist in einer digitalisierten und vollumfänglich vernetzten Lebens- und Arbeitswelt aber zu kurz gegriffen, denn „[h]eute muss man [...] die ‚flüchtigen' forensischen IuK-Spuren bei Cybercrime-Delikten in besonderer Weise berücksichtigen" (Plank, 2017, S. 176). Zwar erfolgt die Einordnung digitaler Spuren in der einschlägigen Literatur mitunter in eine eigene Kategorie (vgl. Pientka und Wolf, 2017, S. 124 f.), aber auch dies reicht aufgrund der vielen verschiedenen Arten digitaler Spuren und dem Umfang ihres Auftretens bei weitem nicht aus. Dies wird u. a. durch die zwar etablierte, sich aber nach wie vor äußerst dynamisch entwickelnde digitale Forensik (auch: IT-Forensik) deutlich[20]. Die sich hier aufzeigenden Tendenzen machen mehr als deutlich, dass digitale Spuren sowohl die IT-Forensik als auch die gesamte polizeiliche Ermittlungsarbeit vor große Herausforderungen stellt. Die stetig wachsende Anzahl von Smartphones, Tablets, Laptops etc. und deren immer umfangreicher werdende Speicherkapazitäten führen zu stetig wachsenden Anforderungen an die Leistungsfähigkeit der an der Auswertung beteiligten Personen und Systeme. Führt man sich zusätzlich die immer populärer werdenden Cloud-Dienste, Smart-Devices oder den Bereit des IoT vor Augen, so ist unschwer zu erkennen, dass sich digitale Spuren nicht nur in ihrer Menge, sondern auch in der Variation ihres Auftretens äußerst dynamisch entwickeln.

[20] Im Land Baden-Württemberg betrug der Anstieg der Anzahl von Aufträgen zur Untersuchung digitaler Spuren im Jahr 2016 4,3% im Vergleich zum Vorjahr (vgl. Landeskriminalamt Baden-Württemberg, 2017, S. 25). Noch deutlicher fiel der Anstieg im Bereich der Datenanalyse aus. Hier stieg im gleichen Vergleichszeitraum die Anzahl der bearbeiteten Fälle um 23% an. (vgl. ebd., S. 34)

2.5 Assoziation einer Spur

In Abschnitt 2.3 wurde dargelegt, dass materielle Spuren auf den Prinzipien der Zerteilbarkeit und der Übertragung (von Materie bzw. Mustern) beruhen. Eine Spur ist also ein Hinweis auf einen Kontakt zwischen zwei Objekten, was in der Kriminalistik auch als Ereignis bezeichnet wird. Die Feststellung eines Ereignisses, also der Weg im Rahmen einer Ermittlung, heißt Assoziation (Inman und Rudin, 2000, S. 170). Als Beispiel einer Assoziation kann die Zuordnung eines konkreten Schuhs zu einem Schuhabdruck oder auch die Zuordnung eines Fingerabdruckes zu einer konkreten Person genannt werden. In den forensischen Wissenschaften ist jede Assoziation von einer gewissen Irrtumswahrscheinlichkeit gekennzeichnet. Häufig wird diese nicht genau quantifiziert, da sich in der Praxis Richtwerte herausgebildet haben, die allgemein als Nachweis einer Assoziation akzeptiert werden, z. B. eine bestimmte Anzahl übereinstimmender Merkmale in der Daktyloskopie[21] (vgl. Dewald und F. C. Freiling, 2015, S. 25). Besonders gut untersucht sind entsprechende Wahrscheinlichkeiten des Ausschlusses oder der Übereinstimmung im Bereich der DNA-Analyse. Ausschlüsse haben hier grundsätzlich eine Aussagewahrscheinlichkeit von 100%. Die Wahrscheinlichkeit von Übereinstimmungen bzw. Einschlüssen wird von den untersuchten DNA-Orten bestimmt. Während Einschlusswahrscheinlichkeiten von 1:10000 bei einer begrenzten Anzahl von in Frage kommenden Personen kriminalistisch oftmals ausreichen, sind technisch Einschlusswahrscheinlichkeiten von 1:5 Mrd. durch erhöhten Untersuchungsaufwand erzielbar (vgl. Benecke, 2005, S. 451). Grundvoraussetzung für die Feststellung eines Ereignisses durch Assoziation ist eine Menge relevanter Spuren, die als Beweismittel in Frage kommen. Einzeln erfolgt dann zuerst die Identifikation einer Spur. Hierbei ist entscheidend, worum es sich bei der Spur handelt, und ob sie zur Klärung eines Tathergangs relevant sein könnte. Im Anschluss daran erfolgt die Klassifizierung einer Spur, beispielsweise durch genauere Analyse ihrer Form, ihrer Größe oder ihres Gewichts. Im dritten Schritt, der Individualisierung, erfolgt die Zuordnung einer Spur idealerweise zu einem oder auch einer begrenzten Menge von Objekten, welche die Spur verursacht haben könnten (vgl. Baier und S. Gärtner, 2019, S. 20 f.). Nicht immer ist die Durchführung aller Schritte bis zur Individualisierung einer Spur notwendig. So kann bei Gegenstands- oder Situationsspuren (siehe Abschnitt 2.4) mitunter die Individualisierung entfallen. Verdeutlichen

[21] siehe Fn. 9

lässt sich dies beispielhaft anhand von Betäubungsmitteln (BtM), deren Identifizierung und Klassifizierung zur Assoziation ausreicht. Eine weitere Individualisierung, also aus welcher Bezugsquelle die BtM genau stammen, ist für die Feststellung eines Ereignisses nicht zwingend notwendig (vgl. Dewald und F. C. Freiling, 2015, S. 28).

Zusammenfassend kann festgehalten werden, dass es sich bei den klassischen Spuren um wahrnehmbare physische Gegebenheiten bzw. Veränderungen handelt, welche überwiegend unmittelbar am Täter, am Tatort oder am Tatopfer zu identifizieren sind und durch Assoziation zugeordnet werden können. Solche Spuren sind sinnlich direkt wahrnehmbar bzw. können unter Verwendung von Hilfsmitteln wahrnehmbar gemacht werden (mikroskopische Spuren, DNA-Spuren etc.). Zu diesem Zweck ist eine unumkehrbare Veränderung der jeweiligen Spur nicht notwendig und im Hinblick auf ihre Beweiskraft explizit nicht erwünscht. Spuren werden mit technischen Mitteln und Verfahren zu ihrer Suche, Sicherung und Auswertung und hierbei angewandter naturwissenschaftlich-technischer Erkenntnisse und Methoden gewonnen und fließen zur Beweissicherung in die Ermittlungsarbeit ein. Überwiegend erfolgt dies durch speziell ausgebildete Kriminaltechniker während der Tatortarbeit (vgl. Ackermann, 2019b, S. 31 ff.). Es ist erkennbar, dass polizeiliche Ermittlungsarbeit und die kriminaltechnische Bearbeitung von Spuren getrennte Arbeitsbereiche sind, welche aber wiederum voneinander abhängig sind und gegenseitig auf ihren Erkenntnissen aufbauen.

3 Digitale Spuren

Mit dem wachsenden Einzug von Elektronik und erster Computertechnik in den modernen Lebens- und Arbeitsalltag begann auch das wachsende Aufkommen „neuartiger“, physisch nicht greifbarer und nicht unmittelbar wahrnehmbarer Spuren. Durch die in Kapitel 1 thematisierte Digitalisierung bzw. durch die digitale Transformation bestimmt diese Art von Spuren die polizeiliche Ermittlungsarbeit jeglicher Couleur. War es anfänglich noch die separat zu betrachtende Computeranlalyse eines sichergestellten PCs aus einer unvernetzten IT-Landschaft, sind es zunehmend neben offensichtlichen Quellen digitaler Spuren wie Laptops, Tablets oder Smartphones auch Alltagsgegenstände, Haushaltsgeräte, Heizungs- und Alarmanlagen oder Fahrzeuge, welche enorme Mengen an digitalen Spuren erzeugen und mitunter untereinander bzw. mit dem Internet vernetzt sind (vgl. Hahn, 2017, S. 4 ff.). Hierbei sind nicht nur die auf den Geräten selbst gespeicherten Daten Quellen der Informationsgewinnung, auch die flüchtigen Daten, welche immer „smarter“[22] werdende Geräte untereinander austauschen, können essentielle Quellen digitaler Spuren sein. „Die [...] klassischen Spuren haben inzwischen eine Erweiterung erfahren“ (Plank, 2017, S. 178). Mitunter werden digitale Spuren gar als „Dritter Meilenstein“ der polizeilichen Forensik angesehen – nach den Möglichkeiten der Daktyloskopie sowie der Etablierung der DNA-Technologie in den achtziger Jahren des 20. Jahrhunderts (vgl. Eisenbraun, 2020). Ungeachtet dessen bieten digitale Spuren enorme Mengen an neuen Ermittlungsmöglichkeiten, aber auch nicht außer Acht zu lassende Risiken, denn sie sind weder greif- noch wahrnehmbar, erfordern ein hohes Maß an technischem Spezialwissen und treten beständig in neuer Art und Weise in Erscheinung. Hinzu kommt, dass sich viele Aktivitäten, welche sich vormals ausschließlich in der physischen Welt abspielten, in digitale bzw. virtuelle Umgebungen verlagert haben. E-Mail- und Messenger-Kommunikation lässt die klassische Briefpost fast überflüssig erscheinen, eine schier endlos wirkende Anzahl von Webshops verdrängt nach und nach klassische Geschäfte und Warenhäuser. Auch im kriminellen Umfeld haben sich viele Tätigkeiten in den virtuellen Raum verlagert. Klassische Delikte wie Betrug oder der Verkauf von illegalen Waren sind nahtlos in den digitalen Raum übertragbar. Das bedeutet aber auch, dass digitale Spuren, welche vor wenigen Jahrzehnten noch als margi-

[22] siehe Fn. 6

nal bzw. obsolet angesehen wurden, heutzutage nahezu jeden Deliktsbereich betreffen und unter Umständen zentral entscheidende, wenn nicht gar die einzigen Hinweise liefern (vgl. Jaquet-Chiffelle, 2014, S. 189). Unterstreichen lässt sich diese Entwicklung durch eine stetig wachsende virtuelle Community Krimineller, die durch die Möglichkeiten von Automatisierung und räumlicher Entgrenzung des Internets Marktplätze krimineller Dienstleistungen etabliert hat. Dieses auch Crime-as-a-Service (CaaS) genannte Phänomen ermöglicht es jeder Person, durch Zukauf benötigter Dienstleistungen ihr kriminelles „Geschäftsmodell“ mit minimalem Aufwand und ohne erforderliche technische Vorkenntnisse umzusetzen (vgl. Manske, 2020). Im Zusammenhang von Straftaten, welche unter Nutzung ebendieser Dienstleistungen begangen wurden, werden keine klassischen physischen Spuren mehr zu finden sein. Allenfalls tritt bei einem begangenen Warenkreditbetrug[23] über einen Webshop eine Lieferung als Gegenstandsspur in Erscheinung.

Dies alles verdeutlicht, dass digitale Spuren nicht als ein einzelnes Phänomen neben den in der Kriminaltechnik fein granulierten klassischen Spuren gesehen werden dürfen. Dieses Kapitel wird zeigen, dass sie wie ihre klassischen Pendants sehr vielfältig in der Art ihres Vorkommens, ihrer Entstehung und ihrer jeweiligen Eigenschaften sind. Hieraus wird bereits erkennbar sein, dass digitale Spuren zwingend spezielle Kenntnisse und Fähigkeiten sowie zukunftsfähige Handlungskonzepte in Bezug auf ihre Identifikation, ihre Sicherung sowie die Interpretation und Weiterverarbeitung der in ihnen enthaltenen Informationen erfordern.

3.1 Definition

Eine einheitlich festgelegte, allgemein gültige und in der entsprechenden Literatur verankerte Definition von digitalen Spuren ist, ähnlich wie für die Kriminalistik (vgl. Plank, 2017, S. 149), nicht gegeben. Den Gesetzen der Informatik folgend, ist jede digitale Spur eine interpretierte Bitfolge[24] bestimmter

[23] Bei dieser auch Versand- oder Bestellbetrug genannten Betrugsart bestellt bzw. kauft ein Täter Ware, ohne dafür zu bezahlen oder fremde Zahlungsdaten zu benutzen. Dies geschieht im Zusammenhang mit Online-Verkaufsplattformen (Webshops) meistens mittels frei erfundener oder missbräuchlicher Verwendung echter Personendaten.

[24] Ein Bit ist die kleinstmögliche Einheit der Information, wird durch die Ziffern „1“ und „0“ codiert und kann somit nur 2 Zustände (wahr oder falsch) annehmen. Diese Form der Datenspeicherung wird auch als Binärform bezeichnet. Um mehr Informationen codieren zu können, werden mehrere Bits verwendet, die sog.

Länge. Da aber nicht jede codierte Information (beliebige Daten) zugleich eine Spur ist, ist hier eine Abgrenzung erforderlich. Das National Institute of Justice der Vereinigten Staaten von Amerika definiert digitale Spuren als Informationen, die in binärer Form gespeichert oder übertragen werden, und welche vor Gericht eine Rolle spielen. Sie können auf Computerfestplatten und Mobiltelefonen gefunden werden und werden häufig mit Cybercrime in Verbindung gebracht (vgl. NIJ, 2019). Diese Definition fokussiert digitale Spuren aber zu sehr auf Beweise und vernachlässigt Daten, die keinen direkten Beweiswert besitzen, aber die Ermittlungsarbeit unterstützen. Auch ist der enge Blickwinkel auf die Quellen digitaler Spuren und den Bereich Cybercrime weniger geeignet, digitale Spuren allumfassend zu definieren. Carrier formuliert es allgemeiner und sieht in digitalen Spuren digitale Daten, die eine Hypothese über digitale Ereignisse oder den Zustand digitaler Daten unterstützen bzw. widerlegen. Eine digitale Spur enthält Informationen, die vor, während oder nach einem untersuchten Ereignis aufgetreten sind. Jedes geeignete Datenelement kann verwendet werden, um eine Hypothese zu unterstützen oder zu widerlegen, und die Suche nach digitalen Spuren bezieht sich auf die Datenelemente, welche einen Bezug zu gestellten Fragen der Untersuchung eines Ereignisses haben (vgl. Carrier, 2006, S. 11 f.). Ähnlich, aber entscheidend komprimierter, formuliert es Casey. Er sieht in digitalen Spuren alle Daten, die unter Verwendung eines Computers gespeichert oder übertragen werden und welche die Theorie über das Auftreten einer Straftat unterstützen bzw. widerlegen oder kritische Elemente wie Vorsatz oder Alibi behandeln (vgl. Casey, 2011, S. 7). Dieser Definition schließen sich auch Baier und Gärtner (vgl. Baier und S. Gärtner, 2019, S. 23) sowie Dewald und Freiling (vgl. Dewald und F. C. Freiling, 2015, S. 29) an. Richtigerweise stellen Baier und Gärtner fest, dass digitale Spuren immer auf physischen Spuren wie der Magnetisierung einer Festplatte, dem Ladeszustand von Transistoren in Speichern oder elektromagnetischen Wellen auf Leitungen basieren. Gleichzeitig konstatieren sie, dass, bevor nach digitalen Spuren gesucht wird, erst physische Spuren gefunden werden müssen (vgl. Baier und S. Gärtner, 2019, S. 23). Dieser Einschätzung ist zumindest teilweise zu widersprechen, begründet sie sich doch in der Annahme, dass digitale Spuren ausschließlich auf Geräten bzw. Objekten zu finden sind, welche sich in der Verfügungsgewalt der ermittelnden Institution befinden. Völlig außer Acht gelassen werden hierbei jene digitalen Spuren, die auf Objekten an einem anderen, oftmals

Bitfolgen. Eine Bitfolge mit der Länge n kann folglich 2^n verschiedene Werte darstellen.

unbekannten Ort zu finden sind. Beispiele hierfür sind Cloud-Dienste, soziale Netzwerke oder auch Daten von Web- und Mailservern. Dewald hingegen kritisiert, dass Caseys Definition digitaler Spuren deren „digitale Natur“ nicht näher festlegt und stützt sich hierfür ausschließlich auf die physische Speicherung von digitalen Daten in elektronischer Form (vgl. Dewald und F. C. Freiling, 2015, S. 29 f.). Diese Bedenken lassen sich allerdings relativieren, denn auch Daten auf Lochkarten[25] sind – trotz ihrer mittlerweile praktischen Bedeutungslosigkeit – binär codiert. Auch Meier stützt sich auf die Definition Caseys, merkt aber an, dass eine Betrachtung digitaler Spuren auf unterschiedlichen Abstraktionsniveaus[26] geschehen muss (vgl. Meier, 2016, S. 23). Wird Caseys Definition digitaler Spuren um die genannten Details und unter Beachtung der aufgeführten Kritiken erweitert, so kann festgehalten werden:

Digitale Spuren sind binär codierte Daten (Bitfolgen), welche mess- oder erfassbar sind und welche nach strukturierter Interpretation unter Nutzung der notwendigen, aufeinander aufbauenden Abstraktionsschichten wichtige Erkenntnisse und Hinweise zu einem Ereignis liefern. Digitale Spuren basieren immer auf physischen Spuren, wobei ein Gewahrsam der physischen Spur oder der direkte Zugriff auf diese zur Interpretation der digitalen Spur nicht zwingend erforderlich ist, sofern benötigte Abstraktionsschritte bereits erfolgt sind.

Insbesondere der zweite Satz dieser etwas abstrakt anmutenden Definition wird sich nach der Betrachtung der verschiedenen Kategorien digitaler Spuren in Abschnitt 3.4 recht anschaulich erschließen.

3.2 Besonderheiten digitaler Spuren

Wie im vorherigen Abschnitt festgestellt wurde, sind physische Spuren immer Grundlage digitaler Spuren. Somit gilt Locards Austauschprinzip grundsätzlich

[25] Eine Lochkarte ist ein „Datenträger“ aus Pappe. Sie ist in 12 Zeilen (Kanäle) und 80 Spalten eingeteilt. Jede Spalte einer Lochkarte kann ein Zeichen aufnehmen, welches durch ein oder mehrere Löcher codiert ist (vgl. Claus und Schwill, 1991, S. 285). Erwähnenswert ist, dass die Lochkarte somit ein Speichermedium ist, dessen digitalen Daten sich nicht nur maschinell lesen lassen, sondern auch visuell wahrnehmbar sind. Unerfreuliche Berühmtheit erlangte die Lochkarte letztmalig im Zusammenhang mit den US-amerikanischen Präsidentschaftswahlen im Jahr 2000, als wegen antiquierter Wahlmaschinen und unsauber gestanzter Lochkarten ein wochenlanges Nachzählverfahren in Gang gesetzt wurde (vgl. National Museum of American History, 2004).

[26] siehe Abschnitt 3.2.2

auch für digitale Spuren, da die Entstehung von Dateninformation auf einem Speicher oder einer Datenleitung auch immer eines physikalischen Vorgangs bedarf. Aber es gibt entscheidende Besonderheiten von digitalen Spuren und im Umgang mit Ihnen. Da ist zum einen die bereits angesprochene notwendige Abstraktion von Daten zur Interpretation ihres Inhalts. Ohne diese Abstraktionen verflüssigt sich eine digitale Spur zu einer bedeutungslosen Ansammlung von Nullen und Einsen unbestimmter Länge. Zum anderen werden Ermittlungspersonen gerade im Bereich der Cyberkriminalität zunehmend mit einem räumlich entgrenzten, globalisierten Tatort konfrontiert, an welchem es keinerlei physische, wohl aber auf ihnen basierende digitale Spuren zu identifizieren gibt. Als weitere Tatsache kommt hinzu, dass der Polizei durch die zunehmende Digitalisierung der Gesellschaft aktuell und insbesondere in der Zukunft eine Flut von Daten gegenüber steht, welche im Zuge der Ermittlungen gezielt gefiltert und sinnvoll reduziert werden müssen (vgl. Pawlaszczyk, 2017, S. 164 f.). Der folgende Abschnitt wirft einen ersten Blick auf die entscheidenden Besonderheiten digitaler Spuren im Hinblick auf ihre Entstehung und ihre Übertragung bzw. der Übertragung der ihn ihnen enthaltenen Spureninformation.

3.2.1 Entstehung digitaler Spuren

Im Zusammenhang mit der Entstehung klassischer Spuren wurde in Abschnitt 2.3 festgestellt, dass niemand eine Straftat begehen kann, ohne eine Spur zu hinterlassen. Spuren entstehen im klassischen Sinn durch Übertragung von Materie und Mustern am Tatort. Da digitale Spuren in ihrer Mehrheit aber in IT-Systemen gespeichert bzw. von diesen übertragen werden, ist der eigentliche Tatort, also der Ort wo eine Tat ausgeführt wurde, oftmals unbekannt. Auch endet ein solcher Tatort nicht an nationalen Grenzen oder nimmt auf diese Rücksicht. Und trotzdem hinterlässt auch eine Straftat an einem virtuellen und unbekannten Tatort zwangsläufig Spuren, denn in jedem hinreichend komplexen IT-System entstehen bei seiner Nutzung zwangsläufig digitale Spuren (vgl. ebd., S. 115). So hinterlässt die Nutzung eines Computers unvermeidbar Spuren im Dateisystem, der Registrierung, den Systemprotokollen oder Protokollen auf Netzwerkebene. Anschaulich wird dies am Beispiel einer E-Mail, welche über einen Webmail-Dienst[27] versendet wird. Der zum Senden der

[27] Ein Webmail-Dienst bietet die Möglichkeit, ein E-Mail-Postfach nicht durch die Verwendung eines hierfür speziellen Programmes, sondern über einen beliebigen

E-Mail verwendete Webbrowser speichert verschiedene Daten, u. a. aufgerufene Webseiten, Suchbegriffe, Zeitstempel und u. U. auch Zugangsdaten (vgl. Mabey u. a., 2018, S. 13 ff.). Dies wären digitale Spuren, die lokal auf einem IT-System identifiziert werden können, welches zum Versenden der E-Mail verwendet wurde. Des Weiteren erzeugt die Übertragung der E-Mail zum Empfänger weitere Spuren auf den beteiligten Systemen der E-Mail-Provider wie Zugriffsprotokolle oder IP-Adressen, die dem versendenden System und eventuell einer Person zugeordnet werden können. Und auch auf dem IT-System, auf welchem die E-Mail letztendlich empfangen wird, können noch immer Spuren identifiziert werden, denn Header-Daten von E-Mails enthalten viel mehr Informationen als nur die Absenderadresse und den Betreff (vgl. Banday, 2011, S. 55 ff.). Aus Sicht der klassischen Forensik hat sich innerhalb dieses Beispieles durch ein einziges Ereignis eine Spur mehrfach übertragen bzw. es wurden mehrere unterschiedliche, aber unmittelbar voneinander abhängende Spuren erzeugt. Somit entpuppt sich schon an dieser Stelle neben dem virtuellen Tatort ein zweites Alleinstellungsmerkmal digitaler Spuren: ihre uneingeschränkte Kopierbarkeit (siehe Abschnitt 3.3.2). Weiterhin zeigt dieses Beispiel, das jede erzeugte digitale Spur für sich nur eine anteilige Information über das Gesamtereignis enthält. Auf dem versendenden IT-System lassen sich der Verfasser, der Zeitpunkt der Erstellung und evtl. noch der Inhalt der E-Mail feststellen. Die Spuren bei den beteiligten Providern beinhalten Informationen zu Sender- und Empfängeradresse sowie Protokolldaten der Zugriffe und auf dem empfangenden IT-System sind der Inhalt der E-Mail sowie weitere Header-Daten identifizierbar. Für eine vollständige Rekonstruktion des Gesamtereignisses (Versenden einer E-Mail) werden folglich alle hierbei erzeugten digitalen Spuren benötigt. Und noch ein weiteres Risiko digitaler Spuren zeigt dieses Beispiel auf: ihre Manipulierbarkeit. Digitale Daten können ohne weiteres entweder vorsätzlich oder fahrlässig verändert werden. Abschnitt 3.3 dieser Arbeit wird notwendige Maßnahmen erörtern, um die Integrität digitaler Spuren zu gewährleisten und nachzuweisen.

Bezieht man das Beispiel des Versendens einer E-Mail auf Locards Austauschprinzip, so stellt man fest, dass das Konzept des Austausches von Materie in Bezug auf digitale Spuren keine Anwendung findet. Jedoch bildet der Transfer von Mustern eine Analogie in der digitalen Welt, denn eine Übertragung von Mustern bedeutet immer auch eine Übertragung von Informationen von einem

Webbrowser zu verwalten. Bekannte Webmail-Dienste sind u. a. „gmx.de“ oder „web.de“

Objekt zu einem anderen. Folglich findet auf einem IT-System ebenfalls eine Übertragung von Mustern statt, denn die Muster der Eingangsdaten bilden sich in den Mustern der Ausgangsdaten ab, wenn auch in reduzierter bzw. abgewandelter Form. Und so konstatiert Dewald, dass für digitale Spuren ebenfalls das Transferprinzip der klassischen Forensik gilt (vgl. Dewald und F. C. Freiling, 2015, S. 33 ff.). Diese Ansicht vertritt auch Casey. So erweitert er jedoch das Austauschprinzip von Locard, welches ursprünglich den Austausch zwischen Täter, Opfer und realem Tatort vorsah, um den bereits benannten virtuellen Tatort (vgl. Casey, 2011, S. 16 f.). Diese Erweiterung nimmt zum einen den Austausch von Spuren von und zu einem virtuellen Tatort zusätzlich zu einem klassischen reellen Tatort auf. Zum anderen findet die Tatsache Anwendung, dass eine digitale Spur immer auf einer physischen Spur basiert und der Austausch digitaler Spuren an einem virtuellen Tatort mit dem Austausch physischer Spuren an einem unbekannten reellen Tatort einhergeht.

3.2.2 Abstraktionsschichten

Eine weitere entscheidende Besonderheit digitaler Spuren ist ihre bereits erwähnte zwingend notwendige Abstraktion, um eine Interpretation der ihnen innewohnenden Informationen zu ermöglichen. Grund hierfür ist, dass eine digitale Spur erst einmal nichts weiter als eine Aneinanderreihung von Nullen und Einsen ist. Diese ursprüngliche Form ist für den Menschen nicht zugänglich, so dass – wie übrigens auch bei einigen physischen Spuren (z. B. DNA) – die Spur durch eine oder mehrere Aufbereitungen in ein unmittelbar les- und interpretierbares Format übersetzt bzw. aufbereitet werden muss. Zur Veranschaulichung der einzelnen Abstraktionsschritte wird erneut das Beispiel der E-Mail zur Hand genommen. Da die Erfassung des gesamten Ereignisses, also das Versenden einer E-Mail, den Rahmen sprengen würde, wird nur die empfangene, auf einem IT-System gespeicherte E-Mail zur Illustration der hierarchisch aufgebauten Abstraktion betrachtet:

1. Die oberste Abstraktionsschicht, die gleichzeitig auch die für den Menschen unmittelbar wahrnehmbare Information bereitstellt, ist die Programmebene, in diesem Fall ein E-Mail-Programm, welche den Inhalt der E-Mail in für den Menschen lesbarer Form darstellt.
2. Die Dateiebene stellt die für das E-Mail-Programm notwendigen Dateien bereit, welche von diesem eingelesen werden.

3. Die Ebene der Medienverwaltung (zur Vereinfachung des Verständnisses werden mehrere Ebenen wie Dateisystem- oder Partitionsebene als eine Einheit betrachtet) organisiert die auf einem Speicher vorhandenen Daten üblicherweise in einem oder mehreren Bereichen in einer baumartigen Verzeichnisstruktur und stellt Metainformationen über Dateien, wie beispielsweise unterschiedliche Zeitstempel, Dateiname oder Größe bereit.
4. Das physische Medium als unterste Ebene interpretiert, ebenfalls sehr vereinfach betrachtet, die auf dem Speicher vorhandenen Bitfolgen durch eine Zeichenkodierung und stellt diese Zeichen der Medienverwaltung zur Verfügung.

Die Daten, und somit auch eine digitale Spur, befinden sich also in mehreren vertikal eingebetteten Schichten oder Ebenen, welche alle die Information einer Spur in unterschiedlicher Form bzw. Kodierung enthalten (vgl. Dewald und F. C. Freiling, 2015, S. 244 f.). Dies gilt übrigens nicht nur für persistent gespeicherte Daten. Auch flüchtige Daten sind in verschiedene Abstraktionsschichten eingebettet, wie u. a. ein Blick auf das ISO/OSI-Schichtenmodell der Datenkommunikation[28] zeigt.

Bei aller Souveränität im Zusammenspiel der einzelnen Abstraktionsschichten können Interpretationsfehler die Informationsgewinnung aus einer digitalen Spur erschweren oder gar verhindern. Gründe hierfür können technische Defekte oder fehlerhaft kodierte Daten sein, die eine erneute Dekodierung unmöglich machen oder auch Fehler im Interpretationsalgorithmus einer einzelnen Abstraktionsschicht. Dies stellt einen nicht unerheblichen Risikofaktor bei der Verarbeitung digitaler Spuren dar. Ein zugegebenermaßen äußerst einfaches Beispiel diesbezüglich ist das Ändern des Suffixes einer Videodatei auf den Wert „txt“. Ohne weiteres Zutun wird diese Videodatei unter Umständen nicht mehr als solche interpretiert. In der IT-forensischen Praxis wird dieser „Fehler“ eine korrekte Interpretation der Videodatei eher nicht verhindern, mit jeder weiteren Abstraktionsschicht aber wächst das Risiko eines kompletten Informationsverlustes.

[28] Das ISO/OSI – Referenzmodell der Datenkommunikation teilt das Problem der digitalen Kommunikation zwischen IT-Systemen in sieben Teilaufgaben auf, welche als „Schichten“ hierarchisch angeordnet sind. Hierdurch ist eine herstellerunabhängige Kommunikation in heterogenen Umgebungen möglich (vgl. Küveler und Schwoch, 2007, S. 192 ff.).

Für die polizeiliche Ermittlungsarbeit ist an dieser Stelle bereits von Relevanz, dass die Sicherung einer digitalen Spur über jede Ebene der Abstraktion erfolgen kann. Es ist prinzipiell machbar (wenn auch nicht erstrebenswert), eine E-Mail durch einen Screenshot des E-Mail-Programms zu sichern. Es ist aber durchaus auch möglich, eine Kopie des physischen Mediums zu erstellen und hieraus die E-Mail forensisch zu extrahieren. Die Sicherung auf den einzelnen Ebenen hat für sich jeweils Vor- und Nachteile. Während ein Screenshot das Maximum an Selektion der zu sichernden Daten bei gleichzeitig minimal zu sichernder Datenmenge bedeutet, so verhält es sich bei der Sicherung des gesamten physischen Mediums genau umgekehrt. Die Möglichkeiten zum Nachweis der Integrität[29]einer gesicherten Spur ist über das physische Medium am höchsten, während der Nachweis auf Programmebene technisch weniger möglich ist und die korrekte Arbeitsweise der sichernden Person wiederum weit ausschlaggebender ist. Dieser unmittelbare Zusammenhang zwischen Sicherungsebene, möglicher Selektion der Menge zu sichernder Daten und Nachweis der Integrität der Daten und somit der digitalen Spuren ist für die polizeiliche Ermittlungsarbeit besonders ausschlaggebend. Dieses Kapitel wird noch aufzeigen, dass es nicht immer möglich ist, jede Art von digitaler Spur so zu sichern, dass allein die Methode der Sicherung einen technischen Nachweis ihrer Integrität ermöglicht. Umso mehr kommt es auf die Kompetenz, das technische Verständnis und eine nachvollziehbare Dokumentation aller durchgeführten Schritte der jeweiligen Ermittlungsperson an, eine digitale Spur und somit einen digitalen Beweis zu identifizieren und verwertbar zu sichern.

3.2.3 Information und Träger digitaler Spuren

Wie festgestellt werden konnte, handelt es sich bei digitalen Spuren im Sinne des Austauschprinzip von Locard im erweiterten Sinn um eine Übertragung von Mustern[30]. Bei den klassischen physischen Spuren wurde zwischen Spureninformation und Spurenträger unterschieden. Hierbei enthält genau ein Spurenträger die Information einer Spur (z. B. Kratzer oder Abdruckspuren eines Spurenverursachers auf einer Oberfläche), und somit erhalten Spurenträger und Spureninformation eine direkte enge Bindung zueinander.

[29] siehe Abschnitt 3.3.4
[30] siehe Abschnitt 3.2.1

In Bezug auf digitale Spuren entsteht die Information durch hierarchisch aufeinander aufbauende Abstraktionsebenen und die Interpretation der durch den Menschen wahrnehmbaren Information aus der obersten Ebene der Abstraktion (die Darstellung des Inhaltes einer E-Mail im Programm). Das heißt im Umkehrschluss, dass die Information einer digitalen Spur erst durch Wahrnehmung und Interpretation, also im Kopf eines Menschen entstehen. Innerhalb dieser abstrakten Modellierung wird die Information von Daten repräsentiert, folglich sind die Daten Träger der Information und somit Spurenträger. Die Information der Daten basiert immer auf Interpretationsvereinbarungen zwischen den einzelnen Abstraktionsebenen, so dass die Kodierung der unteren Ebene genutzt wird, um die Kodierung der nächsthöheren Ebene zu realisieren (vgl. F. Freiling und K. Sack, 2017, S. 324 f.). Das bedeutet aber auch, dass jede Abstraktionsebene gleichzeitig Spurenträger sein, sowie Spureninformationen enthalten kann. Weiterhin wird klar, dass eine digitale Spureninformation unabhängig von einem alleinigen Spurenträger existieren kann, wie es bei physischen Spuren schwer einzusehen wäre, da hier die physische Materie explizit die Spureninformation enthält (vgl. ebd., S. 330). Die Bindung zwischen Träger und Information ist folglich sehr zerbrechlich, denn die wahrnehmbare Information einer Spur kann aus jeder Abstraktionsebene gewonnen werden, sofern deren Kodierungsschema interpretiert werden kann. Auch können Daten auf jeder Ebene ihrer Abstraktion auf einen beliebigen (physischen) Datenträger kopiert werden, ohne dass sich die in ihnen enthaltene Information verändert[31]. Trotz dieser zerbrechlichen Bindung zwischen Information und Träger digitaler Spuren betrachtet sogar aktuelle Literatur häufig noch das physische Trägermedium und die unkörperlichen Daten als eine zusammenhängende Spureneinheit (vgl. Baier und S. Gärtner, 2019, S. 23). Dies mag gewissermaßen daran liegen, dass der Blickwinkel auf die klassische IT-Forensik von Geräten wie Laptops oder Smartphones verengt ist, wird aber dem Phänomen digitaler Spuren in ihrem gesamten Spektrum absolut nicht mehr gerecht[32].

Als ein weiterer Zwischenbefund lässt sich somit festhalten: Träger digitaler Spuren sind die sie repräsentierenden Daten, durch deren Interpretation mittels eines bekannten Kodierungsschemas die in ihnen enthaltene wahrnehmbare Spureninformation gewonnen wird. Ein originäres physisches Trägermedium ist für die Sicherung einer Spureninformation nicht notwendig,

[31] siehe Abschnitt 3.3.2

[32] Im Abschnitt *Remote- bzw. Onlinespuren* wird diese These grundlegend untermauert.

was besonders im Zusammenhang mit flüchtigen bzw. Online-Spuren sowie bei selektiver Sicherung aufgrund stetig wachsender Datenmengen deutlich wird.

3.3 Eigenschaften digitaler Spuren

Der vorherige Abschnitt hat wichtige Besonderheiten digitaler Spuren dargestellt. Sie basieren zunächst auf physischen Spuren und werden über hierarchisch aufgebaute Ebenen der Abstraktion extrahiert und interpretiert. Auf jeder Abstraktionsebene können Interpretationsfehler auftreten, die eine weitere Gewinnung der Information aus einer digitalen Spur erschweren oder verhindern. Dieser Abschnitt setzt den Fokus auf die verschiedenen Eigenschaften digitaler Spuren, welche in einer nennenswerten Anzahl Parallelen zu Eigenschaften klassischer physischer Spuren besitzen. Gleichzeitig lassen sich digitale Spuren anhand ihrer prägnantesten Eigenschaften in Kategorien einteilen.

3.3.1 Flüchtigkeit

Digitale Spuren und die sie repräsentierenden Daten sind immer einem gewissen Grad der Flüchtigkeit unterworfen. Der Grund hierfür ist die bereits festgestellte Tatsache, dass digitale Spuren auf physischen Spuren basieren und damit deren physikalischen und chemischen Eigenschaften und Prozessen unterliegen (vgl. Meier, 2016, S. 24). Diese Flüchtigkeit bestimmt zum einen, wie lange Daten für eine Sicherung zur Verfügung stehen. Zum anderen gibt es je nach Flüchtigkeitsgrad verschiedene Vorgehensweisen zur effektiven Akquise[33], und des Weiteren muss die ungewollte Manipulation der Daten während einer Sicherung vermieden werden (vgl. Baier und S. Gärtner, 2019, S. 26). Generell werden drei Arten der Flüchtigkeit digitaler Spuren unterschieden: persistente, semi-persistente und transiente (flüchtige) digitale Spuren[34]. Dass auch als persistent geltende digitale Spuren von einer Flüchtigkeit betroffen sind, hat zwei entscheidende Gründe. Erstens unterliegt jeder digitale Datenspeicher im Laufe der Zeit einer gewissen physischen

[33] Grundsätzlich werden zwei Formen der Untersuchung in Bezug auf eine IT-System unterschieden: die Live-Response- (vgl. Pawlaszczyk, 2017, S. 119 ff.) und die Post-mortem-Akquise (vgl. ebd., S. 125 ff.).

[34] siehe Abschnitt 3.4

Verschlechterung. Datenstrukturen auf Festplatten verändern sich langfristig durch äußere Umwelteinflüsse wie Magnetfelder, Strukturen auf CD/DVDs werden durch UV-Strahlung mittelfristig zerstört. Die Verschlechterung digitaler Speichermedien erfolgt außerdem schneller als bei analogen Medien wie beispielsweise Papier. Zudem kann eine relativ geringe Verschlechterung bereits zu komplettem Verlust der Information führen, wenn hierdurch eine Abstraktion der Daten nicht mehr möglich ist. Zweitens sorgt die Obsoleszenz des technologischem Fortschritts dafür, dass Hard- und Software sowie verwendete Dateiformate sehr schnell als veraltet gelten und keinen langen Lebenszyklus aufweisen. So ist auch hier ein hohes Verlustrisiko vorhanden, da selbst fehlerfrei gespeicherte digitale Inhalte Gefahr laufen, nicht mehr zugänglich zu sein. Verhindert werden kann der drohende Verlust, indem Daten rechtzeitig auf ein aktuelles Medium kopiert werden. Dies begegnet gleichzeitig der Verschlechterung von Speichermedien sowie deren Obsoleszenz ihrer Hardware.

Die polizeiliche Ermittlungsarbeit ist durch die Flüchtigkeit als persistent geltender digitaler Daten nur indirekt betroffen. Laufende Ermittlungsverfahren überdauern i. d. R. nicht die Haltbarkeit gängiger Speichermedien. Für den langfristigen Erhalt digitaler Spuren bzw. digital gespeicherter Informationen u. a. aus ungeklärten Ermittlungsverfahren sind Strategien der Langzeitarchivierung wiederum unumgänglich (vgl. Schmitz u. a., 2005).

3.3.2 Kopierbarkeit

Eine weitere entscheidende Eigenschaft digitaler Spuren ist ihre verlustfreie Kopierbarkeit. IT-Systeme speichern Daten im binären Zahlensystem und somit in einem eindeutig unterscheidbaren Zustand („0“ oder „1“). In der Informatik wird dieser Zustand als diskret bezeichnet und bedeutet, dass es zwischen den binären Werten „0“ und „1“ keine weiteren Zwischenwerte gibt. Dies steht im Gegensatz zur realen analogen Welt, in welcher Materie nahezu beliebig zerteilbar ist. Digitale Spuren bzw. die ihnen zugrunde liegenden Daten hingegen sind immer bis ins letzte Bit exakt definiert (vgl. Dewald und F. C. Freiling, 2015, S. 40 f.). Ein weiterer wichtiger Parameter digitaler Spuren bzgl. ihrer Kopierbarkeit ist die bereits festgestellte Trennung von Spurenträger und Spureninformation, was dazu führt, dass der Begriff „Kopie“ enger gefasst werden muss. Im Grunde genommen wird bei einem Kopiervorgang nämlich

keine exakte Duplizierung der digitalen Spur an sich vorgenommen, sondern nur die Duplizierung ihrer kodierten Information. Aus Sicht des Spurenträgers werden bestimmte Merkmale, nämlich die kodierten Informationen, perfekt auf einen anderen Spurenträger übertragen. Diese Teilmenge der Spur ist jedoch durch die binäre Kodierung exakt umrissen und ihre Kopie ist ohne Verlust auslesbar (vgl. F. Freiling und K. Sack, 2017, S. 335). Dies ist eine herausragende Eigenschaft und großer Vorteil digitaler Spuren und findet auch im Deliktsbereich der Cyberkriminalität Anwendung (vgl. Brodowski und F. Freiling, 2015). Nicht vernachlässigt werden darf in diesem Zusammenhang aber auch, dass durch jeden Kopiervorgang die Integrität der digitalen Spur in Frage steht und durch geeignete Methoden nachgewiesen werden muss.

3.3.3 Manipulierbarkeit

Digitale Spuren sind, ebenso wie physische Spuren, manipulierbar. Dies kann absichtlich oder auch versehentlich passieren. Aus diesem Grund ist in der polizeilichen Ermittlungsarbeit nicht nur die Suche nach Spuren relevant, welche durch den Täter manipuliert wurden, sondern es ist ebenso unverzichtbar, eine ungewollte Manipulation oder gar Zerstörung von Spuren im Zuge ihrer Sicherung zu vermeiden. Eine Manipulation, also das Einfügen, Löschen oder Ersetzen von Daten, hinterlässt aber auch in der digitalen Welt überwiegend nicht vermeidbare und nachweisbare Spuren (vgl. Meier, 2016, S. 25). So wurde bereits im Abschnitt zur Entstehung digitaler Spuren festgestellt, dass jede Nutzung eines IT-Systems unweigerlich Spuren im Dateisystem, der Registrierung oder den Systemprotokollen hinterlässt. Nichtsdestotrotz sind Manipulationen digitaler Art in bestimmten Fällen kaum nachvollziehbar. Wird auf einem passiv eingebundenen Datenträger[35] ein einzelnes Bit geändert, so handelt es sich zweifelsohne um eine Manipulation der Spur, welche aber kaum nachzuweisen ist, sofern nach einer solchen Manipulation die Daten noch über die einzelnen Abstraktionsschichten dekodiert werden können (vgl. Dewald und F. C. Freiling, 2015, S. 39 f.). Viel wichtiger als die Suche nach bewusst manipulierten Daten ist im Zuge polizeilicher Ermittlungsarbeit die Tatsache, dass digitale Spuren durch ungewollte Manipulation bei ihrer Sicherung regelmäßig entwertet werden, da ihre Integrität nicht mehr belegbar ist.

[35] Gemeint ist in diesem Fall z. B. ein IT-System, welches durch ein Live-System gebootet und dessen Datenträger manuell nach dem Booten eingebunden wird. Hierbei erfolgen i. d. R. keine automatischen Schreiboperationen.

Sie müssen somit während ihrer Akquise und weiteren Verarbeitung entsprechend abgesichert werden (vgl. Meier, 2016, S. 25). Voraussetzung hierfür ist neben der korrekten Vorgehensweise sachkundiges und ausreichend geschultes Personal sowie eine lückenlose Dokumentation aller durchgeführten Ermittlungsschritte.

3.3.4 Integrität und Authentizität digitaler Spuren

Aus den bisher dargestellten Eigenschaften digitaler Spuren, insbesondere aus ihrer Kopier- und Manipulierbarkeit, ergeben sich essenzielle Anforderungen an ihre Integrität und Authentizität und einen lückenlosen Nachweis ebendieser. Aus sich heraus zeigt die Integrität einer digitalen Spur an, dass sie seit dem Zeitpunkt ihrer Sicherung keiner Veränderung oder gar Manipulation unterlag. Dies deckt sich mit der Definition aus dem Bereich der IT-Sicherheit, wonach der vorliegende Status von Daten derselbe sein muss wie in den Quelldokumenten und nicht versehentlich oder böswillig verändert oder gar zerstört wurde (vgl. Gollmann, 2011, S. 36). Die Authentizität einer digitalen Spur hingegen ergibt sich aus dem Nachweis, dass gesicherte Daten (also die Spur) tatsächlich aus der zur Spur angegebenen Quelle stammen (vgl. Casey, 2011, S. 21). Als bewährte Methode, digitale Spuren zum Nachweis der Integrität und Authentizität inhaltlich überprüfbar zu machen, haben sich Hashwertfunktionen in Kombination mit digitalen Signaturen erwiesen.

Ein Hashwert ist gewissermaßen ein digitaler Fingerabdruck. Erzeugt wird aus einer Datenquelle beliebiger Länge per mathematischer Funktion ein Ausgabewert fester Länge, der sog. Hashwert. So gilt im allgemeinen, dass es einerseits nicht möglich ist, hieraus Rückschlüsse auf die ursprüngliche Datenquelle zu schließen, und andererseits soll eine möglichst hohe Kollisionsresistenz sicherstellen, dass niemals durch zwei unterschiedliche Datenquellen derselbe Hashwert erzeugt wird, denn nur so ist garantiert, dass jede beliebige Änderung an der Datenquelle zu einem geänderten Hashwert führt. Da durch verbesserte Rechenleistungen und Schwächen in den Algorithmen gewisser Hashwertfunktionen in der Vergangenheit bereits Kollisionen gezielt provoziert werden konnten[36], ist es für die polizeiliche Ermittlungsarbeit unerlässlich, nur

[36] Der in IT-Forensik-Kreisen weit verbreitete Hashwertalgorithmus „MD5“ gilt bereits seit 2004 als unsicher. Seit dem Jahr 2013 ist eine Methode bekannt, die es erlaubt, mittels handelsüblicher IT-Systeme MD5-Kollisionen in unter einer Sekunde zu erzeugen (vgl. Pawlaszczyk, 2017, S. 126).

als kollisionsresistent[37] geltende Algorithmen zu verwenden bzw. mehrere unterschiedliche Hashwertfunktionen auf eine Datenquelle anzuwenden (vgl. Pawlaszczyk, 2017, S. 126 f.). Eine bestätigte Integrität digitaler Spuren weist jedoch in keiner Weise ihre Authentizität nach. Diese wird auch in aktueller Literatur noch immer direkt mit dem physischen Träger einer digitalen Spur in Verbindung gebracht (vgl. F. Freiling und K. Sack, 2017, S. 335 f.). Die Authentizität lässt sich nämlich jederzeit durch den Hashwert des physischen Datenträgers überprüfen und nachweisen, von welchem sie gesichert wurde. Es handelt sich folglich um einen rein technischen Vorgang der Authentifizierung. Dieser Auffassung ist grundsätzlich nicht zu widersprechen, jedoch ließen sich damit flüchtige oder nicht lokale digitale Spuren nicht validieren, da kein physischer Datenträger als Quelle einer Spur zur Verfügung steht. Zudem wurde bereits festgestellt, dass digitale Spuren keine untrennbare Verbindung zu einem physischen Spurenträger aufweisen. In diesen Fällen kann die Authentizität einer digitalen Spur einzig und allein durch die Person belegt werden, welche deren Sicherung vorgenommen hat. In der Praxis hat sich hierfür die digitale Signatur über eine Public Key Infrastructure (PKI) bewährt. Im ersten Schritt wird für die zu verifizierenden Daten ein Hashwert erstellt, welcher auch zum Nachweis der Integrität Verwendung findet. Dieser Hashwert, und nicht die Daten selbst, werden für die Signatur verwendet. Zum einen ist die Signatur eines Hashwertes weitaus performanter als dies für die gesamten Daten der Fall wäre, zum anderen ist so die Überprüfung der Signatur verschlüsselter Daten möglich, ohne sie vorher entschlüsseln zu müssen. In einem zweiten Schritt wird dann die eigentliche Signatur des Hashwertes vorgenommen. Wie die Bezeichnung PKI bereits erkennen lässt, handelt es sich um ein asymmetrisches [38] Verfahren, welches aus einem Signier- und einem Verifizieralgorithmus besteht. Mittels eines privaten (geheimen) Schlüssels wird die Signatur des Hashwertes vorgenommen, welche dann mit dem dazugehörigen öffentlichen Schlüssel überprüft werden kann. Ohne tiefgreifend auf Details der Kryptografie einzugehen, handelt es sich bei dieser Vorgehensweise um die Umkehrung des Public-Key-Verfahrens [39], wie

[37] dem jeweiligen Stand der Technik entsprechend

[38] Asymmetrische Verschlüsselungsverfahrenverwenden verwenden zum Ver- und Entschlüsseln verschiedene Schlüssel. Dabei wird zwischen öffentlichen und privaten Schlüsseln, welche geheim gehalten werden, unterschieden. Ein Austausch der Schlüssel unter den Teilnehmern ist im Gegensatz zu symmetrischen Verschlüsselungsverfahren, bei welchen für die Ver- und Entschlüsselung der gleiche Schlüssel Verwendung findet, nicht erforderlich (vgl. Witt, 2014, S. 165 f.).

[39] Zum Versenden einer verschlüsselten Nachricht wird durch den Absender der öffentliche Schlüssel des Empfängers verwendet, welcher die Nachricht dann mit dem nur ihm bekannten dazugehörigen privaten Schlüssel wieder entschlüsseln

es beispielsweise zur verschlüsselten Nachrichtenkommunikation verwendet wird. Weil nur die Person, in deren Besitz sich der private Schlüssel befindet, diesen auch kennt, ist mit diesem Verfahren annähernd sichergestellt, dass die Signatur von dieser Person stammt. Im Fall polizeilicher Ermittlungsarbeit ist das die Person, die eine digitale Spur sicherstellt. Die Überprüfung dieser Signatur ist dann wiederum jeder weiteren Person durch Anwendung des dazugehörigen öffentlichen Schlüssels möglich, da dieser nicht geheim ist und allen zur Verfügung steht (vgl. Karpfinger und Kiechle, 2010). Um die Vertrauenswürdigkeit einer elektronischen Signatur zu gewährleisten, werden Schlüsselpaare zusätzlich durch Zertifizierungsstellen, den sog. Certification Authorities (CA), in Form von Zertifikaten bestätigt, die der jeweiligen Signatur beigefügt wird. Eine technisch ausführliche Betrachtung digitaler Signaturen ist im Rahmen dieser Arbeit leider nicht möglich. Das National Institute of Standards and Technology (NIST) hat beispielsweise mit dem Digital Signature Standard (DSS) den Digital Signature Algorithm (DSA) spezifiziert (NIST, 2013) und auch der Algorithmenkatalog der Bundesnetzagentur (Bundesnetzagentur, 2016) vertieft die Thematik entsprechend.

Allerdings wird auch ohne eine technisch tiefgreifende Auseinandersetzung mit der Thematik klar, dass die Wahrung der Authentizität und Integrität digitaler Spuren in der polizeilichen Ermittlungsarbeit eine zunehmend wichtigere Rolle spielen wird. Wenngleich bei der Sicherstellung physischer Datenträger ein Nachweis der Authentizität und Integrität durch diese selbst auch zu einem späteren Zeitpunkt immer wieder möglich ist[40], so entfällt diese Möglichkeit, wenn kein ursprüngliches physisches Trägermedium einer digitalen Spur zur Verfügung steht. In diesem Fall liegt die Verantwortung zum Nachweis speziell der Authentizität bei der ermittelnden Person selbst, welche hierfür idealerweise digitale Signaturverfahren verwendet. Unterbleibt das Signieren einer digitalen Spur, kann dies im Extremfall ihre Entwertung im weiteren Ermittlungsverfahren bedeuten.

kann. Eine der prominentesten Implementationen ist der von Phil Zimmermann entwickelte und zur E-Mail-Verschlüsselung verwendete Standard Pretty Good Privacy (PGP).

40 Die Erstellung von Prüfsummen eines Datenträgers ist jederzeit wiederholbar.

3.4 Kategorien digitaler Spuren

Bereits im Abschnitt zur Flüchtigkeit digitaler Spuren wurde konstatiert, dass digitale Spuren anhand ihres Flüchtigkeitsgrades in unterschiedliche Kategorien eingeteilt werden. In der aktuellen einschlägigen Fachliteratur werden hierzu die folgenden drei Hauptkategorien genannt: persistente, semipersistente und flüchtige bzw. transiente digitale Spuren (vgl. Dewald und F. C. Freiling, 2015; Baier und S. Gärtner, 2019; Meier, 2016; Pawlaszczyk, 2017). Dieser Kategorisierung ist grundsätzlich zuzustimmen, finden sich doch in einem IT-System alle drei Kategorien derartiger Spuren: persistente Daten auf der Festplatte, semipersistente Daten des Arbeitsspeichers sowie flüchtige Daten in den Registern der Prozessoren (vgl. Pawlaszczyk, 2017, S. 117). Und doch kongruiert die Vorgehensweise, digitale Spuren nur anhand ihrer Flüchtigkeit einzuteilen, nicht mit einer allumfassend vernetzten digitalen Lebenswirklichkeit. Digitale Spuren sind nicht mehr wie physische Spuren an eine räumlich-zeitliche Lage gebunden. Daten werden nicht mehr nur auf lokalen IT-Systemen gespeichert, sondern auch zunehmend durch Online-Dienste wie Cloudspeicher, soziale Netzwerke oder Messengerdienste verteilt. Sie sind folglich viel stärker verstreut als noch vor einigen Jahren (ebd., S. 118). Und so können digitale Spuren heutzutage lokal sowie auf tausende Kilometer entfernten IT-Systemen zu finden sein. Dabei ist es auch nicht ungewöhnlich, dass die Lokalisierung von Daten wie bei einigen Cloud-Diensten völlig verschwimmt (vgl. Jaquet-Chiffelle, 2014, S. 189). Jaquet-Chiffelle konzeptualisiert aus dieser Tatsache heraus zwei Typen digitaler Spuren: einerseits diejenigen, welche direkt mit physischen Datenträgern verknüpft sind und andererseits Spuren, die er als rein virtuell bezeichnet. Hieraus folgend trennt Jaquet-Chiffelle digitale Ermittlungen der sog. ersten Generation, also solche, die sich mit lokal vorzufindenden IT-Systemen und deren Datenträgern wie etwa Festplatten, USB-Sticks oder auch DVDs befassen, von digitalen Ermittlungen der zweiten Generation, welche die rein virtuellen Spuren wie etwa Daten aus Kommunikation, Blogs oder sozialen Netzwerken erfassen (vgl. ebd., S. 189 f.). Und auch Baier unterscheidet zwischen lokalen und nicht lokalen digitalen Spuren (vgl. Baier und S. Gärtner, 2019, S. 24). Es zeigt sich also, dass digitale Spuren sich einerseits nach ihrer Flüchtigkeit und andererseits nach ihrer Entfernung zum Tat- bzw. Ereignisort kategorisieren lassen. Trotzdem ist die eindeutige Zuordnung nicht immer gegeben, denn bestimmte digitale Spuren erfüllen die Bedingungen mehrerer Kategorien. So sind

digitale Spuren, welche sich in einer Cloud unbekannter Lokalität befinden, in ihrer Gesamtheit nicht rein virtuell, denn ohne lokal auf einem IT-System gespeicherte Zugangsinformationen zu ihnen wären sie erst gar nicht zu identifizieren (vgl. Martini, Do und Choo, 2015). Des Weiteren ist die Persistenz der sog. virtuellen Spuren nicht immer greifbar. Daten in einer Cloud gelten als persistent, denn ihre Speicherung soll dauerhaft sein. Netzwerkdaten sind im allgemeinen immer flüchtig, denn es handelt sich ausschließlich um Kommunikationsdaten zwischen IT-Systemen. Die Nutzer-Profilseite in einem sozialen Netzwerk wiederum kann einen Mix aus persistenten und dynamisch mittels bestimmter Algorithmen zur Aufrufzeit generierten Inhalten enthalten, so dass verschiedene, auch unmittelbar aufeinander folgende Aufrufe, jeweils unterschiedliche Inhalte der Profilseite generieren.

Es wird deutlich, dass durch die zunehmende Vernetzung einer bunten Vielfalt digitaler Systeme, Smart Devices und nicht zuletzt dem IoT die Einordnung digitaler Spuren in eine eindeutige Kategorie oftmals nicht mehr gegeben ist. Dies ist für die polizeiliche Ermittlungsarbeit jedoch nicht vorrangig von Relevanz, denn für sie steht im Vordergrund, dass digitale Spuren möglichst lückenlos identifiziert und gesichert werden können, sowie dass ihre Authentizität und Integrität zwingend gewahrt und nachweisbar bleibt. Trotzdem ist eine gewisse Klassifizierung auch für die Ermittlungsarbeit notwendig, da sich hieraus einerseits die jeweils passende Technik und Vorgehensweise zur Sicherung und Analyse sowie andererseits die Priorisierung und Reihenfolge zu sichernder Spuren ergibt. Abgesehen davon lässt sich aus der Klassifizierung digitaler Spuren ebenfalls erkennen, welche technischen und vor allem fachliche Voraussetzungen gegeben sein müssen, um zum einen ihre Sicherung und zum anderen ihre kompetente Weiterverwertung im Zuge der Ermittlungsarbeit zu gewährleisten.

Resultierend aus dem bereits dargelegten lässt sich folgendes festhalten: Für die Sicherung lokaler digitaler Spuren ist der Grad ihrer Flüchtigkeit von entscheidender Bedeutung, da in diesen Fällen in der großen Mehrheit ein originärer physischer Datenträger für die Ermittlungen zur Verfügung steht, durch welchen sich die Authentizität und Integrität von Spuren mit technischen Mitteln jederzeit auch wiederholend nachweisen lässt. Die von Jaquet-Chiffelle konzeptualisierten virtuellen Spuren werden als Remote- bzw. Online-Spuren klassifiziert, da für sie keine Lokalisation möglich ist, sowie kein die Spur originär beinhaltender physischer Datenträger zur Verfügung steht. In diesen Fällen ist die Flüchtigkeit eher uninteressant, zugleich ist der Nachweis der

Authentizität und Integrität nicht mehr rein technisch, sondern durch die Ermittlungsperson selbst zu gewährleisten. So werden nachfolgend die Kategorien der persistenten, semipersistenten, transienten und Remote- bzw. Online-Spuren in ihren wichtigsten Eigenschaften beleuchtet und zusätzlich die für sie bewährte Vorgehensweise zur gerichtsfesten Sicherung und Analyse erörtert. Darüber hinaus wird diskutiert, welche fachlichen Qualifikationen für die professionelle Bearbeitung einer Spur der jeweiligen Klasse erforderlich sind, was wiederum für die polizeiliche Ermittlungsarbeit von entscheidender Bedeutung ist. Auf technische Details in Bezug auf Hard- und Software zur Sicherung und Auswertung wird weitestgehend verzichtet, insofern dies für die Hypothesen und Forschungsfragen dieser Arbeit von untergeordneter Bedeutung ist.

3.4.1 Persistente digitale Spuren

Persistente digitale Spuren können gewissermaßen als die Klassiker der IT-Forensik bezeichnet werden. Sie entstammen üblicherweise Datenträgern, welche Daten ohne Stromzufuhr über einen längeren Zeitraum speichern können, wie etwa Festplatten, CD/DVDs, Flash-Speicher wie USB-Sticks und SD-Karten oder die für die langfristige Datensicherung verwendeten Magnetbänder. Durch ihre geringe Flüchtigkeit sind persistente Spuren über einen langen Zeitpunkt auffindbar, so dass sie zeitlich nahezu beliebig lang nach einem Ereignis noch identifiziert und analysiert werden können, ohne dass die Gefahr besteht, dass sie verloren gehen (vgl. Dewald und F. C. Freiling, 2015, S. 37). Auch hat das Abschalten eines IT-Systems i. d. R. keinen Einfluss auf persistent gespeicherte Daten. Eine wichtige Eigenschaft persistenter digitaler Spuren ist, dass sie Informationen zu einem Ereignisses oder einem Vorfall liefern, welches bereits stattgefunden hat und abgeschlossen ist. Die Vorgehensweise zur ihrer Sicherung hat sich seit Jahren bewährt und wird als sog. Post-mortem-Analyse bezeichnet (vgl. ebd., S. 57). Wie die Bezeichnung bereits andeutet, werden Spuren auf einem „toten“, also ausgeschalteten System gesichert. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) liefert folgende Definition: „[. . .] [B]ei der Post-mortem-Analyse (auch bekannt als Offline-Forensik) [wird] der Vorfall nachträglich aufgeklärt. Dies geschieht im Wesentlichen durch die Untersuchung von Datenträgerabbildern (so genannten Images) auf nichtflüchtige Spuren [. . .] von Vorfällen. Das

Hauptaugenmerk liegt dabei auf der Gewinnung und Untersuchung von gelöschten, umbenannten sowie anderweitig versteckten und verschlüsselten Dateien von Massenspeichern“ (BSI, 2011, S. 13).

Die Durchführung der Post-mortem-Analyse erfolgt in zwei Schritten. Im ersten Schritt wird eine forensische Kopie eines Datenträgers erstellt. Diese hält den Ist-Zustand des Datenträgers unverfälscht und unveränderbar fest, was entscheidend für die Auswertbarkeit und Beweiskraft ist (vgl. Pawlaszczyk, 2017, S. 125). Ein besonderes Augenmerk liegt weiterhin darauf, dass auch durch bzw. während der Sicherung keine Veränderung am System entstehen. Neben einer genauen Dokumentation, wann und wie die forensische Kopie durchgeführt wurde, ist die Verwendung eines sog. Write-Blockers[41] so gut wie obligatorisch, so dass sichergestellt ist, dass keine Schreibzugriffe auf den zu sichernden Datenträger stattfinden können (vgl. Müller, 2013, S. 46). Die Eigentliche Untersuchung erfolgt anschließend im zweiten Schritt. Dieser ist zeitlich und örtlich völlig unabhängig vom ersten Schritt, denn die Suche nach digitalen Artefakten erfolgt ausschließlich auf der forensischen Kopie. Hierfür ist keine bestimmte Vorgehensweise festgeschrieben, die angewandten Verfahren und Schritte müssen aber nachvollziehbar und dokumentiert sein, darüber hinaus muss die Integrität der Spur zu jeder Zeit gewahrt sein. Der Analyseprozess selbst ist aus vielen Teilschritten zusammengesetzt, auf die im Zuge dieser Arbeit nicht explizit eingegangen wird. Grob illustriert wird bestimmt, welche Daten sich auf dem Speichermedium befinden und welche gelöschten Daten sich wiederherstellen lassen. Diese Daten werden gesichtet, gefiltert und auf ihre Relevanz hin bewertet (vgl. Pawlaszczyk, 2017, S. 132). Die britische Association of Chief Police Officers (ACPO) mahnt jedoch zu recht an, dass es nicht wünschenswert sei, alle gespeicherten Daten zur Überprüfung durch den Ermittler zu extrahieren. Vielmehr müsse eine forensische Strategie formuliert werden, damit sich die Untersuchung auf relevante Daten konzentrieren kann. Zusätzlich ist gerade bei komplexen Untersuchungen eine enge Zusammenarbeit von Ermittler und IT-Forensiker vonnöten, denn nur so kann mit dem Auffinden digitaler Beweise die forensische Strategie rechtzeitig angepasst und die Richtung der Untersuchung zweckdienlich gesteuert werden (vgl. ACPO, 2012, S. 10).

[41] Ein Write-Blocker ermöglicht den schreibgeschützten Zugriff auf ein Speichermedium, indem ein Hardware- oder Softwarefilter zwischen dem lesenden System und dem Speichermedium wird (vgl. Lyle, Mead und Rider, 2007).

Schlussendlich ist erkennbar, dass persistente digitale Spuren ein fachlich-arbeitsteiliges Vorgehen ermöglichen. IT-Forensiker führen die Sicherung einer Spur durch, Ermittler geben mit präzisen Fragestellungen zu den vorhandenen Daten den Forensikern eindeutige Vorgaben zur Spurensuche. Die Suchergebnisse wiederum werden den Ermittlern zur weiteren Prüfung zur Verfügung gestellt, da diese die zu beantwortenden Fragen des Ermittlungsverfahrens kennen. Durch die komplette Sicherung aller auf einem Speichermedium vorhandenen Daten werden auch gelöschte Daten in die Untersuchung mit eingebunden, gleichzeitig erfolgt keinerlei Veränderung am System durch Tätigkeiten der Sicherung und Auswertung. Im Gegenzug aber ist eine physische Komplettsicherung eines Speichermediums unabhängig von der Menge gespeicherter Daten immer sehr zeitaufwändig. Dieser Nachteil entspannt sich teilweise durch die Tatsache, dass das Erstellen einer Kopie nicht zeitgleich im Rahmen polizeilicher Maßnahmen erfolgen muss, sondern zu einem beliebigen späteren Zeitpunkt erfolgen kann. Ein Vergleich persistenter digitaler Spuren mit ihren physischen Pendants legt zudem offen, dass ihre Bearbeitung in der polizeilichen Ermittlungsarbeit von vielen Parallelen geprägt ist. Am Herausragendsten tritt die strikte Arbeitsteilung zwischen Ermittlungsarbeit und IT-Forensik in Erscheinung, die dazu führt, dass diese Klasse digitaler Spuren relativ überschaubare Anforderungen an die IT-fachliche Kompetenz polizeilicher Ermittlungsarbeit stellt.

3.4.2 Semipersistente digitale Spuren

Die einschlägige Fachliteratur postuliert digitale Spuren übereinstimmend als semipersistent, sofern sie bei entsprechender Stromzufuhr über einen langen bzw. dauerhaften Zeitraum erhalten bleiben. Wird die Stromzufuhr unterbrochen, so sind semipersistente Daten unmittelbar oder kurze Zeit danach vollständig verloren (vgl. Dewald und F. C. Freiling, 2015, S. 37; Baier und S. Gärtner, 2019, S. 26; Meier, 2016, S. 24). Typischer Vertreter dieser Klasse digitaler Spuren ist der Hauptspeicher eines IT-Systems, der sog. Random-Access Memory (RAM). Dessen Daten sind nach Trennung der Stromzufuhr noch einige Sekunden bis hin zu mehreren Minuten erhalten (vgl. Pawlaszczyk, 2017, S. 121). Ein weiterer, meist nur im Fehlerfall in Erscheinung tretender Vertreter ist der Complementary Metal Oxid Semiconductor (CMOS), ein

batteriegepufferter Speicher, in welchem die BIOS[42]-Parameter eines PCs gespeichert werden. Einer rein hardwarenahen Interpretation semipersistenter digitaler Spuren kann nicht direkt widersprochen werden, sie ist jedoch zu sehr auf physische Datenträger fokussiert. Die Abstraktion semipersistenter Spuren auf Systemebene inspiriert hingegen zu einer Erweiterung dieser Sichtweise. Denn jedes IT-System erzeugt innerhalb seiner komplexen Datenstruktur semipersistente Daten, welche nur zur Laufzeit des Systems zu finden sind. Dies sind beispielsweise Daten über laufende Prozesse, geöffnete Netzwerkverbindungen, angemeldete Nutzer oder Dateien zur Speicherauslagerung[43]. Da auch diese Daten beim Abschalten eines Systems unwiederbringlich verloren wären, wird die Sicherung semipersistenter Daten i. d. R. mittels einer Live-Analyse, also am noch laufenden System, vorgenommen. Ohne sich in technische Details zu vertiefen, ist augenscheinlich, dass diese Vorgehensweise zwangsläufig Änderungen des Systemzustandes verursacht, welche technisch nicht zu vermeiden sind. Aber nur durch die Analyse am laufenden System lassen sich bereits genannte Spuren identifizieren und sichern, zusätzlich ist die Chance gegeben, dass sich im RAM eines System Artefakte von Passwörtern bzw. Entschlüsselungspasswörter finden lassen (vgl Pawlaszczyk, 2017, S. 119 f.). Die Live-Analyse umfasst im Wesentlichen die Erstellung eines Speicherabbildes, auch RAM-Dump[44] genannt, sowie die Akquise wichtiger Daten des laufenden Systems. Neben hierfür geeigneten Werkzeugen ist es substantiell, keine Tools des laufenden Betriebssystems oder dessen Anwendungen zu nutzen, da diese manipuliert sein könnten und verfälschte Daten liefern. Des Weiteren ist das Aufspielen oder Entfernen von Daten und Programmen zu vermeiden, da dies die Integrität der Spur unnötig weiter verfälscht (vgl. Brezinski und Killalea, 2002, S. 4).

---

42 Beim BIOS handelt es sich um die Schnittstelle zwischen der Hardware und dem Betriebssystem eines PC. Das Betriebssystem greift auf Funktionen im BIOS zurück, um die angeschlossene Hardware anzusprechen.

43 Wenn die Größe des Hauptspeichers (RAM) eines IT-Systems für die Bearbeitung bestimmter Aufgaben nicht ausreicht, erfolgt eine virtuelle Vergrößerung desselben, indem ein Bereich auf der Festplatte des Systems den RAM nachahmt.

44 Neben der Erstellung eines Abbildes des Hauptspeichers mittels Live-Analyse tritt die sog. Cold-Boot-Attack in der Fachliteratur regelmäßig in Erscheinung. Diese nutzt den Umstand aus, dass Daten im RAM eines Systems auch nach Trennung der Stromzufuhr noch einige Zeit verfügbar sind. Durch zügigen Neustart mittels eines Live-Betriebssystems können die Daten des RAM u. U. nachträglich ausgelesen werden, was z.B. bei gesperrten und verschlüsselten Systemen hilfreich ist (vgl. Pawlaszczyk, 2017, S. 121). Die Cold-Boot-Attack besitzt durch ihre geringe Zuverlässigkeit eher akademischen Charakter und ist zudem durch die Verschlüsselung moderner Hauptspeicher kaum noch von praktischer Bedeutung (vgl. Bauer, Gruhn und F. C. Freiling, 2016).

Neben der Sicherung semipersistenter Spuren ist die Live-Analyse aus einem zweiten Grund auf vernetzten Systemen nahezu unverzichtbar. Zum einen können die Daten eines Systems durch den Eigentümer mittels Verschlüsselung vor unbefugtem Zugriff geschützt sein, und ein Ausschalten des Systems versperrt den Zugriff auf dessen Daten. Zum anderen kann schon währen einer polizeilichen Maßnahme das Bedürfnis bestehen, Inhalte von verbundenen Cloud-Speichersystemen oder E-Mail-Konten einzusehen (vgl. Dewald und F. C. Freiling, 2015, S. 248). Nicht selten werden online gespeicherte Daten durch die Betroffenen im Anschluss einer polizeilichen Maßnahme gelöscht und wären ohne die Sicherung durch eine Live-Analyse verloren.

Infolgedessen kann konstatiert werden, dass semipersistente Spuren weitaus mehr Ansprüche an die Kompetenz polizeilicher Ermittlungsarbeit stellen. Eine Ermittlungsperson muss einerseits über die technischen Voraussetzungen (Hard- sowie Software) verfügen, um eine Live-Analyse gängiger IT-Systeme selbständig durchführen zu können. Andererseits ist eine ausreichend fachlich-technische Kompetenz sowie Handlungssicherheit im Umgang mit den gegebenen Werkzeugen unabdingbar. Da die Integrität der Spur durch Arbeiten am laufenden System beeinträchtigt wird, ist zudem eine lückenlose Protokollierung aller durchgeführten Arbeitsschritte immanent. Wenngleich die Live-Analyse semipersistenter Spuren nicht die tiefgreifenden Kenntnisse eines IT-Forensikers erfordert[45], so initiiert sie doch steigende technische Anforderungen an die polizeiliche Ermittlungsarbeit.

3.4.3 Transiente digitale Spuren

Wie auch die semipersistenten werden transiente oder auch flüchtige Spuren in der Fachliteratur übereinstimmend als solche bezeichnet, die trotz dauerhafter Stromzufuhr nur temporär für kurze Zeit verfügbar sind. Beispielhaft werden wiederkehrend die Daten innerhalb von Prozessorregistern sowie Netzwerkdaten aufgeführt (vgl. Dewald und F. C. Freiling, 2015, S. 37; Baier und S. Gärtner, 2019, S. 26; Meier, 2016, S. 24). Während bei semipersistenten

[45] Bis auf wenige spezielle Tools, z.B. zur Sicherung des RAM-Inhaltes kommen im Zuge der Live-Analyse i. d. R. Standard-Tools zum Einsatz, wie sie in jeder Betriebssystemumgebung zu finden sind (vgl. Brezinski und Killalea, 2002, S. 7 f.). Des Weiteren gibt es eine Vielzahl an Tools, die die Teilaufgaben einer Live-Analyse automatisieren, so dass diese i. d. R. durch jede IT-affine Ermittlungsperson durchgeführt werden kann.

Daten für die Dauer der Stromzufuhr eine Speicherung sicher ist, so unterliegen transiente Daten nicht einmal einer kurzzeitigen Speicherung. Folglich kann diese Klasse Spuren nur zum Zeitpunkt ihres Auftretens identifiziert und gesichert werden. Bei Netzwerkdaten beispielsweise ist dies der unmittelbare Zeitraum während der Datenübertragung. So müssen transiente digitale Spuren entweder im laufenden Betrieb analysiert oder für die spätere Bearbeitung aufgezeichnet und auf einem persistenten Datenträger abgespeichert werden (vgl. Baier und S. Gärtner, 2019, S. 26). Neben Netzwerkdaten auf physischen Leitungen treten zunehmend Funkdaten verschiedenster Protokolle in den Alltag der Ermittlungsarbeit. Populärster Vertreter dieser Funk-Protokolle ist zweifelsohne der WLAN-Standard nach 802.11[46]. Aber auch Bluetooth[47] im Zusammenhang mit Smart-Devices oder die XBee-Protokollfamilie[48] im Bereich des IoT sind sehr weit verbreitet.

Bedingt durch ihre ausschließliche Flüchtigkeit können transiente digitale Spuren nur mittels Live-Analyse gesichert werden. Die Vorgehensweise gleicht grundsätzlich den bei semipersistenten Spuren angewendeten Methoden. Dessen ungeachtet sind Anforderungen an notwendiger Technik und fachlicher Qualifikation ungleich höher. So ist es überwiegend erforderlich, dass zur Sicherung der Netzwerkdaten in kabelgebundenen Umgebungen ein erweiterter Zugang zu Netzwerkkopplungsgeräten gegeben sein muss[49]. Äquivalent verhält es sich mit der Aufzeichnung von Netzwerkdaten in kabellosen Umgebungen. Zwar erfolgt in Funknetzwerken auf physikalischer Ebene keine direkte Zustellung der Datenpakete[50], so dass eine Aufzeichnung der Netz-

46 802.11 bezeichnet eine Protokollfamilie für das Wireless Local Area Network (WLAN) und bildet das kabellose Pendant zu kabelgebunden, mittels Ethernet vernetzten IT-Systemen. Häufig wird diese Protokollfamilie auch als Wi-Fi bezeichnet (vgl. Ballmann, 2015, S. 113 ff.).

47 Bluetooth ist ein Datenübertragungsprotokoll, welches u. a. von Mobiltelefonen, Headsets oder auch kabellosen Tastaturen implementiert wird. Der Standard umfasst die Klassen 1 bis 3 mit einer mittleren Reichweite von 1m bis 100m (vgl. ebd., S. 137 ff.).

48 XBee-Module sind in sich geschlossene, modulare und kostengünstige Komponenten, die mithilfe eines eigenen schlanken Hochfrequenz-Funkprotokolls (2,4 GHz oder 900 MHz) Daten untereinander austauschen (vgl. Bell, 2020, S. 36 ff.).

49 So leitet z. B. ein Netzwerk-Switch im Gegensatz zu den früher verwendeten einfachen Hubs Paketdaten nur zum dem Port, für welchen diese bestimmt sind. Im Umkehrschluss heißt das, dass ein IT-System nur seine eigenen Datenpakete „sieht“. Zum Mitschneiden des gesamten Netzverkehrs für Wartungs- und Testzwecke wurde das sog. Port-Mirroring eingeführt. Die Funktionsweise dieser Technik besteht darin, alle eingehenden sowie ausgehenden Pakete auf einen dedizierten Port, der als Mirror-Port bezeichnet wird, zu spiegeln. Über diesen Port kann dann ein Tool zur Paketerfassung für die Analyse und Speicherung des Netzverkehrs genutzt werden (vgl. Zhang und Moore, 2007).

50 Jedes Funknetzwerk ist aus sich selbst heraus ein sog. Shared-Medium, d. h. „jeder“ empfängt „alles“.

werkdaten in jedem Fall möglich ist, sofern man sich in Reichweite eines entsprechenden Funknetzes befindet. Allerdings wird hier seitens der Ermittlungsperson geeignete Hard- und Software[51] benötigt.

Im Rahmen der polizeilichen Ermittlungsarbeit stellen transiente digitale Spuren eine besondere Herausforderung dar. Sie erfordern nicht nur eine Sicherung „zur Laufzeit“, sondern auch fachlich qualifiziertes Personal sowie eine adäquate technische Ausrüstung am Ereignisort bzw. am Ort einer Maßnahme. Zudem sind die erforderlichen Schritte zum Nachweis von Authentizität und Integrität gesicherter Spuren sowie die lückenlose Protokollierung aller Arbeitsschritte obligatorisch. Darüber hinaus können Informationen aus transienten digitalen Spuren äußerst wertvoll sein. So lassen sich aus Netzwerkdaten nicht nur Informationen zu deren Inhalt verwerten. Auch aus den Metadaten[52] lassen sich zahlreiche Informationen gewinnen, die für die Ermittlungsarbeit von großer Hilfe sein können[53].

3.4.4 Remote- bzw. Onlinespuren

Während sich der konservative Blick auf digitale Spuren definitionsgemäß und inhaltlich auf persistente bis transiente Spuren physischer Geräte und Systeme richtet (vgl. F. Freiling und K. Sack, 2017; Dewald und F. C. Freiling, 2015; Eisenbraun, 2020; NIJ, 2019), erweitert die grenzenlose Vernetzung einer immer heterogener werdenden Systemlandschaft den fachspezifischen Blickwinkel um Spuren, die sich zunehmend außerhalb einer lokalen Zugriffsmöglichkeit zu einem physischen Spurenträger befinden (vgl. Baier und S. Gärtner, 2019, S. 24; Momsen, 2015, S. 71 f.). Pawlaszczyk konstatiert, dass die forensische Analyse von Datenträgern längst nicht mehr ausreiche, um Spuren kriminellen Verhaltens zu identifizieren. Viel mehr müssten im Zuge einer modernen Fallarbeit auch nicht lokale Spuren im Internet, beispielsweise aus Cloud-Speichern und sozialen Netzwerken, identifiziert und analysiert werden. Der Überzeugung, dass dieser Bereich digitaler Spuren zunehmend an Bedeutung gewinnt, ist sich Pawlaszczyk aber zugleich bewusst, dass

---

51 So muss ein WiFi-Adapter zum Mitschneiden aller Daten des Funknetzes u. a. den sog. Monitor-Mode beherrschen (vgl. Meinel und H. Sack, 2012, S. 172).

52 Mit Metadaten sind im Zusammenhang von Netzwerkdaten beispielsweise die Informationen über Hosts eines Netzwerks oder unterschiedlicher Netzwerke in einer Wifi-Umgebung gemeint.

53 mehr dazu in Abschnitt 4.1.2

es sich hierbei um ein recht junges Forschungsfeld handelt, welches methodisch noch unzureichend untersucht ist (vgl. Pawlaszczyk, 2017, S. 113 f.). Und auch Jaquet-Chiffelle postuliert in gleicher Weise die digitalen Ermittlungen zweiter Generation (vgl. Jaquet-Chiffelle, 2014, S. 190) und deutet an dieser Stelle unbewusst an, dass die von ihm genannten virtuellen Spuren weniger Berührungspunkte mit der IT-Forensik als mit der klassischen kriminalistischen Ermittlungsarbeit besitzen, da diese Art Spuren in einer digitalisierten Medienumgebung individueller, kollektiver oder korporativer Akteure generiert werden (vgl. Breiter und Hepp, 2018, S. 30). Sie sind sozusagen Online-Fußabdrücke ihrer Verursacher. Ebendarum ist es konsequent, in einer ubiquitär vernetzten Lebenswelt die Klasse der Remote- bzw. Online-Spuren zu definieren. Dies können Spuren aus klassischen Webseiten, sozialen Netzwerken, Kommunikationsdiensten, Cloud-Speichern, Chatrooms oder auch Kryptowährungs-Systemen sein. Es ist nicht möglich, diese Klasse digitaler Spuren inhaltlich ins Detail zu definieren, denn ihr Auftreten ist zu vielfältig, und sie unterliegen einer sehr großen Dynamik. Es entstehen unaufhörlich neue mögliche Datenquellen mit strukturierten aber auch unstrukturierten Inhalten.

Remote- bzw. Online-Spuren sind im Zuge polizeilicher Ermittlungsarbeit bzgl. ihrer Persistenz und Lokalisation zu einem Großteil unbestimmt, zudem wurden die zur Wahrnehmbarkeit obligatorischen Abstraktionsschritte transparent durchlaufen. Dies bedeutet, dass i. d. R. nur die letzte, also die Spureninformation wiedergebende Abstraktionsschicht für eine Sicherung zur Verfügung steht. Im Zuge der Akquise von Remote- bzw. Online-Spuren stellen sich für die Ermittlungsarbeit in organisatorischer, technischer sowie juristischer Hinsicht ganz neue Fragestellungen und Herausforderungen (vgl. Beebe, 2009, S. 28), welche nachfolgend anhand des mittelbaren Zugriffs[54] auf Cloud-Speicher illustriert werden. Im Allgemeinen ist festzustellen, dass es kein allgemein akzeptiertes festes Schema für das konkrete Vorgehen zur Sicherung von Online-Spuren gibt, denn die meisten klassischen Verfahren zur Identifikation und Sicherung digitaler Spuren beziehen sich auf physische Datenspeicher. Aus diesem Grund greifen die bisher erwähnten Werkzeuge zur Post-mortem- aber auch zur Live-Analyse nur in begrenztem Umfang. Cloud-Speicher sind räumlich entgrenzt, so dass Datenspeicher nicht einfach sichergestellt oder zu späteren Analyse kopiert werden können (vgl. Pawlasz-

[54] Dieser besteht u. a. im Rahmen offener Ermittlungsmaßnahmen, beispielsweise während einer Durchsuchung über das vorhandene Computersystem.

czyk, 2017, S. 148). Zusätzlich ist die Persistenz und im Umkehrschluss die Volatilität von Cloud-Daten völlig unbestimmt. Um den Nutzern dieser Systeme eine größtmögliche Zuverlässigkeit und Skalierbarkeit zu gewährleisten, können Ressourcen wie Speicherplatz und Rechenleistung ebenso schnell gelöscht werden, wie sie bereitgestellt wurden. So ist derweilen nach dem Freigeben von Cloud-Speichern ein Komplettverlust der gespeicherten Daten zu erwarten, da diese Kapazitäten sofort weiteren Nutzern zur Verfügung stehen und selbst auf physischen Datenträgern keine verwertbaren Spuren zu erwarten sind (vgl. Reiser, Rakotondravony und Köstler, 2017, S. 13 f.). Abgesehen davon ist im Zuge der globalen Vernetzung oftmals unklar, an welchem Ort die Daten gespeichert, und ob die Daten dort verschlüsselt abgelegt sind. In diesem Fall hätte selbst der Betreiber eines Cloud-Dienstes keine Zugriffsmöglichkeit auf die Daten (vgl. Pawlaszczyk, 2017, S. 148).

Ohne tiefgründig auf die technischen Details von Cloud-Infrastrukturen einzugehen, ist erkennbar, dass durch sie äußerst hohe Anforderungen an IT-Forensiker sowie Ermittlungspersonen gestellt werden, gleichzeitig sind aber Werkzeuge und Vorgehensmodelle noch nicht in dem Maße etabliert, wie es bei traditionellen IT-Systemen der Fall ist. Neben den unterschiedlichen Cloud-Service-Modellen[55] erschweren die unterschiedlichen Cloud-Arten[56] die Identifizierung digitaler Spuren und die Festlegung einer geeigneten Vorgehensweise zu ihrer Sicherung. Teilweise finden sich durch die Nutzung von Cloud-Diensten Datenspuren auf entsprechenden Endgeräten, so dass sich in solchen Fällen Daten nicht nur auf Seite des Dienstanbieters, sondern auch auf den Endgeräten der Anwender befinden. Im Allgemeinen gilt aber, dass bei der großen Vielfalt an Diensten, Datenformaten und teilweise proprietären Protokollen häufig nicht genau bekannt ist, welche verwertbaren Spuren entstehen können und wie diese auszuwerten sind (vgl. Reiser, Rakotondravony und Köstler, 2017, S. 20). Dass für die Sicherung von Cloud-

[55] Beim Cloud-Computing werden generell drei sogenannte Cloud-Service-Modelle unterschieden: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Im Rahmen von IaaS werden dem Nutzer komplette IT-Basisinfrastrukturen bereitgestellt, während PaaS dem Nutzer integrierte Laufzeit- und Entwicklungsumgebungen für Anwendungen zur Verfügung stellt. SaaS wiederum umfasst lediglich die Bereitstellung einer Anwendung zur Nutzung über das Internet bzw. Intranet (vgl. Biebl, 2012, S. 25).

[56] Neben Cloud-Modellen werden zusätzlich die Arten Private Cloud (wird ausschließlich für eine Organisation oder eine Gemeinschaft betrieben), Public Cloud (wird über das Internet zur Verfügung gestellt und kann von beliebigen Personen und Unternehmen genutzt werden) sowie Hybrid-Cloud (integriert zwei oder mehr voneinander unabhängige Cloud-Infrastrukturen und die traditionelle IT-Infrastruktur so miteinander, dass für den Nutzer eine homogene Umgebung entsteht) unterschieden (vgl. ebd., S. 26).

Daten spezielles Fachwissen erforderlich ist, muss absolut bejaht werden. Wirklich problematisch im Rahmen polizeilicher Ermittlungsarbeit ist aber, dass die Cloud-Forensik erst seit kurzem in den Fokus der wissenschaftlichen Forschung geraten ist und geeignete Ausbildungsprogramme noch nicht ausreichend etabliert sind. Dies stellt hinsichtlich cloud-spezifischer Untersuchungen ein wirkliches Problem dar (vgl. Reiser, Rakotondravony und Köstler, 2017, S. 14)!

Über die technischen Hürden hinaus treten im Zusammenhang mit Remote- bzw. Online-Spuren ebenfalls besondere juristische Herausforderungen zu Tage. Eine dieser besonderen Herausforderungen stellt sich durch den über das *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*[57] vom 21. Dezember 2007 eingeführten § 110 Abs. 3 StPO. Dieser erlaubt es Strafverfolgungsbehörden, bei Durchsuchungen auch auf räumlich getrennte Speichermedien zuzugreifen, wenn der Zugriff von einem Computersystem vor Ort möglich ist. Diese Norm soll der Gefahr entgegenwirken, dass Inhalte vom Beschuldigten vernichtet oder verschoben werden, wenn kein sofortiger Zugriff auf extern gespeicherte Daten erfolgt. Weniger technische, denn mehr juristische Schranken setzen dem Zugriff der Strafverfolgungsbehörden einschlägiger Auffassungen nach enge Grenzen. Im Angesicht der Tatsache, dass große Cloud-Anbieter wie Google, Amazon oder Microsoft ihre Infrastruktur nicht in Deutschland betreiben, findet die Norm dort ihre Grenzen, wo nationale Hoheitsrechte enden. § 110 Abs. 3 StPO gilt dieser Auffassung nach nur, sofern sich die Datenspeicher eines Cloud-Anbieters im Inland befinden, denn inländischen Ermittlungsbehörden stehen im Ausland grundsätzlich keine Hoheitsbefugnisse zu (vgl. Süptitz, Utz und Eymann, 2013, S. 310; Dalby, 2016, S. 214 f.; Czerner, 2017, S. 297 f.). Gleichzeitig wird darauf abgestellt, dass durch die Strafverfolgungsbehörden der physikalische Speicherort zur Bestimmung der örtlichen Zuständigkeit festgestellt werden muss, sofern Kenntnisse über Cloud-Dienste erlangt wurden, um keine Verletzung des völkerrechtlichen Souveränitätsprinzips herbeizuführen (vgl. Dalby, 2016, S. 246 f.). So wird in Ermangelung eines kohärenten Strafanwendungsrechts in der Rechtshilfe durch ausländische Ermittlungsbehörden das einzige Mittel zur Beweisgewinnung über Landesgrenzen hinweg gesehen, welche durch Art. 29. der Cybercrime-Konvention (CCK)[58] effektiviert und beschleu-

[57] BGBl. 2007 I, S. 3198

[58] Die Cybercrime-Konvention vom 23.11.2001 ist ein Übereinkommen, das vom Europarat entworfen wurde und die verstärkte Zusammenarbeit im Bereich des

nigt werden kann. Eine weitere Möglichkeit bietet Art. 32 CCK, welche den transnationalen Zugriff auf Computersysteme und Daten erlaubt, wenn es sich einerseits um offene Quellen handelt oder andererseits der Berechtigte seine freiwillige Zustimmung hierzu erteilt. Eine Verletzung dieses Souveränitätsgrundsatzes durch die Strafverfolgungsbehörden kann im Einzelfall zu einem Beweisverwertungsverbot führen (vgl. Süptitz, Utz und Eymann, 2013, S. 312).

Die aufgezeigten juristischen Hürden verdeutlichen die Diskrepanz zwischen technischen Ermittlungsmöglichkeiten einerseits und rechtlichen Schranken andererseits. Aus einer restriktiven Perspektive vereitelt die Datenauslagerung in die Cloud somit den unmittelbaren Zugriff (Durchsuchung und Beschlagnahme) deutscher Ermittlungsbehörden (vgl. Dalby, 2016, S. 248 f.), obwohl den Nutzern von Cloud-Diensten oftmals weder bewusst sein dürfte, dass die Daten im Ausland gespeichert werden, noch die damit verbundene Absicht besteht, hierdurch den Zugriff der Strafverfolgungsbehörden zu unterbinden. Leider bestätigt selbst die jüngere berufliche Erfahrung des Autors, dass sogar Generalstaatsanwaltschaften diese Ansicht vertreten und Mitarbeitern polizeilicher Ermittlungsbehörden eindeutig vermitteln, dass Cloud-Daten im Zuge von Durchsuchungsmaßnahmen nicht zu sichern seien, wenn die Möglichkeit besteht, dass diese im Ausland gespeichert sind[59].

Einer solch strikten Auslegung der Strafprozessordnung sollte widersprochen werden, entspricht sie doch in keiner Weise der ermittlungstaktischen Lebenswirklichkeit. Hierauf stellt beispielsweise Bär ab. Zwar erkennt auch er die Problematik an, dass der nationalen Befugnis zur Online-Sichtung von Daten keine Rechtsgrundlage für einen Zugriff auf im Ausland gespeicherte Daten innewohnt, da dies bestehende Rechtshilfeübereinkommen[60] unterlaufen würde (vgl. Bär, 2011, S. 54). Dass aber die Verletzung des Souveränitätsrechts durch den transnationalen Datenzugriff fremder Staaten tatsächlich zu einem Verwertungsverbot führt, sei wenig geklärt:

Cybercrime zum Ziel hat (vgl. Council of Europe, 2001). Art. 29. CCK eröffnet eine beschleunigte und effektivere Beweismittelsicherung. Gemäß dieses Artikels ist der ersuchte Staat verpflichtet, im Zuge eines Begehrens umgehend alle nach seinem nationalen Recht möglichen Maßnahmen zur umgehenden Datensicherung zu treffen und die gesicherten Daten mindestens 60 Tage aufzubewahren (vgl. Süptitz, Utz und Eymann, 2013, S. 312).

59 Die propagierte Auffassung einzelner Staatsanwaltschaften geht über die Pflicht zur Ermittlung des Serverstandortes hinaus und verneint die Verwertung von Daten bereits, wenn bereits die Annahme besteht, sie könnten exterritorial gespeichert sein.

60 u. a. auch Art. 29. CCK, dessen Sinnfälligkeit teilweise in Frage stünde

> „Die Verwertbarkeit rechtswidrig erlangter Erkenntnisse ist vielmehr nach inzwischen gefestigter Rechtsprechung jeweils nach den Umständen des Einzelfalls zu beurteilen, insbesondere nach der Art des Verbots und dem Gewicht des Verfahrensverstoßes sowie der Bedeutung der im Einzelfall betroffenen Rechtsgüter. [...] Von einem Beweisverwertungsverbot ist deshalb nur dann auszugehen, wenn einzelne Rechtsgüter durch Eingriffe fern jeder Rechtsgrundlage so massiv beeinträchtigt werden, dass dadurch das Ermittlungsverfahren als ein nach rechtsstaatlichen Grundsätzen geordnetes Verfahren nachhaltig geschädigt wird und folglich jede andere Lösung als die Annahme eines Verwertungsverbotes [...] unerträglich wäre“ (Bär, 2011, S. 59).

In Bezug auf den transnationalen Zugriff auf Cloud-Daten im Rahmen offener Maßnahmen der Strafverfolgungsbehörden, z. B. über das IT-System am Durchsuchungsort, könne nur dann von einem Verwertungsverbot ausgegangen werden, wenn im Gegenzug der betreffende Staat bereits im Vorfeld diesem Zugriff widersprochen hat. Da Strafverfolgungsbehörden vor Ort meistens gar nicht in der Lage sind, den konkreten physikalischen Speicherort von Cloud-Daten festzustellen, sei aber selbst in solchen Fällen keine willkürliche Vorgehensweise zu unterstellen, welche ein Beweisverwertungsverbot nach sich zieht (vgl. ebd., S. 59). Gleichlautend vertritt Schmitt die Auffassung, dass die bloße Möglichkeit des Speicherortes von Cloud-Daten im Ausland keine Rechtshilfeverpflichtung auslöst, wobei ohnehin unklar wäre, wohin sie zu richten sei. Er sieht sogar den Zugriff auf die Daten vom Computer eines betroffenen Cloud-Nutzers als eine von § 110 Abs.3 gedeckte, rechtmäßige Ermittlungshandlung im Inland an (vgl. Meyer-Goßner und Schmitt, 2018, § 110 Rn. 7b f.). Unstrittig ist in jedem Fall, dass in Bezug auf die jeweiligen Rechtsgrundlagen und Umsetzungsmöglichkeiten Verbesserungen geschaffen werden müssen, „[...] damit die Grenzen des eigenen Hoheitsbereichs bei Ermittlungsmaßnahmen nicht einen Freiraum für international agierende Straftäter schaffen“ (Bär, 2011, S. 59).

Technische und rechtliche Unsicherheiten sind nicht die einzigen Herausforderungen, denen sich Strafverfolgungsbehörden im Zuge von Remote- bzw. Online-Spuren zu stellen haben. Bei der Spurensuche sehen sich die Ermittler mit einer stetig wachsenden Menge an Daten aus immer neuen Quellen konfrontiert. Stellvertretend seien Plattformen und soziale Netzwerke wie Youtube, Twitter, Facebook oder auch Snapchat, Instagram und TikTok genannt,

diese Aufzählung könnte um ein nicht unerhebliches Vielfaches erweitert werden. Auf diesen und vielen weiteren nicht genannten Plattformen geben Menschen offen und freiwillig Informationen über sich Preis und vernetzen sich sichtbar, beispielsweise über virtuelle Freundschaftsverbindungen. Es werden Inhalte konsumiert und aktiv produziert, und so entsteht zusehends ein digitaler Fingerabdruck im Netz, welcher für Ermittlungsbehörden mitunter wertvolle Informationen liefert. Die Gewinnung von Informationen aus diesen größtenteils unstrukturierten aber öffentlich verfügbaren Daten wird Open Source Intelligence (OSINT)[61] genannt und spielt in der Strafverfolgung sowie in der Gefahrenabwehr zunehmend eine wichtige Rolle. In der jüngeren Vergangenheit erfuhr in diesem Zusammenhang ebenfalls die Verfolgung von Zahlungsströmen im Bitcoin-Netzwerk[62] eine erhöhte Aufmerksamkeit, da sich die Nutzung von Kryptowährungen[63] bei der Begehung von Straftaten insbesondere im Cybercrime- und BtM-Bereich einer größer werdenden Beliebtheit erfreut.

Ohne im Rahmen dieser Arbeit tiefgreifend in die Vielfalt und Materie der Remote- bzw. Online-Spuren eindringen zu können, deutet sich bereits an, dass sich im Bereich dieser Klasse digitaler Spuren die Grenze zwischen IT-Forensik und digitaler Ermittlungsarbeit mehr und mehr verflüchtigt. Spuren dieser Art beantworten nicht mehr allein aus ihren Einzelinformationen heraus einfache Fragen zu einem Ereignis, sondern diese Informationen müssen genutzt werden, um mit ihnen weiterführende digitale Ermittlungen durchzuführen. Deutlich wird dies allein schon am Beispiel der Verfolgung von Finanzströmen in Bezug auf Kryptowährungen. Abschnitt 4.1.3 wird diese Problematik noch einmal aufgreifen. Letztendlich machen aber die Remote- und Online-Spuren mehr als deutlich, dass die Bearbeitung digitaler Spuren nicht

---

61 Der Begriff OSINT wurde durch das US-amerikanische Militär geprägt und umschreibt die Vorgehensweise, öffentlich verfügbare Informationen für einen bestimmten Zweck zu sammeln, zu filtern und im ermittlungstechnischen Kontext aufzubereiten. Typische OSINT-Quellen sind das Internet, traditionelle Massenmedien wie Tageszeitungen, Zeitschriften, wissenschaftliche Publikationen, Fotos und Videos oder auch Geoinformationen. Im Kontext digitaler Spuren ist das Internet die primäre Quelle von Informationen (vgl. Hassan und Hijazi, 2018, S. 1 ff.).

62 Bei Bitcoin handelt es sich um das erste digitale nicht zentral kontrollierte Zahlungssystem und somit den ersten Versuch, elektronisches Geld ohne Bindung an eine analoge Währung bereitzustellen (vgl. Pawlaszczyk, 2017, S. 156).

63 Kryptowährungen sind alternative Zahlungsmittel ohne zentrale Kontrollinstanz, mit denen man Waren oder Dienstleistungen kaufen kann. Sie können durch keine währungspolitisch aktive Zentralbankgesteuert werden (vgl. Kattwinkel, 2018). Die wohl bekannteste Kryptowährung ist Bitcoin, eine Übersicht von 2019 listet aber weit mehr als 2000 unterschiedliche Arten auf (vgl. Bergen, 2019).

allein dem Fachgebiet einer von der eigentlichen Ermittlungsarbeit abgekoppelten IT-Forensik zugeschrieben werden kann. Das gesamte Fachportfolio polizeilicher Strafverfolgung ist hiervon betroffen, denn nur durch tiefgreifende Kenntnisse eines jeweiligen Ermittlungsverfahrens können digitale Spuren entsprechend bewertet, miteinander in Zusammenhang gebracht und hieraus weitere Schlüsse gezogen werden.

3.5 Zusammenspiel digitale Spuren / Ermittlungsarbeit

Die unterschiedlichen Kategorien digitaler Spuren legen grundlegend den Grad ihrer jeweiligen Flüchtigkeit fest. Wie weiterhin festgestellt wurde, ist im Falle persistenter Spuren ein arbeitsteiliges Vorgehen zwischen polizeilicher Ermittlung und IT-Forensik problemlos möglich, da physisch vorhandene Datenträger sichergestellt und zu einem späteren Zeitpunkt durch fachkundiges Personal analysiert werden kann. Dies ist bei transienten digitalen Spuren nicht mehr möglich, diese erfordern nicht nur eine sofortige Sicherung, sondern des weiteren mitunter spezielle Hard- und Software direkt am Ort einer polizeilichen Maßnahme. Gleiches gilt für Remote- bzw. Online-Spuren. Ihre Sicherung ist nur über die zur Verfügung gestellte Ebene ihrer Abstraktion möglich, zusätzlich können sie jederzeit durch Dritte manipuliert oder gelöscht werden. Mit dem Grad ihrer Flüchtigkeit und insbesondere im Fall von Remote- bzw. Online-Spuren steigen die IT-fachlichen Anforderungen und die Herausforderungen für das polizeiliche Ermittlungspersonal. Gleichzeitig ist der Nachweis der Integrität einer digitalen Spur mit der Zunahme ihrer Flüchtigkeit von der fachlichen Qualifikation des Ermittlungspersonals und dessen verantwortungsvoller Arbeitsweise und lückenloser Dokumentation abhängig. Diese Umstand wiegt umso mehr, als dass neben klassischen IT-Systemen insbesondere mobile Endgeräte wie Smartphones und zunehmend Smart-Devices und das IoT Verbreitung gefunden haben. Jenseits klassischer IT-Systeme nimmt der Grad standardisierter Protokolle und Schnittstellen zur Sicherung von Daten nämlich rapide ab (vgl. N. Gärtner und Wallimann, 2020, S. 194 f.), während gleichzeitig die auf diesen Geräten verarbeiteten Daten zunehmend flüchtig, verschlüsselt oder gar remote in einer Cloud gespeichert werden.

Die Flüchtigkeit digitaler Spuren hat aber nicht nur Einfluss auf die erforderliche Kompetenz polizeilicher Ermittlungsarbeit. Die Einstufung digitaler Spuren nach ihrer Flüchtigkeitseigenschaft ist ebenso wichtig für die Reihenfolge ihrer Sicherung. Diese sog. „Order of Volatility“ (Brezinski und Killalea, 2002, S. 4) legt prinzipiell fest, dass fallbezogene digitale Spuren mit höherer Flüchtigkeit vor Spuren mit geringerer Flüchtigkeit gesichert werden sollen (vgl. Baier und S. Gärtner, 2019, S. 25). Im Bereich klassischer IT-Systeme sind das in erster Linie Arbeitsspeicherinhalte, Zugangs-Token für verschlüsselte Dateisysteme oder temporäre Betriebssystemdaten, gefolgt von Festplattenspeichern und Archivsystemen bzw. Datensicherungen (vgl. Casey, 2011, S. 389 ff.). Bevor also ein eingeschaltetes IT-System für eine spätere, durchaus anzustrebende Post-mortem-Analyse seiner Datenträger sichergestellt wird, ist es einer Live-Analyse zu unterziehen, da Informationen zu eventuell verschlüsselten Dateisystemen oder Zugangsinformationen bzgl. eines Cloud-Anbieters nach dem Abschalten nicht mehr identifiziert werden können. Angesichts einer unbegrenzten Zugriffsmöglichkeit und damit einhergehender Gefahr unbefugter Manipulation oder gar Zerstörung von Cloud-Daten sollten diese in der „Order of Volatility“ der Rangfolge flüchtiger Spuren gleichgesetzt werden. Das gleiche gilt für Smart-Devices bzw. Geräten aus dem Bereit des IoT, denn auch hier ist oftmals zu erwarten, dass nach einer Trennung der Stromversorgung die nur in flüchtigen Speichern abgelegten Daten verloren gehen.

Das Zusammenspiel digitaler Spuren und der polizeilichen Ermittlungsarbeit hat sich in einer digitalisierten Gesellschaft von einer IT-Forensik, welche Ereignisse reaktiv behandelt, hin zu digitalen Ermittlungen erweitert, in deren Umfeld sich Computersysteme und Datenstrukturen als weitaus komplexer im Gegensatz zu früheren (Offline-)Zeiten erweisen (vgl. Casey, 2018, S. 2). Gleichermaßen ist es in diesen komplexen Umgebungen schwierig bis unmöglich, digitale Spuren nach vordefinierten Standards zu gewinnen, wie es bei traditionellen und rein lokal funktionierenden Systemen der Fall ist. Vermehrt angewandte Verschlüsselung von Daten und kontinuierlich wachsende Datenmengen erhöhen die Komplexität und Verzögerung bei der Beschaffung digitaler Spuren um ein weiteres (vgl. Taylor u. a., 2010, S. 307).

3.6 Zwischenfazit

Basierend auf den erarbeiteten theoretischen Grundlagen zu den Besonderheiten, Eigenschaften und Kategorien digitaler Spuren lässt sich konstatieren, dass sich ihre Einbindung in den Kontext polizeilicher Ermittlungen grundlegend von den Handlungsroutinen der klassischen Kriminaltechnik unterscheidet, welche üblicherweise nicht direkt und aktiv in die Ermittlungshandlungen eingebunden ist. Deutlich erkennbar ist, dass der Sicherung und Analyse digitaler Spuren eine weiter wachsende Bedeutung zugeschrieben werden muss, denn sie nehmen innerhalb der (kriminal-)polizeilichen Ermittlungsarbeit eine zentrale Stellung ein. Hierbei stellen permanent neue Datenquellen und Technologien sowie stetig wachsende Datenmengen eine besondere Herausforderung dar. Dass sich gerade im Hinblick auf Remote- bzw. Online-Spuren keine Verstetigung der Methoden und Verfahren zur Sicherung und Auswertung andeutet, liegt einerseits daran, dass es sich um ein noch relativ junges und wenig bearbeitetes Forschungsfeld handelt (vgl. Pawlaszczyk, 2017, S. 113 f.) und andererseits, dass digitale Spuren durch eine äußerst dynamische Diversität gekennzeichnet sind. Dass sich konkrete Handlungsroutinen über Jahre festschreiben lassen und als Empfehlungen für polizeiliches Handeln etablieren, ist eher nicht zu erwarten, denn hierfür wandelt sich das technische Umfeld im Zuge der digitalen Transformation zu rasant.

Die Polizei steht deshalb vor besonderen Herausforderungen. Der Entwicklungs- und Wandlungsprozess im digitalen Bereich zwingt zu schnellen Reaktionen auf technische Neuerungen und erfordert Kreativität und Flexibilität im Vorgehen. Das bedeutet aber auch, dass eine gewisse Akzeptanz von fehlerbehaftetem Vorgehen[64] ausgebildet werden muss, da angesichts neuartiger Technologien und Phänomene nicht auf festgelegte und erprobte Methoden zurückgegriffen werden kann. Umso wichtiger ist es, neben den ohnehin schon unzähligen technischen Herausforderungen rechtliche Handlungssicherheit besonders im Zusammenhang mit vermeintlich transnationalen Zugriffen auf digitale Spuren zu schaffen. Unbestritten muss eine flexiblere internationale Zusammenarbeit jenseits von Rechtshilfeersuchen

[64] Fehlerbehaftetes Vorgehen bedeutet in diesem Fall die bewusste Gefahr, dass die Sicherung und Analyse digitaler Spuren gerade im Angesicht neuer, noch unbekannter Technologie, örtlicher Entgrenzung und zunehmender Verschlüsselung misslingen kann. Explizit ausgeklammert wird vorsätzlich risikoreiches oder fahrlässiges Handeln im Rahmen polizeilicher Ermittlungen.

und Cybercrime-Konvention geschaffen werden. Die hier in juristischen Kreisen intensiv geführte Diskussion zeigt aber, dass sich die Fachwelt dieser Problematik bewusst ist. Des Weiteren wurden in jüngster Zeit zahlreiche Gesetzgebungsvorhaben und internationale Abkommen auf den Weg gebracht bzw. bereits umgesetzt (vgl. Rückert, 2020, S. 22 ff.). Trotz alledem wird es das Straf(verfahrens)recht auch in Zukunft eher nicht schaffen, schon wegen der Langsamkeit demokratischer Willensbildungsprozesse mit der rasenden Geschwindigkeit der technischen Entwicklung Schritt zu halten (vgl. ebd., S. 16). Aber auch angesichts der gegenwärtigen Rechtslage sollte nicht der Weg des vorauseilenden Gehorsams gewählt werden, indem beispielsweise ein transnationaler Zugriff auf digitale Spuren kategorisch als unzulässig erklärt wird. Hier ist mehr Mut gefragt, sich auch als Ermittlungsbehörde in einer Grauzone zu bewegen und eventuell ein drohendes Beweisverwertungsverbot einem Komplettverlust digitaler Spuren vorzuziehen. Andernfalls besteht das Risiko, dass hieraus ein dauerhaftes Ungleichgewicht zum Nachteil der Ermittlungsbehörden entspringt.

4 Chancen und Herausforderungen digitaler Spuren

Die Polizei existiert nicht isoliert von gesellschaftlichen Entwicklungen und ist dadurch gezwungen, ihre Fähigkeit und ihr Handeln an den Bedürfnissen ihrer Zeit auszurichten. Das gilt insbesondere mit Blick auf die digitale Transformation der Lebens- und Arbeitswelt der gegenwärtigen Gesellschaft. Technik durchdringt das Berufs- und Privatleben vollends und birgt nicht nur neue Chancen und Perspektiven, sondern eben auch Risiken im Hinblick auf neue Möglichkeiten für Kriminelle. Durch eine weltweit vernetzte digitale Struktur können sie effektiver als je zuvor organisiert, arbeitsteilig und international agieren. Sich diesem Konflikt zu stellen ist für die Polizei eine unvermeidliche und dringliche Aufgabe.

Für klassische Delikte wie z. B. Erpressung werden womöglich die Forderungsschreiben anstatt in Papierform per E-Mail oder Messengerdienst verfasst, so dass ein physisches Schriftstück als Spurenträger oder das Schriftbild eines Täters nicht mehr zur Verfügung steht. Kriminelle telefonieren heutzutage nicht mehr von Festnetzanschlüssen aus, sondern kommunizieren über Mobiltelefone und dann zunehmend über verschlüsselte Messenger-Dienste, welche paketbasiert ihren Dienst verrichten und so für die klassische Telekommunikationsüberwachung nicht mehr fassbar sind (vgl. Fauth, 2015, S. 147 f.). Heimautomatisierung, Smart Devices sowie das IoT bieten aufgrund ihres geringen Ressourcenverbrauchs kaum Präventionsmaßnahmen gegen Angriffe, da diese die Rechenleistung und somit die Laufzeit verringern würden. Das alles bietet für Kriminelle neue Angriffsvektoren, die bei polizeilichen Ermittlungstätigkeiten zu berücksichtigen sind (vgl. Hoch, 2019, S. 636). Dies hat für die Strafverfolgung nicht nur beweiserhebliche Relevanz, sondern muss ebenfalls bei der Vorbereitung und Durchführung von Einsatzlagen Beachtung finden, um die Eigensicherung der Einsatzkräfte zu gewährleisten und Beweismittelverluste zu verhindern (vgl. ebd., S. 637 f.). Digitale Spuren offenbaren der polizeilichen Ermittlungsarbeit aber nicht nur die geschilderten Risiken, sondern sie ermöglichen auch völlig neue, kreative Einsatztaktiken und Beweismöglichkeiten. Dies bedarf aber nicht nur der Kompetenz einiger weniger IT-Spezialisten, sondern entsprechendes Spezialwissen im Hinblick auf digitale Spuren ist, selbstverständlich auf unterschiedlichen Niveaustufen,

in allen Bereichen der Ermittlungsarbeit gefragt, denn „[...] die überwiegende Masse der Straftaten, [...] die mit dieser Informationstechnologie begangen werden, wird nicht durch die genannten Spezialisten bearbeitet“ (Fauth, 2015, S. 150).

So wird in diesem Kapitel beleuchtet, wie digitale Spuren ihre Integration in die polizeilichen Ermittlungen erfahren sollten, und welche Qualifikationen und digitale Kompetenz hierfür seitens der Polizei erforderlich ist. Das Kapitel beantwortet des Weiteren die zweite Forschungsfrage dieser Arbeit, inwiefern die Polizei strukturell und personell den Herausforderungen digitaler Spuren gewachsen ist und setzt die Perspektive, welche weiteren Konsequenzen gezogen werden sollten und wie in Aus- und Fortbildung reagiert werden kann, damit die Polizei auf diesem zukunftsträchtigen Feld nicht den Anschluss verliert.

4.1 Integration digitaler Spuren in den Kontext polizeilicher Ermittlungshandlungen

„Bits und Bytes sind längst in sehr realer Form untrennbar mit unserem Alltag verwoben. Konsequenterweise sind digitale Spuren aus der kriminalistischen Arbeit nicht mehr wegzudenken. In naher Zukunft wird es kaum noch möglich sein, ‚digitale‘ Phänomenbereiche hinreichend abgrenzen zu können“ (Schneider, 2015, S. 20). In dieser Aussage von Schneider steckt nicht weniger als die Erkenntnis, dass digitales Spezialwissen und noch viel mehr vertiefte digitale Grundkompetenzen in allen Bereichen der polizeilichen Ermittlungsarbeit gefragt ist. Im Umkehrschluss und aus den Erkenntnissen des vorherigen Kapitels ist es ein Grundauftrag aller polizeilichen Ermittlungspersonen, über diese Kompetenzen zu verfügen und ihr Wissen auf einem aktuellen Stand zu halten. Letztendlich soll auch durch digitale Spuren die Beantwortung der folgenden Fragen unterstützt bzw. ermöglicht werden: Was ist geschehen? Wann, wo und wie ist es passiert? Wer hat es getan? Die durch die Polizei angewandten Methoden müssen hierfür allgemein akzeptiert und glaubwürdig sein. Sie müssen also in der Fachwelt beschrieben und anerkannt sein, ihre Funktionalität und Robustheit muss nachgewiesen werden können (vgl. BSI, 2011, S. 22 f.). Die digitale Forensik und somit auch die polizeiliche Ermittlungsarbeit kann für klassische Endgeräte wie PCs mit trennbaren Datenspeichern auf verschiedene bewährte Vorgehensmodelle zurückgreifen.

Ohne die einzelnen Modelle im Rahmen dieser Arbeit erörtern zu können, sei auf das in der Praxis häufig zu Grunde gelegte Staircase-Modell von Casey verwiesen (vgl. Casey, 2011, S. 192 f.), denn dieses schließt auch klassische polizeiliche Aufgaben wie die Tatortsicherung und Beschlagnahme ein und bildet den gesamten investigativen Prozess bis hin zur Präsentation vor Gericht ab. Aus diesem Grund hat sich dieses bereits aus dem Jahr 2004 stammende Vorgehensmodell im angelsächsischen Raum zu einem De-facto-Standard entwickelt (vgl. Dewald und F. C. Freiling, 2015, S. 157). In der Fachliteratur wird für die klassische IT-Forensik auf eine Vielzahl weiterer Vorgehensmodelle verwiesen (vgl. Pollitt, 2007, S. 44 ff.; Casey, 2011, S. 187 ff.; Dewald und F. C. Freiling, 2015, S. 151 ff.). Welches hierbei in der Praxis zum Einsatz kommt, spielt eine eher untergeordnete Rolle. Wichtig ist in jedem Fall, dass ein systematisches Prozessmodell verwendet wird, damit das Ergebnis einer Untersuchung wiederhol- und nachvollziehbar bleibt (vgl. Reiser, Rakotondravony und Köstler, 2017, S. 12).

Mit dem Wissen aus Kapitel 3 ist es insbesondere im Hinblick auf Remote- bzw. Online-Spuren oder im Bereich des IoT leider nicht immer möglich, auf erprobte und allgemein anerkannte Vorgehensweisen zurückzugreifen. Umso wichtiger ist es, dass gerade bei Anwendung neuer oder auch improvisierter Methoden die Integrität und Authentizität im Zusammenspiel mit einer lückenlosen Dokumentation die Glaubwürdigkeit der erlangten Spuren und Erkenntnisse gewährleistet und eine Verfälschung der Daten ausgeschlossen werden kann (vgl. BSI, 2011, S. 23). Durch die ubiquitäre globale Vernetzung wird die Ermittlungsarbeit zudem mit einer wachsenden Menge unstrukturierter und oftmals verschlüsselter Daten konfrontiert. Hierbei hat die Verlagerung von Daten in die Cloud unmittelbare Auswirkungen auf die investigativen Möglichkeiten, zugleich stellen die umfassenden Möglichkeiten von Verschlüsselung und Anonymisierung die Ermittlungen vor besondere Herausforderungen (vgl Ziercke, 2014, S. 15). Gleiches gilt für die Unmengen an Informationen, die sich aus der unüberschaubaren Vielzahl sozialer Netzwerke ergeben. Sie erlangen häufig im Zuge der Strafverfolgung polizeiliche Relevanz, nicht minder aber bei Entstehung von Gefährdungslagen. Diese haben ihren Ursprung vermehrt in der missbräuchlichen Nutzung der Möglichkeiten sozialer Netzwerke. Suizidankündigungen, Drohungen oder der öffentliche Aufruf zu Menschenansammlungen stellten die Polizei in jüngerer Vergangenheit vor nicht unerhebliche Probleme, wenngleich sich Daten und

Informationen aus öffentlich verfügbaren Quellen (OSINT[65]) zu einem leider noch unzureichend genutzten Ermittlungsinstrumentatrium hohen Wertpotentials entwickeln (vgl. Fauth, 2015, S. 153). „In bereits jetzt absehbarer Zukunft wird eine umfassendere polizeiliche Einsatzlage ohne Nutzung und parallel begleitende Auswertung sozialer Netzwerke nicht mehr vorstellbar sein. Auch für diese ganz spezielle Nutzung müssen Beamte hinsichtlich rechtlicher Grenzen und technischer Möglichkeiten ausgebildet sein“ (ebd., S. 153). Dass das Potential von digitalen Spuren aus öffentlich verfügbaren Quellen seitens der Polizei erkannt wurde, zeigt das Projekt SENTINEL[66], welches seinen Fokus zwar hauptsächlich auf die Gefahrenabwehr denn auf die Strafverfolgung legt, nichtsdestotrotz aber den Ermittlungswert von so gewonnen Spuren aufzeigt: Notrufe erzeugen ein hohes Informationsbedürfnis, jedoch werden OSINT-Quellen zur standardisierten Informationsbeschaffung durch die Polizei bislang kaum genutzt. Neben den Informationen von Notrufenden wird bisher hauptsächlich auf den Abgleich mit behördlichen Datenbeständen gesetzt. Im Projektrahmen von SENTINEL wurde das Informationsniveau dahingehend gesteigert, dass durch strukturierte Beschaffung von Informationen aus öffentlichen Quellen und deren Bewertung bereits vorhandene Erkenntnisse sinnvoll ergänzt und ein umfassenderes Bild von einer Situation gezeichnet werden kann (vgl. Ludewig und Epple, 2020, S. 457 f.). OSINT-Daten sind aufgrund ihrer Digitalität und uneingeschränkten Verfügbarkeit mühelos durchsuchbar und besitzen den Vorteil ihrer Aktualität (vgl. ebd., S. 458). Im Projekt wurden die OSINT-Recherchen im Zeitraum vom Eingang eines Notrufs bis zum Eintreffen der Einsatzkräfte am Einsatzort durch sog. „Intel-Officer“[67] an speziell ausgestatteten Arbeitsplätzen umgesetzt. Überwiegend handelte es sich hier um Anlässe wie Suizidandrohungen, Vermisstenfälle oder häusliche Gewalt (vgl. ebd., S. 459 f.). Im Ergebnis konnte dieses Projekt zeigen, dass OSINT-Recherchen trotz erfolgskritischer Hindernisse[68] in der Lage sind, das Informationsniveau zu verbessern, einen besseren Schutz der Ein-

65 siehe Fn. 61

66 In diesem durch die Stüllenberg Stiftung geförderten Pilotprojekt wurde die Hypothese erforscht, ob durch OSINT-Recherchen einsatzrelevante Informationen für Lagen des täglichen Dienstes erlangt werden können, um hierdurch einen besseren Schutz der Einsatzkräfte und eine professionellere Bewältigung der Aufgaben zu erreichen (vgl. DHPol, 2018)

67 Hierbei handelt es sich um speziell geschulte Einsatzbeamte, also keineswegs um IT-Spezialisten.

68 So mussten sich zunächst interne Abläufe einspielen, Strukturierungsprozesse ordnen und Anfangsschwierigkeiten überwunden werden (vgl. Ludewig und Epple, 2020, S. 461).

satzkräfte und der Bevölkerung zu gewährleisten sowie zu einer effektiveren Einsatzbewältigung beizutragen (vgl. Ludewig und Epple, 2020, S. 461).

In gleicher Weise wird das Thema IoT[69] die polizeiliche Ermittlungsarbeit in naher Zukunft ebenso ergreifen wie es durch mobile Endgeräte bereits vollzogen wurde. Wenngleich die Existenz bereits gestarteter Projekte und Partnerschaften das Bewusstsein für diese Problematik bestätigt (vgl. Hahn, 2017; Mundt, 2020; Eggert, 2019), so steht die Polizei an dieser Stelle erst am Anfang ganz besonderer Herausforderungen. Gegenwärtig sind keine forensischen Tools verfügbar, die in der Lage sind, Daten zuverlässig und automatisiert von IoT-Geräten zu gewinnen. Des Weiteren ist im allgemeinen unbekannt, welche Daten überhaupt vorhanden sind, welche anderen Geräte darauf zugreifen und ob Daten generell les- und zugreifbar sind (vgl. Watson und Dehghantanha, 2016, S. 5). IoT-Geräte sind keine vollwertigen Computer in traditioneller Form, sie besitzen aber genug Funktionalität um vernetzt zu sein, Befehle zu empfangen und Daten zu senden. Forensische Software wurde bislang vorrangig für traditionelle IT-Systeme geschaffen, selbst Tools für mobile Endgeräte wie Smartphones sind nur für diese spezielle Art von Embedded-Devices[70] konzipiert. Auf Datenspeicher von IoT-Geräten kann nicht mit traditionellen forensischen Methoden zugegriffen werden, die Daten können an verschiedenen Orten gespeichert sein und sind mit existierenden Tools weder les- noch auswertbar. Zusätzlich treten IoT-Geräte in einer Vielfalt in Erscheinung, wie man es von klassischen IT-Systemen bisher nicht gewohnt war. Von Wearables[71] und medizinischen Geräten über Sensornetzwerke und Drohnen bis hin zu Smart-Homes und Sicherheits- und Zutritts-Systemen wartet die IoT-Landschaft mit einem Feld oftmals völlig neuer und noch unbekannter Dinge auf (ebd., S. 6). Diesem werden sich die Ermittlungsbehörden und allem voran die Polizei stellen müssen, denn sie sind es, die in erster Instanz nach (strafrechtlich) relevanten Ereignissen die Ermittlungen führen und alle nach dem Stand von Wissenschaft und Technik geeigneten Beweismittel einzusetzen haben. Eine offene Frage kann u. a. sein, was passiert, wenn ein smartes, IoT-basiertes Sicherheitssystem miss-

69 siehe Fn. 7

70 Embedded Devices oder auch eingebettete Systeme bzw. Embedded Systems genannt sind energiesparende Computersysteme, bei denen Prozessoren und Controller mit ergänzender Elektronik wie Spannungsversorgung oder Sensoren in ein Gehäuse gefasst und für dedizierte Aufgaben eingesetzt werden. Wesentliches Abgrenzungsmerkmal zu klassischen IT-Systemen ist eine i. d. R. fehlende Mensch-Maschine-Schnittstelle (vgl. Asche, 2016, S. 1 f.).

71 Bei sog. Wearables handelt es sich um tragbare elektronische Geräte mit spezieller Funktion, wie z. B. Fitness-Armbänder oder Smartwatches.

braucht wurde, um sich Zutritt zu verschaffen oder die Ermittlungspersonen sich mit einer Vielzahl unbekannter Geräte konfrontiert sehen, von denen nicht klar ist, welche Funktion sie erfüllen und welche Art von Netzwerkkommunikation sie durchführen. In solchen Fällen werden zwangsläufig Antworten erwartet, welche Rolle bestimmte Geräte und Systeme im Zusammenhang mit einem Ereignis gespielt haben. Welche Auswirkungen digitale Spuren in ihren aktuellen Ausprägungen auf polizeiliche Standardmaßnahmen haben, wird im Folgenden beleuchtet.

4.1.1 Sicherungs- und Auswertungsangriff

Die Polizeidienstvorschrift (PDV) 100[72] definiert im Rahmen des ersten Angriffs den sog. Sicherungs- und den Auswertungsangriff, geht also davon aus, dass das polizeiliche Handeln hierbei in zwei Abschnitten abläuft. Der Sicherungsangriff ist weitestgehend von Sofortmaßnahmen geprägt, während dem Auswertungsangriff mehrheitlich die Aufnahme und Dokumentation eines Ereignisses innewohnt (vgl. Clages, 2019b, Rn. 31 f.). Hierbei muss oftmals unter Zeitdruck ein Gesamtüberblick hergestellt werden, um weitere Maßnahmen wie den Schutz und die Sicherung des Tatortes einzuleiten mit dem Ziel, vorhandene Spuren vor äußeren Einflüssen zu schützen und möglichst in ihrem Zustand zu bewahren (vgl. ebd., Rn. 50 ff.). Im nachgeordneten Auswertungsangriff erfolgt die Sicherung aller Spuren und darüber hinaus bereits ihre beginnende Auswertung (vgl. Zirk und Vordermaier, 1998, S. 52). Bereits im Rahmen dieser genannten Maßnahmen ist durch die polizeilichen Ermittlungskräfte ein besonderes Augenmerk auf den Umgang mit digitalen Spuren zu legen. Das sich immer weiter verbeitende Smart-Home sei als Beispiel genannt. So nutzen mittlerweile 4 von 10 Menschen in Deutschland Smart-Home-Anwendungen, fast 20% von ihnen im Bereich Sicherheit und Videoüberwachung. Über 50% der Nutzer steuern ihr Smart-Home per Sprachbefehl und fast 80% mittels Smartphone (vgl. Rohleder, 2020, S. 6 ff.). Diese Systeme kommunizieren miteinander und erzeugen permanent Daten. Die Existenz eines Smart-Home-Systems „[...] geht mit einer veränderten

[72] Die PDV 100 VS-NfD - „Führung und Einsatz der Polizei“ ist eine grundlegende Vorschrift über die Führung und den Einsatz der Polizei, orientiert sich stark an polizeilichen Einsatzanlässen und hat einen hohen Praxisbezug. Die PDV 100 legt den ersten Angriff begrifflich nicht fest, sondern benennt die zu ergreifenden Maßnahmen (vgl. Clages, 2019b, Rn. 1 f.).

Spurenlage einher, die von den Beamten vor Ort erkannt und korrekt gesichert werden muss“ (Tecklenborg und Stupperich, 2018, S. 204). Es sind also längst nicht mehr nur offensichtlich sicherzustellende PCs oder Datenträger an einem Ereignisort anzutreffen. Smart-Homes und IoT-Geräte können nicht nur wertvolle Informationen zu einem Ereignis liefern, sondern auch selbst Teil dessen sein, nämlich dann, wenn sich Täter einer neuen Generation mittels Laptop und ausnutzbarer Schwachstellen dieser Geräte Zutritt verschaffen, gänzlich ohne mechanische Beschädigungen. So sind umfangreiche Schulungsmaßnahmen aufgrund neuer Tatbegehungsweisen unumgänglich (vgl. ebd., S. 204), so dass die digitale Spurenlage beispielsweise bei Einbrüchen unter Ausnutzung von Schwachstellen im Smart-Home erkannt wird (vgl. ebd., S. 206). Betrachtet man die Tatsache, dass der Sicherungsangriff im überwiegenden Teil von Angehörigen der Schutzpolizei durchgeführt wird (vgl. Zirk und Vordermaier, 1998, S. 49), wird die Notwendigkeit für die Polizei, das Bewusstsein für digitale Spuren in der Breite zu vermitteln, umso deutlicher.

Infolge der technischen Weiterentwicklung spielt die digitale Spurenlage selbst bei Verkehrsunfällen eine zunehmend wichtige Rolle. In modernen Fahrzeugen ist heutzutage eine hohe Menge an Daten aus Navigation, Entertainment, Mobilfunktechnik sowie Fahrzeugsensorik zu finden (vgl. Grabowski, 2018, S. 208). Und auch hier liegt es in der Verantwortung der Polizei, „... dass möglichst alle Spuren und Beweismittel erkannt, dokumentiert und fachkundig gesichert werden, damit sie für die anschliessende [sic!] Auswertung zur Verfügung stehen“ (Arnold, 2015, S. 743). Leider gilt auch im Bereich der Fahrzeug-Forensik, dass für das Auslesen von Daten derzeit kein standardisiertes Verfahren zur Verfügung steht, da es sich bei Fahrzeugen um herstellerspezifische und hochkomplexe Systeme handelt. Die Datenerhebung ist oftmals einzelfallabhängig und mitunter aufwändig und mühselig (vgl. Brummer und Hoch, 2017, S. 647). Hinzu kommt, dass nicht nur auf den Fahrzeugen selbst Daten gespeichert werden. Neben reichlichen Online-Funktionalitäten bieten Fahrzeughersteller ihren Kunden eine Vielzahl an Service- und Zusatzdienstleistungen wie automatische Fahrtenbuchservices oder spezielle Notrufsysteme an (vgl. Grabowski, 2018, S. 209 ff.). Folglich hat der erste Angriff auch im Zusammenhang mit Kraftfahrzeugen eine gewichtige Bedeutung. Es muss sichergestellt werden, dass Aktivierungen und mögliche Datenveränderungen auf den im Fahrzeug befindlichen Systemen unterbleiben. So kann das Einschalten von Navigationssystemen zur Ermittlung der letzten Wegstrecke spätere Ergebnisse der Untersuchung

negativ beeinflussen. Folglich sollte gelten, dass in Abhängigkeit vom zu untersuchenden Ereignis die Auffindesituation weitestgehend unverändert bleibt und weitere Schritte in Ermangelung technischer Möglichkeiten vor Ort mit Spezialdienststellen abzustimmen sind. Hinsichtlich der erwähnten Online-Funktionalitäten ist besonders in Zukunft zu erwarten, dass Anfragen bei den Fahrzeugherstellern potentiell beweiserhebliche Informationen aus den von ihnen gespeicherten Daten liefern (vgl. Grabowski, 2018, S. 2010).

Aus polizeilicher Sicht ist es wichtig festzustellen, dass Beteiligte des ersten Angriffs ein Bewusstsein über die Möglichkeiten des Vorhandenseins digitaler Spuren besitzen müssen. In Anbetracht des Umstandes, dass eben nicht Spezialisten die Phase des Sicherungsangriffs durchführen oder an Verkehrsunfallorten zugegen sind, sondern in der Mehrheit Angehörige der Schutzpolizei, gilt es, die Thematik der digitalen Spuren fest in die gesamte Aus- und Fortbildung der Polizei zu integrieren, um später vor Ort einen Zugewinn an Handlungssicherheit zu erreichen sowie die Ermittlungs- und Kontrollkompetenz zu steigern (vgl. Brummer und Hoch, 2017, S. 647). Hierbei geht es vorrangig um die Erkennung einer möglichen digitalen Spurenlage und die notwendigen Handlungen, diese bestmöglich vor versehentlicher bzw. vorsätzlicher Manipulation oder gar Zerstörung zu schützen.

4.1.2 Durchsuchung

Eine im Ermittlungsalltag alltägliche kriminaltaktische Ermittlungsmethode ist die Durchsuchung. Ihr Zweck besteht in der Suche bzw. dem Auffinden von Personen, Sachen, Spuren und anderen Beweisgegenständen auf Grundlage der StPO[73] bzw. der Polizeigesetze zur Gefahrenabwehr von Bund und Ländern (vgl. Ackermann, 2019a, Rn. 1). Wesentliche Kernpunkte der Durchsuchung in ermittlungstaktischer Hinsicht sind ihre Planung und Vorbereitung (vgl. ebd., Rn. 13 ff.) sowie schlussendlich ihre Durchführung (vgl. ebd., Rn. 47 ff.). Die Vorbereitung einer Durchsuchung inkludiert u. a. eine je nach Sachlage möglichst gründliche Personen- und Sachaufklärung (vgl. ebd., Rn. 19). Neben Erkenntnissen aus den einschlägigen polizeilichen Informationssystemen (vgl. ebd., Rn. 21) sind es vor allem OSINT-Recherchen[74], die

[73] Die §§ 102 ff. StPO gestatten eine Einschränkung der Grundrechte nach Art 2, 3 GG durch diese offene Ermittlungsmaßnahme, wobei Beschuldigte die Durchsuchung in weiterem Maße dulden müssen als Unverdächtige (§ 103 StPO) (vgl. Meyer-Goßner und Schmitt, 2018, § 102 Rn. 1)

[74] siehe Abschnitt 4.1

ergänzende und zumeist aktuellere Informationen zu Personen und Objekten wie Wohnungen oder Firmensitzen liefern. Des Weiteren ist schon bei der Planung einer Durchsuchung zu berücksichtigen, welche Systeme, Datenträger und Kommunikationsmittel wie Smartphones vor einem Zugriff geschützt werden müssen, damit Daten und somit digitale Spuren nicht vorsätzlich und unwiderruflich zerstört werden können (vgl. Fauth, 2015, S. 150). Aber die technischen Möglichkeiten bieten auch neue taktische Einsatzszenarien, über welche vernetzte IT-Systeme durch die Polizei in der Vorbereitungsphase von Durchsuchungen zielgerichtet eingesetzt werden können. So könnten Smart-Speaker zur Audio-Überwachung, Smart-Watches zur GPS-Ortung eingesetzt oder die Kontrollfunktionen von Smart-Cars manipuliert werden, wobei eine rechtliche Zulässigkeit nicht gegeben bzw. äußerst fragwürdig sein dürfte (vgl. Hoch, 2019, S. 639).

Eine absolut realistische Einsatzmöglichkeit digitaler Spuren in der Phase der Vorabaufklärung von Durchsuchungen ist die Nutzung von Metadaten vorhandener WiFi-Netze[75] an Durchsuchungsorten. Kommunikationsdaten von Funknetzen sind je nach individueller Reichweite uneingeschränkt empfangbar[76], und sie enthalten im Fall des WiFi-Standards verschlüsselte Inhalts- und unverschlüsselte Meta-Daten[77]. So lassen sich ohne Weiteres die an einem bestimmten Ort in Reichweite befindlichen WiFi-Netzwerke mitsamt ihren Clients ermitteln. Die Erfassung dieser Metadaten liefert für die Vorbereitung einer Durchsuchung wichtige Informationen und kann bei Durchführung derselben eine entscheidende Rolle spielen[78]. Eine tiefgreifende Betrachtung der verschiedenen Möglichkeiten (vgl. Davidoff und Ham, 2012, S. 224 ff.) ist im Rahmen dieser Arbeit nicht möglich, unstrittig ist aber, dass digitale Spuren

75 siehe Abschnitt 3.4.3

76 Die Ausbreitung von Funkwellen ist nicht an ein Trägermedium gebunden, mit zunehmender Entfernung und durch Hindernisse nimmt ihre Signalstärke aber ab.

77 Der Aufbau einer verschlüsselten Verbindung, vereinfacht dargestellt die erste Kontaktaufnahme eines WiFi-Clients zu einem Access-Point erfolgt technisch bedingt generell unverschlüsselt. Auch senden Access-Points zyklisch Pakete mit Informationen ihrer Existenz ins Netz, WiFi-Clients prüfen unaufhörlich, ob sich bekannte Netzwerke in ihrer Reichweite befinden. Der WiFi-Standard enthält eine Vielzahl solch unverschlüsselter Meta-Pakete, die technischen Details sind für diese Arbeit eher von untergeordneter Wichtigkeit.

78 So verhinderte zu Beginn einer Durchsuchungsmaßnahme, bei welcher der Autor zugegen war, der Tatverdächtige mittels des Rufes „Alexa! Strom aus!“ die Sicherung digitaler Spuren auf seinem in Betrieb befindlichen, mehrfach verschlüsselten IT-System. Im Nachhinein wäre eine Verhinderung dieser Handlung möglich gewesen, wenn bei der Vorbereitung der Durchsuchung eine Aufklärung des WiFi-Netzes und während der Durchsuchungsmaßnahme eine gezielte Trennung des Alexa-Smart-Speakers durch das Versenden entsprechend konfigurierter WiFi-Pakete durch die Einsatzkräfte erfolgt wäre.

trotz neuer Chancen sogleich erhebliche Einsatzrisiken bergen, denn neben einer plötzlichen Stromabschaltung oder dem Löschen von Daten stellt beispielsweise die Aktivierung von Polizeifallen ein erhebliches Gefahrenpotential dar(vgl. Hoch, 2019, S. 637 f.).

Während der Durchführung von Durchsuchungen stellt eine wachsende Menge an unterschiedlichen digitalen Spuren hohe Anforderungen an die Kompetenz der jeweiligen Ermittlungspersonen. Die Sicherstellung einer digitalen Spurenlage klassischer IT-Systeme hat sich seit langem in der polizeilichen Ermittlungsarbeit etabliert. Diese beschränkt sich grob umschrieben in der Erkennung von PCs, Datenträgern und mobiler Endgeräte sowie der anschließenden Übergabe an die IT-Forensik, welche die Suche nach digitalen Spuren mittels Post-mortem-Analyse[79] durchführt und die Ergebnisse für weitere Ermittlungen aufbereitet. Wie aber bereits erkannt wurde, hat sich das Feld digitaler Spuren in den letzten Jahren in seiner Vielfalt und dem Umfang seines Auftretens äußerst dynamisch entwickelt. Durchsuchungen ohne entsprechende aktuelle Kenntnisse und Fähigkeiten zur Umsetzung verschiedener Sicherungsmöglichkeiten vor Ort laufen Gefahr, eine Vielzahl solcher Spuren zu übersehen bzw. nicht vor ihrer Zerstörung zu bewahren. So ermöglicht beispielsweise vorhandenes Fachwissen zu Kryptowährungen den Ermittelnden, ihr „... Augenmerk auf Spuren zu richten, die auf Wallets, Backups oder Wiederherstellungshinweise von Kryptowährungen hindeuten“ (Eugster, 2018, S. 43). Dies sollte bereits am Durchsuchungsort geschehen, denn zum einen ist der direkte Zugriff auf geschützte Zugänge zu Wallets und Krypto-Exchangern[80] oftmals über die IT-Systeme vor Ort möglich, zum anderen muss verhindert werden, dass Vermögenswerte durch die Betroffenen nach Abschluss der Maßnahme verschoben werden. Hinsichtlich Kryptowährungen muss der Polizei folglich eine Sicherstellung möglich sein. Aufgrund ihrer Virtualität kann man sie weder in ein Couvert verstauen noch in einem Tresor verwahren. Vermögenswerte in Krypto-Währung müssen also zwingend auf ein polizeiliches oder staatsanwaltschaftliches Wallet verschoben werden[81] (vgl. ebd., S. 44). Demzufolge müssen seitens der Ermittlungsbe-

79 siehe Abschnitt 3.4.1

80 Ein Krypto-Exchanger, oftmals auch Krypto-Börse genannt, ist ein Anbieter, der es ermöglicht, reale Geldbeträge in verschiedene Kryptowährungen zu tauschen. Sie sind neben dem sog. Schürfen ein Weg, um Beträge von Kryptowährungen zu erzeugen. Ein bekannter Krypto-Exchanger in Deutschland ist die Firma Bitcoin Group SE (*bitcoin.de*).

81 Entgegen vieler Erfolgsmeldungen zu erfolgreichen Maßnahmen der Strafverfolgungsbehörden (vgl. Metropolnews, 2020) ist der polizeiliche Alltag diesbezüglich noch von vielen Unzulänglichkeiten gekennzeichnet. So konnten während einer

hörden die personell-fachlichen und technischen Voraussetzungen gegeben sein, um digitale Spuren zu Krypto-Währungen identifizieren und sicherstellen zu können.

Regelmäßig erstrecken sich Durchsuchungsmaßnahmen auch auf Fahrzeuge. Ging es bisher vorrangig um das Auffinden von Gegenständen und anderen (analogen) Beweismitteln, so wird der Fokus neben IT-Geräten in Wohn- und Geschäftsräumen in Zukunft zusätzlich auf gespeicherten Daten eines jeweiligen Fahrzeugs liegen. Wie im vorherigen Abschnitt bereits festgestellt, sind verschiedene Dienste wie Fahrtenbuchservices oder verbundene Geräte ermittlungsrelevant. Trackpoints, gefahrene Geschwindigkeiten und weitere Events ermöglichen die Erstellung von Bewegungsprofilen oder liefern einen Hinweis auf die Anzahl mitgefahrener Personen, so dass sich mitunter Erkenntnisse im Zuge von Ermittlungen zu begangenen Straftaten gewinnen lassen (vgl. Grabowski, 2018, S. 210). Umso wichtiger ist es dann auch, nicht nur die Datenbasis der Fahrzeuge selbst im Blick zu haben, sondern zu erkennen, dass Hersteller von Fahrzeugen und Anbieter von Zusatzdiensten potentiell über weitere ermittlungsrelevante Daten verfügen können. Das Bewusstsein hierüber und die entsprechende Fachkompetenz ist für die polizeiliche Ermittlungsarbeit unverzichtbar, um notwendige Eingriffsmaßnahmen einerseits anzuregen, diese andererseits auch umsetzen zu können (vgl. ebd., S. 214).

So lässt sich als weitere Erkenntnis festhalten, dass im Rahmen der Vorbereitung und Durchführung von Durchsuchungen ein reines Bewusstsein für das Auftreten und die Vielfalt digitaler Spurenlagen nicht ausreicht. Entsprechende Fachkompetenz zur konkreten Umsetzung entsprechender Maßnahmen und eine aktuelle technische Ausstattung sind hierfür unabdingbar. Ohne bereits an dieser Stelle reflektierend auf die gegenwärtige Sachlage innerhalb der Polizei einzugehen, sind die aktuellen und zukünftigen Herausforderungen nicht zu übersehen.

Durchsuchung, bei welcher der Autor zugegen war, keine Vermögenswerte in Bitcoin gesichert werden, weil sich weder die Polizei noch die Staatsanwaltschaft verwaltungsrechtlich in der Lage sah, entsprechende Wallets zur Sicherstellung anzulegen.

4.1.3 Von der digitalen Spur zur digitalen Ermittlung

Die Kategorie der Remote- und Onlinespuren lies bereits erkennen, dass digitale Spuren außerhalb isolierter und für sich autark agierender IT-Systeme mehr sind als direkte Antworten auf eindeutige und geschlossene Fragen der polizeilichen Ermittlungen zu einem Ereignis. So haben sich insbesondere Smartphones zu einer riesigen Fundgrube für digitale Beweise entwickelt, aus denen sich Aufenthaltsorte, Kontakte, Browserverläufe oder Nachrichten verschiedenster Kommunikationsplattformen extrahieren lassen (Ghermann und Neumann, 2019, S. 536). Digitale Spuren unterschiedlichster Quellen sind mittlerweile Fußabdrücke, über welche Kausalzusammenhänge erkannt werden können, wenn man sie zueinander in Beziehung setzt. Sie haben sich zu einer Art von Daten entwickelt, „[...] die sozial bedeutungsvoll werden, weil diese eine technologisch basierte Konstruktion sind, bei der ein bestimmter Akteur oder ein bestimmtes Akteurshandeln oder ein durch Akteure entwickelter Algorithmus Bezugspunkt der Konstruktion sind“ (Breiter und Hepp, 2018, S. 29 f.). Die Herausforderung dieser vielen unterschiedlichen Spuren ist es also, Zusammenhänge und Beziehungen jenseits einfacher Aggregation und Korrelation aufzudecken, so dass sie im sozialen Sinn bedeutungsvoll werden und für anspruchsvollere Erklärungen und Verfahren der Theoriebildung nutzbar sind (vgl. ebd., S. 33 f.). Und so müssen neben zu sichernden Informationen auf Geräten immer mehr Spuren im Internet, beispielsweise aus sozialen Netzen verfolgt, gesichert und analysiert werden (Pawlaszczyk, 2017, S. 113). Jaquet-Chiffelle differenziert gar zwischen forensischen IT-Ermittlungen erster Generation und digitalen Ermittlungen der zweiten Generation, welche neben physischen Medien die um sich greifende Virtualisierung von Daten und Kommunikation umfasst (vgl. Jaquet-Chiffelle, 2014, S. 189 f.). Ähnlich postulieren es Dewald und Freiling: Sie unterscheiden zwischen *forensic computing* und *digital investigation* (vgl. Dewald und F. C. Freiling, 2014, S. 4). Während *forensic computing* den traditionellen Teil der IT-Forensik umfasst, so untersuchen digitale Ermittlungen (*digital investigation*) Fragen zu digitalen Spuren in Verbindung mit kriminalistischen Kenntnissen und Fähigkeiten. Personen, die digitale Ermittlungen durchführen, verfügen zwar über tiefgreifende IT-Kenntnisse, das Wissen eines IT-Forensikers ist aber nicht notwendig, so dass diese Art Ermittlungen durchaus von speziell trainierten Polizeibeamten durchgeführt werden können (vgl. ebd., S. 7). Am Beispiel von Ermittlungen im Umfeld der Kryptowährung *Bitcoin* lässt sich dies gut veranschaulichen. So werden bei der forensischen Untersuchung

eines Datenträgers Spuren zu Bitcoin-Adressen gefunden. Die Arbeit des klassischen IT-Forensikers ist getan, nur erzeugt diese Spur im ersten Schritt keinen Mehrwert, denn es handelt sich lediglich um eine kryptische Adresse ohne Bezug zu irgendetwas. Jedoch ist die Bitcoin-Blockchain[82] wie ein Kontoauszug aller jemals getätigten Transaktionen und für jedermann ohne die Notwendigkeit eines Auskunftsersuchens einsehbar, wobei Sender und Empfänger jedoch nur über ihre jeweilige anonyme Bitcoin-Adresse bekannt sind. Durch die Verfolgung entsprechender Transaktionen in der Bitcoin-Blockchain ist mitunter eine Deanonymisierung der Transaktion über den Tausch in echte Währung, dem sog. Exchanging[83] möglich (vgl. Schulze und Pawlaszczyk, 2018, S. 31). Ein weiteres Beispiel sind Ermittlungen im Bereich krimineller Internetplattformen, wo Pseudonyme, E-Mail-Adressen, Profilbilder oder vergessene Metadaten in Dateien u. U. Verbindungen zu Personen herstellen lassen. Die Polizei muss in der Lage sein, solche Kompetenzen zur Führung digitaler Ermittlungen auszubilden und diese in der gesamten Breite der Aus- und Fortbildung nachhaltig zu vermitteln.

4.1.4 Einbindung externer Dienstleister

Die Inanspruchnahme externer Hilfe aus der Privatwirtschaft mangels eigenen Sachverstands erfreut sich seitens der Strafverfolgungsbehörden einer wachsenden Beliebtheit (vgl. Braun und Roggenkamp, 2012, S. 141). Die Gründe hierfür sind vielfältig. Bedingen personelle Ressourcen seitens Polizei und Staatsanwaltschaft eine endliche Kapazität, so stehen oftmals mangelnder Sachverstand und fehlende Ausrüstung einer kompetenten, technisch gestützten Ermittlung im Weg. Dort, wo die Sicherstellung und anschließende Sichtung, Analyse und Auswertung großer Datenmengen schnell die Grenzen personeller und technischer Ressourcen ausschöpft, wird zur Lösung dieses Dilemmas vermehrt dazu übergegangen, Unterstützung privater Dienstleister auf dem Weg der Sachverständigenbestellung in Anspruch zu nehmen (vgl. Wackernagel und Graßie, 2021, S. 12). Zurückgegriffen wird durch Richter und insbesondere Staatsanwaltschaften hierbei auf die §§ 72 ff.,

[82] Die Bitcoin-Blockchain ist grob umschrieben eine Datenbank, in der alle jemals durchgeführten Transaktionen gespeichert sind. Sie stellt also eine Art öffentliches Buchungssystem dar, in welchem jede Zahlung vermerkt ist (vgl. Pawlaszczyk, 2017, S. 158 f.).

[83] siehe Fn. 80

161a Abs. 1 S. 2 StPO. In dieser Eingrenzung ergeben sich für den Sachverständigen die folgenden vier Tätigkeitsfelder, wobei es immer um die Übermittlung und/oder Anwendung der jeweiligen Sache geht: Die Verrichtung einer speziellen Tätigkeit, die Tatsachenbekundung, die Vermittlung von Erfahrungswissen sowie die Gutachtenerstattung (vgl. Meyer-Goßner und Schmitt, 2018, Vor § 72 Rn. 3 ff.). Wackernagel und Graßie kritisieren, dass in dieser Form vermehrt die Beauftragung externer Dienstleister unter dem Deckmantel der Sachverständigentätigkeit erfolgt, obwohl es sich eigentlich um ein Outsourcing genuiner Ermittlungstätigkeit handelt (vgl. Wackernagel und Graßie, 2021, S. 13). Voraussetzung ist für sie, „[...] dass seitens des Sachverständigen auf besondere Erfahrungssätze und Fachwissen zurückgegriffen wird, die in dieser Form bei den Ermittlungsbehörden bzw. dem Gericht nicht vorhanden sind“ (vgl. Wackernagel und Graßie, 2021, S. 13; Meyer-Goßner und Schmitt, 2018, Vor § 72 Rn. 1). Wird aber beispielsweise die Auswertung eines Datenträgers in Bezug auf Kommunikationsdaten durch einen externen Dienstleister vorgenommen, so handle es sich nicht um die Bereitstellung besonderer Sachkunde, sondern um eine organisatorische bzw. technische Dienstleistung, die keine besondere Sachkunde erfordere, jedoch oftmals mit wertenden Initiativen verbunden sei (vgl. Wackernagel und Graßie, 2021, S. 14 f.). Gleichlautend formuliert es Wenzel. Den Staatsanwaltschaften stehe es zwar in ihrem Ermessen, Hilfsorgane für Ermittlungstätigkeiten hinzuzuziehen. Zwingende Voraussetzung sei aber, dass diesen Hilfsorganen gesetzliche Ermächtigungsnormen zur Seite stünden, die Ermittlungsgeneralklausel des § 161 Abs. 1 S. 1 StPO jedoch auf die Strafverfolgungsbehörden wie beispielsweise die Polizei beschränkt sei (vgl. Wenzel, 2016, S. 86). „Eine Übertragung der Ermittlungsbefugnis auf private Dritte wie Unternehmen oder gewerbliche Dienstleister sei nicht möglich, denn eine Auslagerung von Tätigkeiten wie das Suchen, technische Aufbereiten, Sichten und Katalogisieren von Daten durch private Dritte bzw. IT-Dienstleister wären im Rahmen dieser Ermittlungsgeneralklausel rechtlich nicht zulässig“ (ebd., S. 86). Nicht zuletzt auch, weil die Bürger auf die unabhängige hoheitliche Tätigkeit staatlicher Strafverfolgung vertrauen (vgl. Wackernagel und Graßie, 2021, S. 18), distanzieren sich Wackernagel und Graßie von dem Trend, „[...] dass Ermittlungsbehörden sich aufgrund personeller und technischer Engpässe ihrer originären, staatlich zugewiesenen Pflichten entledigen und diese an private Dienstleister abtreten. Die Strafrechtspflege war und ist das Monopol des Staates, für welches dieser die erforderlichen Ressourcen bereitzustellen hat“ (ebd., S. 18).

4.1.5 Zwischenfazit

Die Integration digitaler Spuren in die polizeiliche Ermittlungsarbeit ist von vielen Herausforderungen gekennzeichnet. Relativ unproblematisch, gut in den Kontext der Ermittlungshandlungen eingebunden und in der Vorgehensweise etabliert ist der Umgang mit digitalen Spuren nach außen abgeschlossener und für sich autark arbeitender IT-Systeme. Diese werden durch eine eigenständige IT-Forensik bearbeitet, dies entspricht der Vorgehensweise der klassischen Kriminaltechnik. Allerdings hat sich die digitale Spurenlage in den letzten Jahren rasant fortentwickelt. Vor allem durch einen uneingeschränkten Internetzugriff und die Online-Fähigkeit selbst kleinster Smart-Devices ist die digitale Lebens- und Arbeitswelt allumfassend vernetzt. Daten finden sich nicht nur auf den jeweiligen Geräten, sondern auch an oftmals unbekannten Orten im Internet, auf Cloud-Speichern oder bei Anbietern selbst. Die Polizei muss in ihrer gesamten Handlungsbreite über das Bewusstsein für die Vielfalt des Auftretens digitaler Spuren verfügen. Dies reicht aber gerade für kriminalpolizeiliche Ermittlungen nicht mehr aus. Wie der Abschnitt zu Durchsuchungen zeigte, ist deliktsübergreifend ein sehr gut ausgeprägtes IT-Knowhow unverzichtbar, denn zunehmend erfordern digitale Spuren sofortige qualifizierte Sicherungsmaßnahmen, so dass bei Durchsuchungen und u. U. auch im Rahmen des ersten Angriffs auf Personal mit tiefgreifenden IT-Spezialkenntnissen und entsprechender technischer Ausstattung nicht verzichtet werden sollte. Anschließende digitale Ermittlungen zur Gewinnung weiterer Erkenntnisse und Zusammenhänge sind zunehmend unabdingbar, damit digitale Spuren ihren vollen Beweiswert entfalten können. Auch verlagert sich die Ermittlungsarbeit weg von der Straße hinein ins Internet zu verschiedensten Plattformen, sozialen Netzwerken und kriminellen bzw. legalen Vertriebskanälen. Hier helfen der Polizei keine externen Dienstleister, zudem ist das Outsourcen spezieller Tätigkeiten zur Einsparung von Kosten oder zur Reduzierung eigener personeller und struktureller Belastungen nicht zulässig ist (vgl. Wackernagel und Graßie, 2021, S. 16; Wenzel, 2016, S. 86). Unbestritten werden Ermittlungsmaßnahmen durch die technische Weiterentwicklung immer anspruchsvoller, umso stärker sind jedoch die Strafverfolgungsbehörden gefordert, sich dieser Entwicklung durch zeitgemäße Handlungskompetenz zu stellen.

4.2 Erforderliche Qualifikationen und digitale Kompetenz

Die Arbeit konnte bisher aufzeigen, dass technisches Wissen heute für die Polizeiarbeit unabdingbar und äußerst wichtig ist. Wenn ein Team von Polizisten an einem Ereignis- oder Durchsuchungsort eintrifft, muss es in der Lage sein zu erkennen, ob es eine smarte Uhr oder eine Kamera gibt und ob Haushaltsgeräte internetfähig sind, da sich digitale Spuren dieser Objekte als nützlich erweisen könnten. Das Team muss wissen, welche Beweise am Tatort gefunden werden können und welche Rolle sie bei der Untersuchung des Verbrechens spielen (vgl. F. Freiling, 2020, S. 4). Die folgenden Abschnitte beleuchten nach einer kurzen Begriffsklärung, welche Qualifikationen und Kompetenzen seitens der Polizei vorhanden sein bzw. ausgebildet werden müssen, um sich den Herausforderungen digitaler Spuren zu stellen und die aus ihnen hervorgehenden neuen Ermittlungsmöglichkeiten zu nutzen.

4.2.1 Kompetenzbegriff

Mitunter werden die Begriffe *Kompetenz* und *Qualifikation* in der Diskussion um grundlegende berufliche und soziale Fähigkeiten nicht deutlich voneinander abgetrennt oder gar vermengt. Die Kompetenzforschung nimmt ein zwar relativ junges Feld der Sozialforschung ein (vgl. Kunze, 2018, S. 170), aber der Begriff lässt sich deutlich von dem der Qualifikation abgrenzen. So sehen Hechenleiter und Schwarzkopf im Begriff der Qualifikation die „[...] konkrete, personenunabhängige Befähigung bzw. Eignung [...], eine Tätigkeit regelmäßig auf einem bestimmten Niveau ausführen zu können“ (Hechenleitner und Schwarzkopf, 2006, S. 1). Dies wird häufig auch als Nachweis der Befähigung und somit als Berechtigung zu einem bestimmten Tun angesehen (vgl. ebd., S. 2). Alsonso wiederum bezieht sich auf Heyse (vgl. Heyse, 2014) und konstatiert, „[...] dass Qualifikationen häufig für die adäquate Bewältigung von offenen, komplexen Arbeitskontexten nicht ausreichen, da in solchen Situationen kein vorgefertigter Weg zum Ziel führt, sondern unterschiedliche Kompetenzen zur kreativen Lösungsfindung benötigt werden“ (Alonso, 2019, S. 330). Folgt man dieser Auffassung im Wissen um die Vielseitigkeit und Dynamik digitaler Spuren, so spiegelt sich in erster Linie die Frage wider, wie solche Kompetenzen zu definieren sind. Frank sieht in der Kompetenz

einer Person „[. . .] ihre Möglichkeit zum selbstverantwortlichen und selbstorganisierten Handeln in konkreter Situation zum Erreichen einer erwarteten Wirkung in einem jeweils definierten Kontext“ (Frank, 2019, S. 319). Und auch Kunze versteht in Anlehnung an Weinert (vgl. Weinert, 2002) unter Kompetenz verfügbare bzw. erlernbare kognitive Fähigkeiten und Fertigkeiten zur Lösung bestimmter Probleme sowie die Möglichkeit, diese Fähigkeiten in variablen Situationen erfolgreich nutzen zu können (vgl. Kunze, 2018, S. 170). Er erweitert dieses Verständnis um die Definition von Rosenstiel (vgl. Rosenstiel, 2004), dass Kompetenzen auf die eigenverantwortliche Bewältigung von komplexen und unüberschaubaren Aufgaben ausgerichtet sind (Kunze, 2018, S. 170 ff.). In Bezug auf digitale Spuren ist es somit vordergründig die digitale Kompetenz, die es ermöglicht, auf die Dynamik sich ständig wandelnder und in der Vielfalt wachsender digitaler Spurenlagen adäquat zu reagieren, da Qualifikation im Kontext dieses Verständnisses eher auf die Anwendung mehr oder weniger vorgefertigter Handlungsroutinen abstellt. Wer also seine Kompetenzen kennt und seine Profession beherrscht, bewegt sich sicher in veränderten Umgebungen (vgl. Frank, 2019, S. 319). Hinsichtlich digitaler Kompetenz werden mitunter die sog. *Digital Natives*[84] ins Spiel gebracht. Hierzu sei abschließend angemerkt, dass Digital Natives nicht automatisch digitale Kompetenz innewohnt. Die besitzen zwar ein umfassendes Verständnis der Möglichkeiten von Anwendungen, oftmals aber nicht über die Auswirkungen von ausgeführten Interaktionen im digitalen Raum (vgl. Zink, Zimmermann und Müller-Dofel, 2020, S. 49).

4.2.2 Digital-Forensik und Digitale Ermittlungen

Die in dieser Arbeit voneinander abgegrenzten Handlungsfelder der IT-Forensik und der digitalen Ermittlungen stellen ganz unterschiedliche Anforderungen an die IT-fachliche Kompetenz. Die klassische IT-Forensik verfügt weitestgehend über anerkannte Verfahren und kann auf bewährte Schnittstellen zurückgreifen und auch die Mobilfunk-Forensik ist in gewisser Weise durch die Nutzung

[84] Als Digital Natives wird die Generation von Menschen bezeichnet, welche ins digitale Zeitalter nach 1980 hinein geboren wurde und in ihm aufgewachsen ist. Unterschieden wird diese Generation von den sog. *Digital Immigrants*, welche mit der Digitalisierung erst im Laufe ihrer späteren persönlichen Entwicklung konfrontiert wurden (vgl. Wang, Myers und Sundaram, 2013, S. 409). Den Digital Natives wird oftmals ein geschickterer Umgang mit digitalen Technologien nachgesagt, was durch Studien bisher nicht gelegt werden konnte. Vielmehr wird dies durch psychologische, organisatorische und soziale Faktoren als allein durch das Lebensalter bestimmt (vgl. ebd., S. 416).

verschiedener Software-Lösungen[85] für Standard-Auswertungen gut in den Kontext polizeilicher Ermittlungsarbeit eingebunden. Im Gegensatz dazu kann im Bereich der KFZ-Forensik (noch) nicht auf einheitliche Verfahren oder Schnittstellen zur Datenerhebung zurückgegriffen werden (vgl. Brummer und Hoch, 2017, S. 646 f.). Hier ist spezielle und kreative Handlungskompetenz erforderlich, um einzelfallabhängig die notwendigen Entscheidungen zur jeweiligen Vorgehensweise zu treffen. Ähnlich verhält es sich im Bereit des IoT und des Smart-Home: Diese Systeme stellen für Ermittlungspersonen oftmals eine unbekannte Black Box[86] dar. Da zudem keinerlei forensische Tools verfügbar sind, um eine Datenerhebung in diesem Bereich zu standardisieren (vgl. Watson und Dehghantanha, 2016, S. 5), ist an dieser Stelle ebenfalls die fachliche Kompetenz der jeweiligen Ermittlungspersonen über Erfolg oder Misserfolg entscheidend.

Im Bereich der digitalen Ermittlungen ist die hierfür notwendige fachliche Kompetenz nicht weniger entscheidend, denn einerseits sind digitale Spuren aus der kriminalistischen Arbeit nicht mehr wegzudenken, und andererseits müssen durch zielgerichtete digitale Ermittlungen aus der Kenntnis über das jeweilige Verfahren heraus weitere Zusammenhänge erkannt werden, durch welche digitale Spuren ihre volle Beweiskraft entwickeln können. Das bereits erwähnte konzeptionelle Verständnis für die Funktionsweise von Kryptowährungen ist hier immanent (vgl. Eugster, 2018, S. 43). Digitale Ermittlungen setzen somit zwingend Kenntnisse der modernen Datenverarbeitung, das Wissen um mögliche Ermittlungsansätze und eine sog. digitale Spurenkunde voraus, um die Möglichkeiten digitaler Spuren zielführend nutzen zu können (vgl. Kunze, 2018, S. 164).

---

85 So nutzen Ermittlungsbehörden der Bundesrepublik Deutschland für die Auswertung von Mobilfunkgeräten Programme der Firmen Cellebrite, MSAB, Elcomsoft, Oxygen Forensic, X-Ways, Access Data und Magnet Forensics (Deutscher Bundestag, Drucksache 19/3762 vom 10.08.2018, S.27 ff.). Mittels dieser Software-Lösungen ist es teilweise möglich, durch hierfür qualifizierte Polizeibeamte die Mehrzahl aktueller Mobilfunkgeräte forensisch zu sichern und die gesicherten Daten automatisiert zur weiteren Auswertung aufzubereiten.

86 Der Begriff *Black Box* stammt aus dem Bereich der Kybernetik bzw. Systemtheorie und bezeichnet ein in seiner Struktur relativ unbekanntes System, dessen Ein- und Ausgangsgrößen aber bekannt sind oder vorgegeben werden können (vgl. Gottschalk u. a., 1971, S. 262 ff.).

4.2.3 Anforderungen an Kompetenz und Qualifikation

Schulz hat im Jahr 2018 in Rahmen einer empirischen Untersuchung zum Tätigkeitsprofil von Kriminalist*innen[87] herausgefunden, dass fast 56% der befragten Personen für ihre Tätigkeit eine überdurchschnittliche bzw. sehr ausgeprägte IT-Kompetenz als notwendig ansehen (vgl. Schulz, 2018, S. 101). Dies ein relativ hoher Anzeil, wenn man bedenkt, dass nur 4,4% der befragten Personen im Bereich Cybercrime/ Internetkriminalität arbeiten (vgl. ebd., S. 100 f.), zeigt aber gleichzeitig, dass IT-Kompetenz nicht nur in einigen Spezialbereichen relevant ist. Frank postuliert, dass die Nutzung neuer Technologien auch neuer bzw. ergänzender Kompetenzen bedarf, um die komplexe Wirkung und die Zusammenhänge digital gesteuerter und vernetzter Systeme einschätzen zu können (vgl. Frank, 2019, S. 319 f.). Und auch Alonso konstatiert, dass Schlüsselkompetenzen für eine digitalisierte Arbeitswelt notwendig seien. Diese sieht er „[...] als erwerbbare interdisziplinäre Wissensbestände, Fähigkeiten, Fertigkeiten und Einstellungen [...], die die situationsangemessene Realisierung von persönlichen und beruflichen Anforderungen in vielfältigsten Anwendungsbereichen ermöglichen“ (Alonso, 2019, S. 331). Als eine dieser Schlüsselkompetenzen des Digitalen Zeitalters sieht Alonso die Lernkompetenz, um die Chancen der Digitalisierung intelligent nutzen zu können, denn insbesondere solche Kompetenzen, die sich nicht automatisieren lassen, werden in Zukunft weiter an Bedeutung gewinnen (vgl. ebd., S. 332 f.). Des Weiteren wird in Zukunft eine ausgeprägte IT-Kompetenz aller Ermittlungspersonen unverzichtbar sein, wie es Ziercke treffend formuliert:

> „IuK-Kompetenz ist heute eine der Schlüsselkompetenzen, über die Kriminalisten verfügen müssen, um Straftaten zukünftig erfolgreich aufzuklären. Was heute die Aufgabe von Spezialisten ist, muss morgen das Handwerkszeug jedes Kriminalisten sein. Die Curricula unserer Ausbildungseinrichtungen müssen dazu neu justiert werden. Das gilt für die Ausbildung zum höheren Dienst an der Deutschen Hochschule der Polizei ebenso wie für die Fachhochschulausbildung an den Fachhochschulen der Polizei für den gehobenen Dienst.“ (Ziercke, 2014, S. 16).

[87] siehe Abschnitt 4.3.1

Ohne eine ausgeprägte IT- und Medienkompetenz ist eine effektive Strafverfolgung im Zeitalter digitaler Spuren und des Internets kaum noch möglich. Die Herausbildung dieser Kompetenz sollte in den jeweiligen Lehrplänen der polizeilichen Aus- und Fortbildung fest verankert werden. Hering und Vera fordern gar, dass im Zuge von Personalauswahlverfahren Mindeststandards im Zuge der Digitalisierung nachgewiesen werden müssen, damit in der Aus- und Fortbildung hierauf aufgebaut werden kann (vgl. Hering und Vera, 2020, S. 226 f.). Die Durchdringung der polizeilichen Ermittlungsarbeit durch digitale Spuren lässt erkennen, dass insbesondere in Zukunft nicht nur auf speziell ausgebildete Fachleute gesetzt werden kann. Allen Ermittler*innen müssen zumindest Grundkenntnisse im Zusammenhang mit Hard- und Software zu eigen sein und sie müssen sich mit (digitalen) Sicherungs- und Untersuchungsmethoden auskennen (vgl. Fenyvesi, 2016, S. 514). Sie benötigen technisches Hintergrundwissen und müssen in der Lage sein, entsprechende Tools einzusetzen. Da polizeiliche Ermittlungsarbeit aber zusätzlich tiefgründige sozialwissenschaftliche und psychologische Kenntnisse erfordert, ist die Bündelung aller benötigten Kompetenzen keine leichte Aufgabe (vgl. F. Freiling, 2020, S. 1). Miteinander vereint lassen sie aber die Wahrnehmung der positiven und negativen Folgen der digitalen Welt zu, wenngleich hier ein niemals endendes, lebenslanges Lernen inbegriffen ist (vgl. Jaeger, 2019, S. 23). Bei aller Unumgänglichkeit digitaler Kompetenzen in der gesamten Breite polizeilicher Ermittlungsarbeit wird aber je nach Fachspezifik eine Abstufung des jeweiligen Spezialisierungsgrades weiterhin gegeben sein.

4.3 Status Quo und notwendige Konsequenzen

Die Recherchen im Rahmen dieser Arbeit machten deutlich, dass die Thematik der digitalen Kompetenz innerhalb der Polizei wenig erforscht ist. Verschiedene Zukunftsstrategien zur Polizei werden in der Fachwelt zwar diskutiert, inhaltlich setzen sie sich aber eher mit gesellschaftlichen Trends und der polizeilichen Organisationskultur auseinander und inkludieren das Thema digitale Kompetenz nicht (vgl. Lange, Model und Wendekamm, 2019) bzw. reißen es eher an (Rüdiger und Bayerl, 2018). Schulz hat im Rahmen seiner Dissertation grundlegend festgestellt, dass weder ein einheitliches Berufsbild der Kriminalpolizei noch ein tiefes Bewusstsein zur notwendigen Spezialisierung innerhalb der Polizei vorhanden ist (vgl. Schulz, 2018, S. 8 ff.). Diese Erkennt-

nisse sind den Forschungsfragen dieser Arbeit primär nicht zuträglich, jedoch erfasste die empirische Untersuchung im Rahmen dieser Dissertation auch Fragen zur IT-Nutzung von Kriminalbeamt*innen und kann zur Bewertung der digitalen Kompetenz innerhalb der Polizei beigezogen werden. Zusammen mit Experteninterviews aufgrund einer durch die PricewaterhouseCoopers (PWC) GmbH durchgeführten Studie zum Thema der öffentlichen Akzeptanz digitaler Technologien für die deutsche Polizei (vgl. Zink, Zimmermann und Müller-Dofel, 2020) und dem Blick auf die Personalgewinnungsstrategien des Bundes und einiger Länder lassen sich aber ein recht gutes Bild der derzeitigen Situation innerhalb der Polizei und Tendenzen für die Zukunft ableiten.

4.3.1 Digitale Kompetenzen von Kriminalist*innen

Die Items zur IT-Nutzung in Schulz' Dissertation sind überwiegend allgemeiner Natur, jedoch lassen sich Essenzen speziell aus zwei Erkenntnissen ziehen: Über zwei Drittel aller befragten Beamt*innen gab an, mit der Auswertung von Speichermedien, also digitalen Spuren, zu tun zu haben, ohne die entsprechenden Berührungspunkte genauer zu definieren. Lediglich 2,9% fühlten sich hierauf durch die Ausbildung bzw. das Studium gut bis sehr gut, über 60% aber gar nicht vorbereitet. Die dienstliche Fortbildung kann dieses Verhältnis ein wenig relativieren, jedoch spiegeln diese Zahlen die große Diskrepanz zwischen dienstlicher Realität und notwendiger Aus- bzw. Fortbildung wider, was dadurch bekräftigt wird, dass fast 70% der Befragten ihr Wissen regelmäßig durch *Learning by Doing* generiert (vgl. Schulz, 2018, S. 152 ff.). In gleicher Weise bemängelt Kunze, dass beispielsweise in Nordrhein-Westfalen der Bereich der digitalen Spuren in den Curricula gegenüber der klassischen Tatortarbeit und Spurenkunde deutlich unterrepräsentiert sei. Das Thema Cybercrime würde zwar beleuchtet, jedoch erfolge auch in den Fachpraktika in keiner Weise die Berücksichtigung von Spuren in digitaler Form (vgl. Kunze, 2018, S. 169).

Rüdiger und Povalej bestätigen die defizitäre Lage im Bereich der digitalen Spuren und der IT-Kompetenz im Allgemeinen. Die digitale Ausbildung bei der Polizei stehe noch ganz am Anfang, jedoch müsste zwingend digitales Basiswissen vermittelt werden (vgl. Zink, Zimmermann und Müller-Dofel, 2020, S. 49). Povalej konstatiert, dass es sich bei den sog. *Digital Natives* eher um

Digital Naive handle, welche sich nie tiefgründiger mit den neuen Technologien befasst hätten und von einer großen Naivität erfüllt seien, was hinter diesen Technologien steckt und wie sie missbraucht werden können. IT-Kenntnisse und der bewusste Umgang mit neuen Technologien müssten bei der Rekrutierung und Ausbildung viel stärker in den Fokus rücken. Folglich müssten Polizist*innen hierfür kontinuierlich sensibilisiert werden, damit sie von Beginn an richtig handeln und so an digitale Informationen herankommen (vgl. Zink, Zimmermann und Müller-Dofel, 2020, S. 54 f.). Wie ernst die Defizite im Bereich digitaler Kompetenzen tatsächlich sind, untermauert der Prozess um den Anschlag von Halle aus dem Jahr 2019. Die Unzulänglichkeiten digitaler Ermittlungen durch das Bundeskriminalamt (BKA) traten so offensichtlich zutage, dass ein Anwalt es mit einem „humpelnden Patienten, der der Zeit hinterherläuft“ verglich (Jäger, 2020, vgl.).

4.3.2 derzeitige Personal(gewinnungs)strategien

Die Vermittlung und Herausbildung von Kompetenzen ist für den Polizeiberuf unmittelbar vom Personal und dessen Aus- und Fortbildung abhängig. Gemäß Art. 30 GG ist die Zuständigkeit für das Polizeiwesen, und damit auch für die Aus- und Fortbildung des Personals, den Ländern vorbehalten (vgl. Kutscha, 2006, S. 229). Die Ausbildung erfolgt i. d. R. an den hierfür vorgesehenen Fachhochschulen (vgl. Schümchen, 2006), und auch die Rekrutierung des Nachwuchses liegt in der alleinigen Verantwortung der Länder[88]. Im Wesentlichen haben sich hierbei zwei Modelle der Polizeiausbildung etabliert: So setzen einige Länder weiterhin auf Laufbahnen des mittleren und gehobenen Dienstes [89], andere verfolgen konsequent nur noch auf die Ausbildung des gehobenen Dienstes, dessen höherer Anspruch den Abschluss eines dreijährigen Bachelor-Studiums erfordert (vgl. Jasch, 2019, S. 233). Den Prognosen zufolge wird sich die Zahl der potentiellen Bewerber*innen auf dem Ausbildungsmarkt bis zum Jahr 2025 weiter verringern (vgl. BMBF, 2020, S. 18). Die Zahl der studienberechtigten Schulabgänger*innen verhält sich zwar stabil (vgl. ebd., S. 18), jedoch hat die Komplexität und Schwierigkeit des Polizeiberufs

[88] Des Weiteren unterhält der Bund u. a. für die Bundespolizei und das BKA eigene Ausbildungsstellen wie z. B. die Hochschule des Bundes für öffentliche Verwaltung.

[89] So etwa Berlin, Bayern, Schleswig-Holstein und Mecklenburg-Vorpommern (vgl. Jasch, 2019, S. 233)

im Allgemeinen zugenommen (vgl. Jasch, 2019, S. 232 f.), so dass die Herausforderungen, geeignete Bewerber*innen für den Polizeiberuf zu gewinnen, tendenziell größer werden. Ebenso wie die Ausbildungsmodelle unterscheiden sich die Ausbildungsinhalte von Bundesland zu Bundesland. Bieten einige Bundesländer sowie das BKA den Direkteinstieg in die Kriminalpolizei über einen eigenen Studienzweig getrennt zur Ausbildung der Schutzpolizei an (vgl. Mohr, 2015; Bundeskriminalamt, 2018; FHVD, 2018), so verfolgt die Mehrheit der Bundesländer nach wie vor den Weg der Einheitsausbildung, also der Herausbildung von sog. *Generalisten* (vgl. Schulz, 2018, S. 13; HSPV NRW, 2020; FHöVPR, 2020; Polizeiakademie Niedersachsen, 2019).

Unabhängig von den Details der jeweiigen Curricula sollten grundlegende IT-Kompetenzen und die damit verbundenen Kompetenzen im Bereich der digitalen Spuren bereits während der Ausbildung bzw. des Studiums vermittelt und herausgebildet werden. Die Untersuchung einzelner Modulhandbücher offenbart hier jedoch ein äußerst asymmetrisches Bild. So werden die Themen Cybercrime bzw. IuK-Kriminalität mitunter nur als Randerscheinung eines Gesamtmoduls gelehrt (vgl. HSPV NRW, 2020, S. 74 f.), während andere Bundesländer die Thematik tiefgründiger in mehreren Teilmodulen (vgl. Polizeiakademie Niedersachsen, 2019, S. 110 f.)[90] behandeln. Schleswig-Holstein vermittelt im Zuge des Bachelor-Studiums für die Kriminalpolizei konsequent Inhalte aus dem Bereich Cybercrime in einem eigenen Theorie- (vgl. FHVD, 2018, S. 163 f.) und Praxismodul (vgl. ebd., S. 74 f.). Zusätzlich wird die konkrete Thematik der digitalen Spuren für die Bereiche WLAN/ Internet (vgl. ebd., S. 129), Smartphones (vgl. ebd., S. 135) und im Zusammenhang mit Kraftfahrzeugen (vgl. ebd., S. 173) behandelt [91].

Als weiteres zukunftsweisendes Beispiel lässt sich die Ausbildung des Polizeinachwuchses des Landes Hessen heranführen. Hier ist ein Direkteinstieg in die Kriminalpolizei über ein spezialisiertes Bachelor-Studium[92] (vgl. HfPV,

[90] Das Beispiel Niedersachsens zeigt, dass die Thematik Cybercrime bzw. digitale Spuren auch im Rahmen der Einheitsausbildung vermittelt wird. Auch wenn der Grund- und Intensivkurs Cybercrime Ersteinschreiter (vgl. Polizeiakademie Niedersachsen, 2019, S. 111) nur erste Grundlagen vermitteln kann, so zeigt sich doch das Bewusstsein für die Dringlichkeit dieser Thematik.

[91] Als Grund für die umfangreiche Aufnahme digitaler Spuren in das Studium lässt sich vermuten, dass die Polizei Schleswig-Holstein die Ermittlungskompetenz im Bereich der digitalen Spuren seit ein paar Jahren konsequent ausbaut (vgl. Wieczorek, 2018; Landesportal Schleswig-Holstein, 2019).

[92] Eine gesondertes Studium für die Kriminalpolizei impliziert nicht automatisch eine bessere Ausbildung im Bereich digitaler Spuren und von IT-Kompetenz im Allgemeinen. Jedoch ist die Entscheidung zur Spezialisierung schon in der Ausbildung ein erster Schritt in die gezielte Vermittlung spezieller Fähigkeiten

2016) bereits seit dem Jahr 2006 möglich (vgl. Brandt, 2010, S. 27). Hierdurch werden u. a. Bewerber erreicht, die mit ihrem Vorwissen[93] den Weg zur Kriminalpolizei über die Schutzpolizei nie gewählt hätten (vgl. ebd., S. 29). Zusätzlich erzeugen in Hessen externe Spezialisten[94] aus den Bereichen der Informatik und Wirtschaftswissenschaften bereits seit vielen Jahren positive Impulse. Durch sie konnten deutliche Synergiegewinne in der gesamten Polizeiarbeit erzielt werden (vgl. ebd., S. 29). Im Wissen um die notwendigen Kompetenzen im Bereich von Cybercrime wurde zum Wintersemester 2020/2021 der Start eines Kriminalpolizei-Studiums mit der Vertiefungsrichtung „Cyberkriminalistik“ avisiert. Hierdurch sollen in der hessischen Polizei die Kompetenzen im Bereich Cyberkriminalität und digitale Spuren direkt gestärkt werden (vgl. Klein, 2020). Leider gelang es nicht, genug potentiellen Nachwuchs zu gewinnen, so dass der Start verschoben wurde (vgl. Perske, 2020). Die Einführung eines solch spezialisierten Studiums ist grundsätzlich zu begrüßen und es sollte eruiert werden, warum die Zielgruppe technikinteressierter junger Menschen nicht in der erhofften Breite erreicht werden konnte[95].

Als Zwischenbefund lässt sich festhalten, dass sich aus der föderalen Struktur der polizeilichen Aus- und Fortbildung ein äußerst heterogenes Bild ergibt, wie zielführend und tiefgründig die Ausbildung digitaler Kompetenzen verfolgt wird. Die Vermittlung von Wissen im Bereich Cybercrime und digitaler Spuren wird weder einheitlich noch in der Breite konsequent verfolgt und umgesetzt. Folglich ergeben sich langfristig Niveau-Unterschiede zwischen den Polizeien der einzelnen Bundesländer und es ist zu befürchten, dass hieraus ein regionales Gefälle der Ermittlungsqualität entsteht.

4.3.3 Weiterentwicklung der Aus- und Fortbildung

Die zuvor beschriebenen Momentaufnahme der polizeilichen Aus- und Fortbildung offenbart einen Teil der Achillesferse in der Frage, ob die Polizei den

---

und Kompetenzen, was mittelbar auch die Ermittlungsqualität im Bereich digitaler Spuren verbessert.

93 So bewerben sich für den Kripo-Direkteinstieg auch lebenserfahrene Personen, welche ihre Kenntnisse aus vorherigen Berufen und Studien mit einbringen (vgl. Brandt, 2010, S. 27).

94 siehe Abschnitt 4.3.4

95 Es sollte z. B. hinterfragt werden, ob die Bewerber eines solchen Studiums das gesamte Eignungsauswahlverfahren durchlaufen müssen, oder ob nicht auch Zugeständnisse u. a. beim Sporttest zielführend wären.

Herausforderungen digitaler Spuren gewachsen ist. Fauth postuliert analog hierzu, dass die Themen des Kriminalitätsfeldes Cybercrime (und somit auch digitaler Spuren) aus der Fortbildung in die Grundausbildung eines jeden Polizeibeamten übergehen muss:

> „Grundkenntnisse über Datenverarbeitung sowie Hard- und Software der Informations- und Kommunikationstechnologie muss künftig jeder Polizeibeamte ebenso beherrschen, wie das Wissen über Sicherungsmaßnahmen an einem klassischen Tatort, an dem in aller Regel nicht die Spezialisten der Cybercrime zu allererst vor Ort sind. Beweissicherung an elektronischen Speichermedien nehmen bereits jetzt einen nicht mehr wegzudenkenden Raum in der Tatortarbeit der Polizeibeamten ein. [...] Eine ausgeprägte Medienkompetenz für jeden polizeilichen Sachbearbeiter wird sich in naher Zukunft als unverzichtbar darstellen“ (Fauth, 2015, S. 156).

Da digitale Kompetenz eine strukturierte und algorithmische Denkweise verlangt, sollte Informatik nicht nur als Pflichtfach in die Schulausbildung, sondern auch in die Polizeiausbildung integriert und auf Denkweisen abgestellt werden, welche digitales Denken und Lernen bestimmen. Das hiermit seit langem in der „freien Wirtschaft“ als Grundsatz angesehene lebenslange Lernen muss sich auch in der Polizei etablieren, da die Digitalisierung sich permanent fortentwickelt und aktuelles Wissen überdurchschnittlich schnell veraltet (vgl. Jaeger, 2019, S. 24). Im Jahr 2018 wurde für diese Zwecke an der Hochschule der Polizei Rheinland-Pfalz das Fachgebiet IX *Cybercrime und Digitale Ermittlungen* gegründet und das Curriculum des Studiums entsprechend angepasst (vgl. Brummer und Hoch, 2017, S. 647 f.; Hochschule der Polizei Rheinland-Pfalz, 2020). So verantwortet dieses neu gegründete Fachgebiet nicht nur eigene Lehrveranstaltungen in der Fortbildung und einzelnen Modulen, sondern ist in die gesamte Breite des Studiums mit eingebunden (vgl. Hochschule der Polizei Rheinland-Pfalz, 2018), was als zielführend angesehen werden kann, da digitale Spuren in einem großen Teil des polizeilichen Einsatzspektrums eine Rolle spielen. Die frühzeitige Herausbildung entsprechender Kernkompetenzen ist für die Polizei unverzichtbar, denn die Last der digitalen Spurengewinnung liegt allein auf ihr. Allerdings lässt sich das hierfür notwendige Fachwissen nicht mehr nur autonom generieren, so dass sich zusätzlich Kooperationsformen mit Dritten ergeben sollten (vgl. Schneider, 2015, S. 20). Fauth ist der Überzeugung, dass es polizeiinterne Bildungseinrichtungen allein

eher nicht schaffen werden, mit der Weiterentwicklung der IT-Technologie und ihrer Nutzung durch international agierende Straftäter standzuhalten, so dass die Inanspruchnahme externer Hochschulangebote obligatorisch erscheint (vgl. Fauth, 2015, S. 156). Zukunftsorientierte Studiengänge im Bereich der IT-Forensik und -Sicherheit haben sich an mehreren Hochschulen etabliert. So bietet u. a. die Hochschule Mittweida den Fernstudiengang IT-Forensik/ Cybercrime an (vgl. Schulze und Pawlaszczyk, 2018, S. 31) und auch an der Hochschule Albstadt-Sigmaringen lässt sich berufsbegleitend Digitale Forensik studieren. Dieses so gewonnene interdisziplinäre Fachwissen könnte die Ermittlungsarbeit durchweg mit positiven Synergieeffekten beeinflussen (vgl. Korinth, 2019).

Leider zeichnet die gegenwärtige Situation der polizeilichen Ausbildung in der Mehrheit ein konträres Bild, denn größtenteils wird noch immer an der Einheitsausbildung festgehalten. Jedoch ist die Diskussion an dieser Stelle äußerst lebendig, was am Beispiel von Nordrhein-Westfalen (NRW) illustriert werden kann: Hier liegt der gegenwärtige Fokus noch auf der schutzpolizeilichen Ausbildung, jedoch werden die Stimmen zu Neukonzeptionen lauter (vgl. Frings und Zeitner, 2019). So beschloss der Landtag NRW bereits im Jahr 2015, dass durch die Landesregierung zur Verbesserung der polizeilichen Ausbildung eine Schwerpunktsetzung im Studium zu erfolgen hat[96], (Busch, 2015). Eine solche Initiative ist unbedingt zu begrüßen, denn die oftmals aus ideologischen Gründen priorisierte Einheitsausbildung vermag keine Experten für den Polizeiberuf im digitalen Zeitalter zu generieren (vgl. Jaeger, 2019, S. 24). Analog hierzu konstatiert Mahnken: „Die Aufgaben und Ausrichtung der Kriminalpolizei zeigen [...] die Notwendigkeit ganz eigener Studieninhalte, was sich auch in der wachsenden Zahl unterschiedlicher kriminalistischer Bachelorstudiengänge widerspiegelt. Im Zuge der digitalen Transformation entstehen immer mehr Notwendigkeiten der Spezialisierung“ (Mahnken, 2020, S. 51 f.). Schäfer und Schnell postulieren gar, dass die polizeiliche Ausbildung als Bildungsprozess und nicht primär als dauerhafte Übung hierarchisch geführter Einsätze gestaltet werden sollte, da nur so Fähigkeiten erworben werden, auf nicht standardisierbare Handlungsanforderungen fachlich, methodisch und sozial kompetent mit Orientierungs- und Erfahrungswissen zu

[96] Landtag Nordrhein-Westfalen: Drucksache 16/8124 - Die Anwärter*innen sollen nach einem gemeinsamen Grundstudium die Möglichkeit haben, einen Schwerpunktstudiengang „Kriminalpolizei“ oder einen Schwerpunktstudiengang „Schutzpolizei“ zu belegen, um sich dadurch im Hinblick auf ihre spätere Verwendung frühzeitig zu spezialisieren.

reagieren (vgl. Schäfer und Schnell, 2020, S. 343). Eine zeitgemäße Polizeiarbeit verlange eine wissenschaftlich-methodische Kompetenzentwicklung, diese kollidiere aber allzu oft mit dem als soziokulturellem Zement wirkenden Institutionenpatriotismus (vgl. ebd., S. 344).

4.3.4 Rekrutierung von Spezialisten

Neben der zielgerichteten Aus- und Fortbildung des polizeilichen Personals wird von nicht wenigen Bundesländern die Möglichkeit der Einstellung von IT-Spezialisten mit entsprechendem Hochschulabschluss zur Steigerung der eigenen Kompetenz im Bereich Cybercrime und digitaler Spuren Gebrauch gemacht. Der Rückgriff auf diese oftmals als Seiten- oder Quereinsteiger bezeichneten Mitarbeiter erfolgt durch die Länder mehrheitlich seit der Evaluierung ihrer jeweiligen Cybercrime-Bekämpfungsstrategien (vgl. Ministerium des Innern und für Sport Rheinland-Pfalz, 2020; Ministerium für Inneres Digitalisierung und Migration Baden-Württemberg, 2020b; Niedersächsisches Ministerium für Inneres und Sport, 2020). Die Strategie, IT-Spezialisten durch eine gezielte Einarbeitung als Polizeibeamte zu qualifizieren, ist der reziproke Lösungsweg zur Herausbildung von entsprechender IT-Kompetenz durch die Polizei selbst und hat sich in der Praxis seit Jahren bewährt. Des Weiteren sprechen für die Einstellung von IT-Spezialisten die hohen Anforderungen der polizeilichen Aufgaben insbesondere im Bereich der Cybercrime-Bekämpfung sowie der hohe Aufwand von entsprechenden Qualifikationsmaßnahmen für Polizeibeamte (vgl. Erhart, 2014, S. 62). Rossberger macht in diesem Zusammenhang darauf aufmerksam, dass die Personalauswahl eine effiziente Stellschraube zur Unterstützung der digitalen Transformation sei, und dass bei der Rekrutierung geeigneter Mitarbeiter nicht nur auf fachliche Fähigkeiten, sondern auch auf innovationsrelevante Persönlichkeitsfaktoren zu achten sei. Eine hiermit verbundene wissenschaftlich valide Personalauswahl sei zwar aufwendig und teuer, wirke sich langfristig aber nachhaltig positiv aus (vgl. Rossberger, 2019, S. 32). Hering und Vera merken in diesem Zusammenhang an, dass die Polizei vor einem doppelten Dilemma steht. Auf dem ohnehin schon hart umkämpften Arbeitsmarkt wirke sich die Tarifbindung des öffentlichen Dienstes im Wettbewerb mit der freien Wirtschaft als nachteilig aus, so dass man mit finanziellen Anreizen nicht locken könne. Vielmehr müsse man die Vorteile öffentlicher Arbeitgeber wie angenehmes Arbeitsklima, Work-Life-Balance sowie den sicheren und unbefristeten Arbeitsplatz in den Vordergrund

rücken. Zusammen mit einem interessanten Tätigkeitsfeld und dem hohen Ansehen der Polizei in der Bevölkerung lassen sich die unmittelbaren Nachteile im Hinblick auf eine mitunter geringere Vergütung abschmelzen (vgl. Hering und Vera, 2020, S. 240). Schlussendlich mahnt Schneider an, dass nicht nur die Rahmenbedingungen des öffentlichen Dienstes eine Herausforderung darstellen. Im Wissen dass informationstechnische Kompetenz rasch veraltet, genüge nicht allein die Rekrutierung von IT-Spezialisten. Ohne kontinuierliche und den Anforderungen entsprechende Weiterbildungsmaßnahmen verlieren diese Mitarbeiter mittelfristig ihre positiven Synergieeigenschaften oder kehren der Polizei desillusioniert den Rücken (vgl. Schneider, 2015, S. 20). Neben diesen genannten Punkten ist es darüber hinaus unabdingbar, IT-Spezialisten sinnvoll und zielführend in die Ermittlungsarbeit zu integrieren. Eine bloße Aufgabenübertragung anhand eines starren Zuständigkeitskatalogs juristischer Tatbestände ohne jeweilige Abwägung der für die Ermittlungen benötigten Spezialkenntnisse verschenkt wertvolles Potential. Zweck des Einsatzes dieser hochqualifizierten Mitarbeiter sollte immer die Bearbeitung qualitativ anspruchsvoller Aufgaben sein und nicht die massenhafte Abarbeitung einfach gelagerter Sachverhalte, für welche keinerlei Spezialkenntnisse erforderlich sind (vgl. Büchele, 2018, S. 20).

4.3.5 Flexibilisierung des Anforderungsprofils bzw. Wandel des Berufsbildes

Der digitale Alltag der Gesellschaft erzeugt nicht nur eine Erwartung der Bürger an entsprechend zeitgemäße Kommunikationsmöglichkeiten mit der Polizei[97], sondern wirkt sich zunehmend auch auf deren Kernaufgaben und hier insbesondere die Kriminalitätsbekämpfung aus (vgl. Hering und Vera, 2020, S. 201 f.). Zentrale Dienststellen oder einige wenige IT-Spezialisten zur Bearbeitung von Cybercrime und digitalen Spuren sind bereits heute keine ausreichende Antwort mehr auf die vielseitigen Herausforderungen. Die Polizei in ihrer ganzen personellen und auch institutionellen Breite muss über entsprechende Kompetenzen zur professionellen Umsetzung der an sie gestellten Aufgaben verfügen (vgl. Ziercke, 2014, S. 16). Digitale Spuren

[97] Die Polizei ist bereits auf einer Vielzahl an Kommunikationskanälen präsent bzw. über diese erreichbar, u. a. Facebook, Twitter oder Instagram. Die Polizei Nordrhein-Westfalens verfügt seit dem Jahr 2020 gar über einen eigenen Account auf der gerade bei jugendlichen angesagten Plattform TikTok.

stellen somit nicht nur allein Anforderungen an Technik und die mit ihr verbundenen Prozesse, sondern haben Auswirkungen auf die gesamte polizeiliche Arbeit, ihre Organisation und ihre Mitarbeiter. Sie verändern in gewisser Weise die polizeiliche Arbeit als Ganzes (vgl. Hering und Vera, 2020, S. 207). Das Berufsbild der Polizei ist bereits heutzutage deutlich von digitaler Datenverarbeitung und IT-gestützten Systemen gekennzeichnet. Eine ausgeprägte IT-Affinität und IT-Kompetenz können körperliche Fitness sowie soziale und taktische Fähigkeiten zwar nicht ersetzen, finden jedoch in Auswahlverfahren und der Ausbildung bisweilen zu wenig Berücksichtigung (vgl. ebd., S. 241). So ist auch diesem Bereich ist eine Anpassung unumgänglich, denn Methoden zur digitalen Spurensuche und -bearbeitung müssen kontinuierlich (weiter-)entwickelt und effektiv in die Ermittlungsarbeit übernommen werden. Die Bedeutung der Technik erfordert eine permanente enge Zusammenarbeit von Kriminalisten und IT-Spezialisten sowie eine Anpassung der bestehenden Personalgewinnungs- und Personalentwicklungsmodelle. Eine kriminalpolizeiliche Sachbearbeitung in Einzelkämpfer-Manier muss einer Vorgehensweise weichen, die sich durch vielfältige Kooperationsformen, arbeitsteiliges Vorgehen und Bündelung von Kernkompetenzen auszeichnet (vgl. Schneider, 2015, S. 20). Fauth konstatiert hierzu, dass sich das Berufsbild des Polizeibeamten im Zuge der Digitalisierung grundlegend verändert hätte und diese Entwicklung als neue und zusätzliche Herausforderung betrachtet werden müsse. Allerdings ließen diese Veränderungen des Berufsbildes klassische Tugenden und Fähigkeiten sowie kriminalistische Denkweisen keinesfalls als obsolet erscheinen (vgl. Fauth, 2015, S. 159). Kretschmer formuliert ein ähnliches Bild: Moderne Polizeiarbeit erfordere Flexibilität und eine schnelle Anpassung an neue Gegebenheiten, und man müsse überdenken, ob der Generalist[98], wie wer noch immer überwiegend ausgebildet wird, diese Bedingungen erfüllen könne oder ob nicht bereits bei der Ausbildung zu spezialisieren sei. Nichtsdestoweniger müssten innovative digitale Möglichkeiten auch von der Polizei so genutzt werden, dass ein zielführender und ressourcenschonender Einsatz der verfügbaren Kräfte erfolgen kann (vgl. Kretschmer, 2019, S. 44). Dieser Einschätzung kann uneingeschränkt zugestimmt werden, wobei das bis hierhin Erkannte weniger einen Wandel, sondern eher einen höheren Anspruch an das Berufsbild der Polizei bedeutet, denn trotz aller neuen Maßstäbe im Hinblick auf digitale Spuren kann auch in Zukunft nicht auf bisherige Anforderungen und Kompetenzen verzichtet werden. Hier wiederholt sich das

[98] siehe Abschnitt 4.3.3

Dilemma der Nachwuchsgewinnung und lenkt den Blick auf die Frage, ob in der polizeilichen Ermittlungsarbeit stärker als je zuvor auf Spezialisierung und bedarfsorientierte kollektive Zusammenarbeit gesetzt werden sollte. Ansonsten droht eine Polizei, „[...] die sich aus einem schnell größer werdenden Bereich der Lebenswirklichkeit zurückzieht. Kaum vorstellbar, dass dann noch der präventive und repressive Auftrag auch nur annähernd erfüllt werden kann“ (Schneider, 2015, S. 20).

4.3.6 Institutionelle Anpassungen

Die Polizeiarbeit wird in Deutschland oftmals noch immer als traditioneller Beruf wahrgenommen - mit dem Generalisten im Mittelpunkt, der überall einsetzbar ist. Hinzu kommt die immer noch gelebte (und aus der schutzpolizeilichen Denkweise unreflektiert übernommene) Praxis, dass Ermittler für eine sog. „Verwendungsbreite“ regelmäßig das Fachgebiet zu wechseln haben. Im Bereich von Cybercrime und digitalen Spuren ist man aber erst nach ein bis zwei Jahren Einarbeitung produktiv, so dass sich häufige Wechsel des Fachgebiets kontraproduktiv auswirken (vgl. F. Freiling, 2020, S. 2). Das institutionelle Beharren auf verfestigte Denkweisen und Routinen in einer Welt ausgeprägter Spezialisierung, sich anpassender Täter, Tatgelegenheiten und Modi Operandi stellt demnach eine Gefahr dar. Gerade die Heterogenität digitaler Spuren zwingt zu weiterer Spezialisierung im Bereich der IT-Forensik und digitaler Ermittlungen. Die Analyse und Dokumentation flüchtiger Informationen u. a. aus der Cloud erfordern neue Organisationsformen und Arbeitsprozesse (vgl. Schneider, 2015, S. 19). Plank ist hierzu der folgenden Ansicht: „Dies erfordert ein z. T. neues Denken und umfangreiche kriminaltaktische Expertise, [...] idealerweise immer in der fallanalytisch arbeitsteiligen Kombination erfahrener Kriminalisten und kriminalistisch fortgebildeter IT-Professionals bzw. IT-Forensikern unter der Klammer einer permanenten ermittlungsbegleitenden IT-unterstützten Fallanalyse“ (Plank, 2020, S. 14). Und auch Mahnken konstatiert in Anlehnung an Lévesque und Vonhof, dass sich behördliches Denken in Zuständigkeiten und eine Ermittlungsarbeit durch Einzelkämpfer als nicht mehr zeitgemäß erweisen (vgl. Mahnken, 2020, S. 52).

Lévesque und Vonhof stellen des Weiteren fest, dass sich komplexe Sachverhalte[99] weder trivialisieren noch reduzieren lassen, sondern besser durch

[99] Bei digitalen Spuren und digitalen Ermittlungen handelt es sich zweifellos um äußerst komplexe Sachverhalte.

koordinierte Arbeit in multiprofessionellen Teams und dem Zuwachs an Erkenntnissen bearbeitet werden (vgl. Lévesque und Vonhof, 2018, S. 17). In VUKA-Umwelten[100] sei es zu Beginn eines Prozesses kaum möglich zu erkennen, was das richtige Vorgehen bei einer Problemlösung sei. Durch agiles Vorgehen, nämlich die Bildung interdisziplinärer und zuständigkeitsübergreifender Teams, erfolge eine weitaus effektivere Aufgabenbearbeitung, und die gemeinsame Suche nach Lösungsideen helfe jedem Beteiligten, aus der Position des isolierten Einzelkämpfer herauszutreten, Unterstützung im Team zu erfahren und mit ihm zu wachsen (vgl. ebd., S. 19). Folglich sollten IT-Spezialisten und Ermittler mit speziell kriminalistischer Expertise organisatorisch dicht aneinandergegliedert sein, denn nur so lässt sich eine dynamische und flexible Zusammenarbeit zeitnah gestalten. Zusätzlich können IT-Spezialisten bei der Bewertung digitaler Spuren unterstützen sowie ihre Erkenntnisse aus digitalen Ermittlungen unmittelbar in den Kontext des jeweiligen Verfahrens einbringen. Und auch kriminalpolizeiliche Ermittler erfahren durch die enge Zusammenarbeit mehr Wissenstransfer zu erforderlichen Spezialkenntnissen als dies durch Fortbildungen zu erreichen wäre (vgl. Büchele, 2018, S. 21 f.). Damit die dargelegte enge Verzahnung erfolgen kann, ist eine organisatorische Nähe von Spezial- und Ermittlungsdienststellen notwendig. Zentralen Cybercrimedienststellen wohnt zweifelsohne die gesamte Breite an benötigter IT-Kompetenz inne, jedoch sind sie „in der Fläche“ für eine lebendige Zusammenarbeit i. d. R. zu weit entfernt. Als zielführender kann als Beispiel die Neustrukturierung der Polizei Baden-Württemberg im Jahr 2013 gelten. Hier wurde in den zwölf Präsidien jeweils die Kriminalinspektion „Cybercrime/ Digitale Spuren“ ins Leben gerufen, so dass ein Netz von Spezialisten in der Fläche zur Verfügung steht (vgl. Fauth, 2015, S. 157; Ministerium für Inneres Digitalisierung und Migration Baden-Württemberg, 2020a). Eine weitere Steigerung organisatorischer Nähe würde eine von Büchele vorgeschlagene Matrixorganisation dezentral angeordneter Cybercrime-Dienststellen ermöglichen, welche deren Gewichtung neben der Bearbeitung wertiger Cybercrime-Verfahren vorrangig in der IT-Forensik und Ermittlungsunterstützung vorsieht, da digitale Spuren und Ermittlungen in jedem Deliktsfeld von Belang sind und Spezialressourcen sowie fachliche Unterstützung so zielgerichtet eingesetzt werden können (vgl. Büchele, 2018, S. 21 f.). Dennoch ist, wie bereits in Abschnitt 4.3.3 festgestellt wurde , die Integration des technologischen Aspektes in

[100] siehe Fn. 16, Digitale Spuren erfüllen, gerade durch ihre fortwährende Weiterentwicklung, ohne Einschränkung die VUKA-Bedingungen, denn sie sind durch Flüchtigkeit, Unsicherheit, Komplexität und Mehrdeutigkeit gekennzeichnet.

die Polizeiausbildung unverzichtbar, denn einzig und allein auf den Einsatz zusätzlicher IT-Spezialisten zu setzen, kann nicht als zielführend angesehen werden. Digitale Technologien spielen eine ubiquitäre Rolle und zuständige Ermittler müssen auch über entsprechende technische Kenntnisse verfügen, um in der Lage zu sein, Beweise selbst zu analysieren (vgl. F. Freiling, 2020, S. 4).

Eine gegenwartsnahe Polizei täte gut daran, sich Innovationen und bewährter Vorgehensmodelle zur VUKA-Welt außerhalb ihrer eigenen Reihen, beispielsweise der freien Wirtschaft, nicht zu verschließen, was natürlich nicht unreflektiert erfolgen darf, denn im Mittelpunkt ihrer Arbeit steht nicht irgendeine Dienstleistung, sondern immer der Faktor Mensch (vgl. Hering und Vera, 2020, S. 234). Dies würde zugleich die Etablierung einer innovationsfördernden Fehlerkultur im bis dato stark hierarchischen, null-fehlertoleranten System der Polizei erfordern, denn nur ein geringeres Fehlervermeidungsbedürfnis fördert Innovations- und Handlungswillen. Nichtsdestoweniger sind Fehler nicht per se als negativ einzuordnen, sondern ihnen entspringen oftmals gewinnbringend neue Erkenntnisse (vgl. Lévesque und Vonhof, 2018, S. 20). Rossberger hingegen fürchtet, dass Innovationen, da sie oft unsicherheitsbehaftet sind, in stark geregelten, hierarchisch strukturierten und fehlerintoleranten Organisationen selten erfolgreich umgesetzt werden können. Zudem wirken sich autoritäre Führungsstile im Innovationskontext äußerst kontraproduktiv aus. Innovation könne also nicht top-down befohlen werden, sondern es müssten innovationsfördernde Rahmenbedingungen geschaffen werden (vgl. Rossberger, 2019, S. 26). Zugleich wirke sich „[...] partizipatives Führungsverhalten und das Gewähren von Freiheitsgraden positiv auf das innovative Verhalten von Mitarbeitern [aus]“ (ebd., S. 26). An dieser Stelle muss leider registriert werden, dass die Institution Polizei in der Mehrheit derzeit weder über fehlertolerante noch innovationsfördernde Rahmenbedingungen verfügt. Dies ist zweifelsohne ihrer stark hierarchisch geprägten Struktur geschuldet. Jedoch sollte hierbei gerade im Bereich digitaler Spuren eine Transformation erfolgen, denn nur so „[...] wird ein ständiger Lern- und Verbesserungsprozess in Gang gesetzt. [...] So entsteht stabiles Systemwissen, ohne in Routinen zu verfallen, die nicht mehr reflektiert werden oder nach dem Motto funktionieren: ‚Wenn ich einen Hammer habe, wird jedes Problem zum Nagel‘“ (Lévesque und Vonhof, 2018, S. 21).

5 Schlussbetrachtung und Ausblick

Die Motivation dieser vorliegenden Masterarbeit war die kritische Frage, welche Risiken und Herausforderungen, aber auch welche neuen (aufgrund von Kompetenzdefiziten oftmals noch ungenutzten) Möglichkeiten digitale Spuren für die polizeiliche Ermittlungsarbeit bergen. Hierzu wurden mit Hilfe der drei Thesen die beiden forschungsleitenden Fragen erarbeitet, die zum einen die Klärung der notwendigen (digitalen) Kompetenz seitens der Polizei in Bezug auf digitale Spuren ermöglichen sollte, um dann erkennen zu können, ob die Polizei strukturell und vor allen Dingen personell den Herausforderungen digitaler Spuren gewachsen ist.

Die theoretische Begriffsbestimmung rund um die Thematik der klassischen analogen Spuren bildete die Grundlage für die Auseinandersetzung mit der hierauf in Teilen aufsetzenden Thematik der digitalen Spuren und war gleichzeitig die Ausgangsbasis für die These, dass sich digitale Spuren aufgrund ihrer besonderen Eigenschaften deutlich von ihren analogen Pendants abheben. Diese These fand sich im darauf folgenden Kapitel bestätigt. Digitale Spuren sind nicht unmittelbar wahrnehmbar, sondern müssen erst mit Hilfe aufeinander aufbauender Abstraktionsschichten wahrnehmbar gemacht werden. Auch konnte gezeigt werden, dass digitale Spuren abhängig von ihrer jeweiligen Kategorie über entsprechend unterschiedliche Eigenschaften im Hinblick auf Flüchtigkeit, Kopierbarkeit und Manipulierbarkeit aufweisen, wovon wiederum eine starke Abhängigkeit ihrer Integrität und dem Nachweis ihrer Authentizität besteht. Als eine wichtige Erkenntnis ging hierbei hervor, dass mit zunehmender Flüchtigkeit digitaler Spuren die Anforderungen an die informationstechnische Kompetenz des polizeilichen Personals und an die technische Ausrüstung in starkem Maße zunehmen und dass sich eine lückenlose Dokumentation aller durchgeführten Arbeitsschritte als obligatorisch darstellt, da einmal durchgeführte Handlungen u. U. nicht wiederholbar sind. Der in der IT-forensischen Fachliteratur bisher so gut wie nicht in Erscheinung tretenden Kategorie der Remote- bzw. Online-Spuren wurde ein etwas umfangreicherer Abschnitt gewidmet, da sich mit ihnen nicht nur völlig neue technische, sondern ebenso juristische Herausforderungen ergeben. Allem voran aber ist es die ubiquitäre Vernetzung der digitalen Welt, welche dieser Kategorie digitaler Spuren in naher Zukunft wohl die vorrangige Rolle zuspielt. Zudem sind sie örtlich entgrenzt und stellen in der Gesamtheit ihrer

spezifischen Eigenschaften viele unbekannte Größen bereit. Ein weiteres Novum ist die Einschränkung technisch möglicher Sicherungen transnationaler Spuren durch die Strafprozessordnung und internationale Abkommen. Trotz lebendiger Diskussion in den entsprechenden Fachkreisen wird seitens der Strafverfolgungsbehörden leider keine einheitliche Auffassung vertreten, woraus wiederum Handlungsunsicherheit seitens der Polizei entspringen.

Digitale Spuren stellen aufgrund ihrer aufgezeigten Besonderheiten, insbesondere aber wegen ihres mittlerweile deliktsunabhängigen Auftretens weitere zentrale Anforderungen an die Strafverfolgungsbehörden. Da sich, auch im Zuge von Standardmaßnahmen[101], die digitale Spurenlage rasant fortentwickelt, betreffen sie die gesamte Breite polizeilicher Arbeit, so dass die Polizei in ihrer vollumfänglichen Handlungsbreite über entsprechende Kompetenzen verfügen muss. Eine weitere wesentliche Erkenntnis dieser Arbeit entspringt der ubiquitären Vernetzung der digitalen Lebens- und Arbeitswelt: der Übergang digitaler Spuren zu digitalen Ermittlungen. Damit spezielle Spuren[102] ihre volle Beweiskraft entwickeln können, müssen mittels zielgerichteter digitaler Ermittlungen weitere Zusammenhänge erkannt und hieraus die entsprechenden Schlüsse gezogen werden. Auch hier findet sich eine Antwort auf die erste Forschungsfrage, denn digitale Spuren und digitale Ermittlungen sind ohne Kenntnisse der modernen Datenverarbeitung und das Wissen um entsprechende Ermittlungsansätze nicht greifbar. Dieses Wissen muss fortwährend auf einem aktuellen Stand gehalten werden, denn es veraltet in rasanter Schnelligkeit. Zudem lassen sich durch die unüberschaubar wachsende Menge und Vielfalt digitaler Spuren kaum vorgegebene Handlungsroutinen definieren und verstetigen. Ein zielgerichtetes Vorgehen in sich verändernden Umgebungen und das Finden von Lösungen zu bis dato nicht gekannten Problemen sind von primärer Bedeutung. Somit verdeutlicht sich, dass die speziellen Anforderungen digitaler Spuren nicht nur technischer, sondern auch personell-institutioneller Natur sind. Des Weiteren wird hierdurch die zweite einführende These dieser Arbeit untermauert, dass eine strikte Trennung von Ermittlungsarbeit und IT-Forensik in der Praxis kaum einzuhalten ist, denn das Zusammenspiel digitaler Spuren und polizeilicher Ermittlungsarbeit erfolgt in einem weitaus komplexerem Geflecht als zu früheren (Offline-)Zeiten.

Kapitel 4 widmete sich hauptsächlich der zweiten zentralen Forschungsfrage dieser Arbeit: Ist die Polizei strukturell und vor allen Dingen personell den

[101] u. a. der des ersten Angriffs oder bei Durchsuchungen
[102] siehe Abschnitt 4.1.3

Herausforderungen digitaler Spuren gewachsen? Es wurde systematisch untersucht, wie digitale Spuren in den Kontext polizeilicher Ermittlungsarbeit integriert sind bzw. sein sollten, welche entsprechenden Qualifikationen und Kompetenzen vorhanden bzw. erforderlich sind, und ob dies durch die gegenwärtige Aus- und Fortbildungssituation, die Personalstrategie sowie den strukturellen Aufbau der einzelnen Landespolizeien gegenwartsnah und zukunftsfähig gewährleistet ist. Selbstverständlich konnten im Rahmen dieser Arbeit nur einige ausschnitthafte Vergleiche mehr und auch weniger positiver Beispiele aus einzelnen Landespolizeien vollzogen werden. Dennoch war eine Beantwortung der ausgehenden Frage ohne Weiteres möglich. Die Polizei sieht sich in ihrer täglichen Arbeit neben den hinlänglich erörterten digitalen Spuren klassischer IT-Systeme vermehrt mit neuartigen u. a. Smart-Home-, Smart-Car- oder IoT-Umgebungen konfrontiert. Da gerade in Situationen von Durchsuchungsmaßnahmen, Maßnahmen des ersten Angriffs oder auch Verkehrsunfall-Szenarien kaum flächendeckend auf entsprechende Spezialisten zurückgegriffen werden kann, ist nicht nur ein Bewusstsein, sondern eben auch entsprechende (Handlungs-)Kompetenz im Zusammenhang mit digitalen Spuren und digitaler Ermittlungen unverzichtbar. Dass z. T. gegenwärtig mangels eigener Sachkompetenz durch die Ermittlungsbehörden auf kommerzielle Dienstleister zurückgegriffen wird, überschreitet oft den eng gestrickten Rahmen der dafür vorgesehenen Sachverständigenbestellung. Auch spricht hier der Anspruch des Staates dagegen, Monopol der Strafrechtspflege zu sein. Zweifelsohne ist so auch kein Zuwachs an eigener digitaler Kompetenz zu erwarten, der Zuwachs externer Abhängigkeiten steigt jedoch überproportional an. Insofern dürfen die erforderlichen Schlüsselkompetenzen im Zeitalter digitaler Spuren und des Internets nicht auf den Schultern weniger Spezialisten verteilt sein, sondern alle Ermittler*innen müssen zumindest über Grundkenntnisse in diesem Bereich verfügen. Schulz' Umfrage aus dem Jahr 2018 konnte zwar zeigen, dass die überwiegende Mehrheit der Kriminalbeamt*innen in ihrer täglichen Arbeit mit digitalen Spuren in Berührung kommt, jedoch gab die weitaus größere Mehrheit auch an, das hierfür notwendige Wissen nicht durch Aus- und Fortbildung vermittelt bekommen, sondern sich selbst angeeignet zu haben. Eine vergleichende Auswertung der Curricula zur Ausbildung des Polizeinachwuchses verschiedener Bundesländer offenbarte tatsächlich entscheidende Unterschiede, wie zielführend und tiefgründig die Herausbildung digitaler Kompetenzen verfolgt wird. Einerseits ist es die sog. Einheitsausbildung, welche noch immer von einem Großteil der Bundesländer favorisiert wird, aber bereits frühzeitig der notwendigen Spezialisierung einer

gegenwartsnahen Polizei entgegenwirkt. Andererseits hängt vielmehr von der Gewichtung, mit welcher digitale Spuren und Cybercrime in der polizeilichen Ausbildung platziert ist, der zukünftige Erfolg polizeilicher Arbeit auf diesem Gebiet ab. Somit muss bis hierhin leider konstatiert werden, dass die Polizei im Hinblick auf die Aus- und Fortbildung ihres Personals den Herausforderungen digitaler Spuren bundesweit zurzeit nicht kongruent gewachsen ist. Dem sollte mit einer frühzeitigen Spezialisierung[103] und der Anpassung der jeweiligen Studieninhalte begegnet werden. Cybercrime und digitale Spuren dürfen nicht länger „unter ferner liefen“ in Erscheinung treten, sondern müssen mit einer Gewichtung in der Aus- und Fortbildung vertreten sein, die der derzeitigen und zukünftigen Arbeits-Realität entspricht.

Indessen haben sich nahezu alle Bundesländer im Bewusstsein um die Ermangelung eigener IT-Kompetenz in der Ermittlungsarbeit seit vielen Jahren sog. Seiteneinsteigern, also IT-Spezialisten mit entsprechenden Hochschulabschlüssen, geöffnet. Diese werden entweder zu Polizeivollzugsbeamten mit allen hoheitlichen Befugnissen ausgebildet oder unterstützen entsprechend als Tarifangestellte die polizeiliche Arbeit. Obgleich die Integration dieser Spezialisten in die polizeiliche Struktur nicht immer optimal gestaltet ist, so sollte der zunehmende Einsatz dieser hoch qualifizierten Mitarbeiter uneingeschränkt fortgeführt werden. Neben einer entsprechenden Aus- und Weiterbildung von Polizeibeamten gewinnt die Institution Polizei so die dringend notwendige IT-Kompetenz. Zusätzlich fördert eine flexible und enge Zusammenarbeit von IT-Spezialisten und Kriminalisten ein arbeitsteiliges Vorgehen und die Bündelung von Kernkompetenzen. An dieser Stelle erschließt sich ein weiterer Baustein zur Antwort auf die zweite Forschungsfrage dieser Arbeit: Weder der Generalist ohne Spezialkenntnisse noch eine kriminalpolizeiliche Sachbearbeitung in Einzelkämpfer-Manier sind in der Lage, den umfangreichen Herausforderungen digitaler Spuren mit entsprechender Handlungskompetenz zu begegnen. Vielmehr ist an dieser Stelle ein zielführender, bedarfsorientierter und kollektiver Ressourceneinsatz des Personals entsprechend der jeweiligen Spezialisierung gefragt. Hierzu gehört auch, dass in einer Umwelt mit vielen bisher unbekannten Fragestellungen, wie sie durch sich rasant fortentwickelnde digitale Spuren erzeugt werden, Innovationsförderung und keine Fehlervermeidungs-Kultur gelebt wird. Hierauf ist die Polizei

[103] z. B. die Unterteilung des Studiums für die Schutz- und Kriminalpolizei. Auch der Vorstoß Hessens mit einer Spezialisierungsrichtung „Cybercrime“ (siehe Abschnitt 4.3.2) ist durchaus begrüßenswert und sollte durch andere Bundesländer aufgegriffen werden.

durch ihre stark hierarchische Struktur nicht optimal vorbereitet. Jedoch bedeutet das starre Festhalten an althergebrachten Denk- und Arbeitsweisen eine zunehmende Entfremdung von der Lebensrealität. Negiert die Polizei die ihr vorgegebenen Umstände der Digitalisierung, so besteht die Gefahr, dass sie sich zusehends aus einem schnell größer werdenden Bereich der Lebenswirklichkeit zurückzieht. Dies würde zwangsläufig zu der Gefahr führen, dass der ihr zugetragene präventive und repressive Auftrag durch sie nicht mehr erfüllt werden kann (vgl. Schneider, 2015, S. 20). Für die Sicherheit einer modernen Gesellschaft jedoch ist eine ebenso moderne Polizei, die effektiv arbeitet, gut geschult ist und zielgenau in die Welt digitaler Spuren eintaucht, von existenzieller Bedeutung.

6 Literatur

Ackermann, Rolf (2019a). „Durchsuchung/Beschlagnahme“. In: *Handbuch der Kriminalistik - Kriminaltaktik für Praxis und Aufklärung*. Hrsg. von Rolf Ackermann, Horst Clages und Holger Roll. 5. Auflage. Stuttgart: Richard Boorberg Verlag, S. 499–563.

– (2019b). „Einführung in die Kriminalistik“. In: *Handbuch der Kriminalistik - Kriminaltaktik für Praxis und Aufklärung*. Hrsg. von Rolf Ackermann, Horst Clages und Holger Roll. 5. Auflage. Stuttgart: Richard Boorberg Verlag, S. 1–54.

ACPO (2012). *ACPO Good Practice Guide for Digital Evidence*. URL: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (besucht am 19. 09. 2020).

Alonso, Gardenia (2019). „Technik braucht Kultur – Lernkultur und Kompetenzentwicklung im Zeitalter der Digitalisierung“. In: *Gestaltung und Management der digitalen Transformation : Ökonomische, kulturelle, gesellschaftliche und technologische Perspektiven*. Hrsg. von Ronny Alexander Fürst. Wiesbaden: Springer Fachmedien Wiesbaden, S. 329–346.

Arnold, Jörg (2015). „Digitale Spuren in Fahrzeugen – die Zukunft ist bereits Realität“. In: *Kriminalistik* Heft 12, S. 742–747.

Asche, Rüdiger R. (2016). *Embedded Controller*. Wiesbaden: Springer Fachmedien Wiesbaden.

Baier, Harald und Sebastian Gärtner (2019). *Einführung in die digitale Forensik[DigiFor]*. 3. Auflage. Darmstadt: Hochschule Darmstadt.

Ballmann, Bastian (2015). *Understanding Network Hacks*. Berlin, Heidelberg: Springer Berlin Heidelberg.

Banday, M. (2011). „Technology Corner: Analysing E-Mail Headers for Forensic Investigation“. In: *Journal of Digital Forensics, Security and Law* Vol. 6(2), S. 49–64.

Bär, Wolfgang (2011). „Transnationaler Zugriff auf Computerdaten“. In: *Zeitschrift für Internationale Strafrechtsdogmatik* Heft 2, S. 53–59.

Bauer, Johannes, Michael Gruhn und Felix C. Freiling (2016). „Lest we forget: Cold-boot attacks on scrambled DDR3 memory“. In: *Digital Investigation* 16, S65–S74.

Beebe, Nicole (2009). „Digital Forensic Research: The Good, the Bad and the Unaddressed“. In: *Advances in Digital Forensics V*. Hrsg. von Gilbert Peterson und Sujeet Shenoi. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 17–36.

Bell, Charles (2020). *Beginning Sensor Networks with XBee, Raspberry Pi, and Arduino*. Berkeley, CA: Apress.

Benecke, Mark (2005). „Genetischer Fingerabdruck“. In: *Der Große Brockhaus, Enzyklopädie in 30 Bänden*. 21. Auflag. Leipzig: F.A. Brockhaus, S. 449–454.

Bennett, Nathan und James Lemoine (2014). „What a Difference a Word Makes: Understanding Threats to Performance in a VUCA World“. In: *SSRN Electronic Journal* 57, S. 311–317.

Bergen, Natalie (2019). *Alle Kryptowährungen Liste – August 2019*. URL: https://www.bestekrypto.de/alle-kryptowaehrungen (besucht am 14. 09. 2020).

Biebl, Jürgen (2012). „Wofür steht Cloud Computing eigentlich?“ In: *Wirtschaftsinformatik & Management* 4.1, S. 22–29.

BMBF, Hrsg. (2020). *Berufsbildungsbericht 2020*. Bonn: Bundesministerium für Bildung und Forschung, Referat Grundsatzfragen der beruflichen Aus- und Weiterbildung.

Brandt, Günter (2010). „Hessen geht den richtigen Weg bei der Einstellung und Ausbildung für die Kripo“. In: *der kriminalist* Heft 9, S. 27–29.

Braun, Frank und Jan Dirk Roggenkamp (2012). „Privatisierung technisch gestützter Ermittlungsmaßnahmen?“ In: *NK - Neue Kriminalpolitik* Heft 4, S. 141–146.

Breiter, Andreas und Andreas Hepp (2018). „Die Komplexität der Datafizierung: zur Herausforderung, digitale Spuren in ihrem Kontext zu analysieren“. In: *Neue Komplexitäten für Kommunikationsforschung und Medienanalyse: Analytische Zugänge und empirische Studien*. Hrsg. von Christian Katzenbach u. a. Bd. 4. Digital Communication Research. Berlin, S. 27–48.

Brezinski, Dominique und Tom Killalea (2002). *RFC 3227: Guidelines for Evidence Collection and Archiving*. URL: http://www.ietf.org/rfc/rfc3227.txt (besucht am 17. 10. 2020).

Brodowski, Dominik und Felix Freiling (2015). „Cyberkriminalität - Erscheinungsformen, Entwicklungslinien, Herausforderungen“. In: *FIfF-Kommunikation* Nr. 4, S. 22–26.

Brummer, Patrick und Martin Hoch (2017). „Das Kraftfahrzeug als Beweismittel“. In: *Kriminalistik* Heft 11, S. 643–648.

BSI (2011). *Leitfaden „IT-Forensik“*. Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Büchele, Christoph (2018). „Internetkriminalität: Veränderte Kriminalitätsformen erfordern veränderte Organisationsformen“. In: *der kriminalist* Heft 7, S. 18–22.

Bundeskriminalamt (2018). *Modulhandbuch Cyberkriminalisten*. URL: https://www.bka.de/DE/KarriereBeruf/Landingpages/Cyber-Kriminalist/_module/09_Das_koennte_auch_interessieren/modulhandbuch_node.html (besucht am 10. 11. 2020).

Bundesnetzagentur (2016). *Algorithmenkatalog 2016*. URL: https://www.bundesnetzagentur.de/EVD/SharedDocuments/Downloads/QES/Algorithmen/2016Algorithmenkatalog.pdf (besucht am 29. 10. 2020).

Busch, Wibke (2015). „Schupo und/ oder Kripo ?“ In: *Landtag Intern* Heft 8, S. 13.

Carrier, Brian (2006). *A hypothesis-based approach to digital forensic investigations*. West Lafayette: Purdue University, Center for Education, Research in Information Assurance und Security.

Casey, Eoghan (2011). *Digital Evidence and Computer Crime*. 3. Auflage. San Diego: Academic Press.

– (2018). „The need for translational research in digital investigation“. In: *Digital Investigation* 26, S. 1–2.

Clages, Horst (2019a). „Beweislehre, Beweisführung“. In: *Handbuch der Kriminalistik - Kriminaltaktik für Praxis und Aufklärung*. Hrsg. von Rolf Ackermann, Horst Clages und Holger Roll. Stuttgart: Richard Boorberg Verlag, S. 55–74.

– (2019b). „Erster Angriff“. In: *Handbuch der Kriminalistik - Kriminaltaktik für Praxis und Aufklärung*. Hrsg. von Rolf Ackermann, Horst Clages und Holger Roll. Stuttgart: Richard Boorberg Verlag, S. 107–168.

Claus, Volker und Andreas Schwill (1991). *Duden Die Informatik*. 2. Auflage. Mannheim: Bibliographisches Institut & F.A. Brockhaus AG.

Council of Europe (2001). *Convention on Cybercrime*. URL: https://www.refworld.org/docid/47fdfb202.html (besucht am 09. 11. 2020).

Czerner, Frank (2017). „Digitale Forensik zwischen (Online-)Durchsuchung, Beschlagnahme und Datenschutz“. In: *Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten*

realen Welt. Hrsg. von Dirk Labudde und Michael Spranger. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 265–300.

Dahm, Markus H. und Eva Walther (2019). „Digitale Transformation“. In: *Strategie und Transformation im digitalen Zeitalter: Inspirationen für Management und Leadership*. Hrsg. von Markus H Dahm und Stefan Thode. Wiesbaden: Springer Fachmedien Wiesbaden, S. 3–21.

Dalby, Jakob (2016). *Grundlagen der Strafverfolgung im Internet und in der Cloud*. Wiesbaden: Springer Fachmedien Wiesbaden.

Davidoff, Sherri und Jonathan Ham (2012). *NetworkForensics*. Upper Saddle River: PearsonEducation, Inc.

Dewald, Andreas und Felix C. Freiling (2014). „From Computer Forensics to Forensic Computing: Investigators Investigate, Scientists Associate“. In: *Technical Reports, CS-2014-04, May 2014*. Erlangen: Friedrich-Alexander-Universität Erlangen-Nürnberg, Dept. of Computer Science.

– (2015). *Forensische Informatik*. Hrsg. von Friedrich-Alexander-Universität Erlangen (FAU). Norderstedt: BoD - Books on Demand.

DHPol (2018). *SENTINEL - Sicherheit im Einsatz durch Open-Source-Intelligence (OSINT) in Einsatzleitstellen*. URL: https://www.dhpol.de/departements/departement_II/FG_II.1/projekt-sentinel.php (besucht am 10. 11. 2020).

Dolle, Wilhelm (2009). „Computer-Forensik in der Praxis“. In: *Datenschutz und Datensicherheit - DuD* 33.3, S. 183–188.

Eggert, Marc (2019). *Medieninfo: Internet of Things - Wenn die Kaffeemaschine den Zutritt blockiert - Network of Smart Thinkers, Der Expertenkongress für Cyber-Experten am 25. und 26. September in Filderstadt*. Landeskriminalamt Baden-Württemberg.

Eisenbraun, Markus (2020). „Digitale Spuren: der dritte Meilenstein“. In: *Moderne Polizei* Heft 1, S. 37–38.

Erhart, Michael (2014). „Die Cybercrimebekämpfung in Mecklenburg-Vorpommern“. In: *Kriminalistik* Heft 1, S. 60–64.

Eugster, Andreas (2018). „Kryptowährung Bitcoin“. In: *Kriminalistik* Heft 1, S. 40–51.

Fauth, Jürgen (2015). „Veränderungen polizeilicher Alltagsarbeit durch die Entwicklung der IT und die Auswirkungen auf das Berufsbild des Polizeibeamten“. In: *Cyber-Sicherheit*. Wiesbaden: Springer Fachmedien Wiesbaden, S. 147–159.

Fenyvesi, Csaba (2016). „Entwicklungsmöglichkeiten und Herausforderungen der Kriminalistik“. In: *Kriminalistik* Heft 8-9, S. 509–516.

FHöVPR, Hrsg. (2020). *Modulhandbuchdes Bachelorstudienganges nach § 12 PolLaufbVO M-V*. Fachhochschule für öffentliche Verwaltung Polizei und Rechtspflege des Landes Mecklenburg-Vorpommern, Fachbereich Polizei.

FHVD, Hrsg. (2018). *Polizeivollzugsdienst (B.A.) - Kriminalpolizei - modularisiertes Curriculum*. Altenholz: Fachhochschule für Verwaltung und Dienstleistung.

Frank, Gudrun (2019). „Digitalisierung und Kompetenzwandel – Erfolg durch Transformation: Das 5-K-Prinzip“. In: *Gestaltung und Management der digitalen Transformation : Ökonomische, kulturelle, gesellschaftliche und technologische Perspektiven*. Hrsg. von Ronny Alexander Fürst. Wiesbaden: Springer Fachmedien Wiesbaden, S. 311–328.

Freiling, Felix (2020). *When a smart toaster can become an alibi*. URL: https://www.fau.eu/2020/02/24/news/research/when-a-smart-toaster-can-become-an-alibi/ (besucht am 09. 11. 2020).

Freiling, Felix und Konstantin Sack (2017). „Zur Authentizität und Integrität bei (digitalen) Beweismitteln“. In: *Festgabe Institut für Recht und Technik: Erlanger Festveranstaltungen 2011 und 2016*. Hrsg. von Klaus Vieweg. Köln: Carl Heymanns Verlag, S. 319–337.

Frings, Christoph und Jürgen Zeitner (2019). „Die Neukonzeption der Polizeiausbildung in Nordrhein-Westfalen: Qualitätssteigerung im Bereich der Kriminalitätsbekämpfung“. In: *Die Kriminalpolizei* Heft 1, S. 15–19.

Gärtner, Nathalie und Patrick Wallimann (2020). „Mobilforensik“. In: *Kriminalistik* Heft 3, S. 192–197.

Ghermann, Diana und Mareike Neumann (2019). „Wirtschaftskriminalität im digitalen Zeitalter“. In: *Kriminalistik* Heft 8-9, S. 535–539.

Gollmann, Dieter (2011). *Computer Security*. 3rd ed. Chichester: John Wiley und Sons.

Gottschalk, G. u. a. (1971). „Systemtheorie in der Analytik“. In: *Fresenius' Zeitschrift für analytische Chemie* 256.4, S. 257–270.

Grabowski, Tobias (2018). „Vernetzte Fahrzeuge: Neue Ermittlungsansätze im Strafverfahren?“ In: *Kriminalistik* Heft 4, S. 208–215.

Hahn, Alexander (2017). „Der Smart-Ort als Tatort - wie neue digitale Spuren die Ermittlungsarbeit verändern“. In: *Die Kriminalpolizei* Heft 3, S. 4–7.

Hassan, Nihad A. und Rami Hijazi (2018). *Open Source Intelligence Methods and Tools*. Berkeley, CA: Apress.

Hechenleitner, Andrea und Karin Schwarzkopf (2006). *Kompetenz ...mehr als nur Wissen!* München: Staatsinstitut für Schulqualität und Bildungsforschung.

Hering, Andreas und Antonio Vera (2020). „Polizei 4.0 und digitale Arbeitswelt". In: *Management und Organisation in der Polizei : Studien zu Digitalisierung, Change Management, Motivation und Arbeitsgestaltung*. Hrsg. von Rolf Ritsert und Antonio Vera. Wiesbaden: Springer Fachmedien Wiesbaden, S. 199–260.

Heyse, Volker (2014). „Entwicklung von Schlüsselkompetenzen in deutschen Hochschulen. Bilden deutsche Hochschulen wirklich kompetente Fachleute aus?" In: *Aufbruch in die Zukunft - Schlüsselkompetenzen in Schulen und Hochschulen*. Hrsg. von Volker Heyse. Münster: Waxmann Verlag GmbH, S. 202–213.

HfPV, Hrsg. (2016). *Vorbemerkungen zu den Studiengängen Bachelor of Arts Schutzpolizei und Kriminalpolizei*. Wiesbaden: Hessische Hochschule für Polizei und Verwaltung.

Hoch, Martin (2019). „Das Internet Der Dinge - Alles vernetzt?!" In: *Kriminalistik* Heft 11, S. 635–640.

Hochschule der Polizei Rheinland-Pfalz, Hrsg. (2018). *Curriculum der Hochschule der Polizei Rheinland-Pfalz im Bachelorstudiengang Polizeidienst*. Büchenbeuren: Hochschule der Polizei Rheinland-Pfalz.

– (2020). *Fachgebiete Polizei*. URL: https://www.polizei.rlp.de/de/karriere/studieren-bei-der-polizei/studium/bachelorstudiengang-polizeidienst/fachgebiete (besucht am 19. 10. 2020).

Hochschule Wismar (2020). *Die Locard'sche Regel*. URL: https://it-forensik.fiw.hs-wismar.de/index.php/Locard'sche_Regel (besucht am 23. 10. 2020).

Howorka, Horst (2013). „Informationsgehalt einer Spur". In: *Kriminalistik-Lexikon*. Hrsg. von Ingo Wirth. Heidelberg: Verlagsgruppe Hüthig Jehle Rehm GmbH.

HSPV NRW, Hrsg. (2020). *ModulhandbuchBachelorstudiengang PVD 2016*. Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen.

IBM Institute for Business Value (2016). *Digital Reinvention in action - What to do and how to make it happen*. Somers. URL: https://www-01.ibm.

com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03752USEN (besucht am 14. 10. 2020).

Inman, Keith und Norah Rudin (2000). *Principles and Practice of CRIMINALISTICS - The Profession of Forensic Science*. Boca Raton: CRC Press LLC.

Jaeger, Rainer (2019). „Digitalisierung der Polizeiarbeit - Wo stehen wir und wie geht es weiter?“ In: *der kriminalist* Heft 3, S. 20–25.

Jäger, Roland (2020). *Das BKA, der humpelnde Patient*. URL: https://www.mdr.de/sachsen-anhalt/magdeburg/magdeburg/reportage-siebter-tag-prozess-halle-attentaeter-bka-der-humpelnde-patient100.html (besucht am 16. 11. 2020).

Jaquet-Chiffelle, David-Olivier (2014). „Digital Forensics - Betrachtungen zu einer neuen Disziplin“. In: *Kriminalistik* Heft 3, S. 188–190.

Jasch, Michael (2019). „Kritische Lehre und Forschung in der Polizeiausbildung“. In: *Polizei und Gesellschaft*. Hrsg. von Christiane Howe und Lars Ostermeier. Wiesbaden: Springer Fachmedien Wiesbaden, S. 231–250.

Karpfinger, Christian und Hubert Kiechle (2010). „Signaturverfahren“. In: *Kryptologie*. Wiesbaden: Vieweg+Teubner, S. 209–218.

Kattwinkel, Oliver (2018). *Eine Einführung in das Themengebiet der Kryptowährungen*. Techn. Ber. Sankt Augustin.

Kawelovski, Frank (2018). *KRIMINALTECHNIK für Studierende und Praktiker*. Mülheim an der Ruhr: Kawelovski Eigenverlag.

Klein, Manfred (2020). *Hessen startet Kriminalpolizei-Studium mit Vertiefungsrichtung Cyberkriminalistik*. URL: https://www.egovernment-computing.de/hessen-startet-kriminalpolizei-studium-mit-vertiefungsrichtung-cyberkriminalistik-a-925307/ (besucht am 09. 11. 2020).

Korinth, Corinna (2019). „Absolvent der Hochschule legt Kriminellen im Internet das Handwerk“. In: *der kriminalist* Heft 10, S. 16–18.

Krcmar, Helmut (2018). „Charakteristika digitaler Transformation“. In: *Digitale Transformation: Fallbeispiele und Branchenanalysen*. Hrsg. von Gerhard Oswald und Helmut Krcmar. Wiesbaden: Springer Fachmedien Wiesbaden, S. 5–10.

Kretschmer, Michael (2019). „Globale Trends und ihre Auswirkungen auf die Polizeiarbeit“. In: *Zukunft der Polizei: Trends und Strategien*. Hrsg. von Hans-Jürgen Lange, Thomas Model und Michaela Wendekamm. Wiesbaden: Springer Fachmedien Wiesbaden, S. 35–45.

Kunze, Dirk (2018). „Basiskompetenzen im Bereich Cybercrime und digitale Spuren“. In: *Digitale Polizeiarbeit: Herausforderungen und Chancen*. Hrsg. von Thomas-Gabriel Rüdiger und Petra Saskia Bayerl. Wiesbaden: Springer Fachmedien Wiesbaden, S. 161–181.

Kutscha, Martin (2006). „Polizeihoheit der Länder“. In: *Wörterbuch zur Inneren Sicherheit*. Hrsg. von Hans-Jürgen Lange. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 229–232.

Küveler, Gerd und Dietrich Schwoch (2007). *Informatik für Ingenieure und Naturwissenschaftler 2*. Wiesbaden: Friedr. Vieweg & Sohn Verlag, GHV Fachverlage GmbH.

Landeskriminalamt Baden-Württemberg (2017). *Jahresbericht 2016 Cyberkriminalität und digitale Spuren*. Stuttgart: Landeskriminalamt Baden-Württemberg.

Landesportal Schleswig-Holstein (2019). *Wir können mithalten*. URL: https://www.schleswig-holstein.de/DE/Landesregierung/IV/_startseite/Artikel2019/III/190801_Cybercrime.html (besucht am 12. 11. 2020).

Lange, Hans-Jürgen, Thomas Model und Michaela Wendekamm, Hrsg. (2019). *Zukunft der Polizei*. Forum für Verwaltungs- und Polizeiwissenschaft. Wiesbaden: Springer Fachmedien Wiesbaden.

Lévesque, Veronika und Cornelia Vonhof (2018). „Komplexität, VUKA und andere Schlagworte – was verbirgt sich dahinter?“ In: *Agile Verwaltung: Wie der Öffentliche Dienst aus der Gegenwart die Zukunft entwickeln kann*. Hrsg. von Martin Bartonitz u. a. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 15–22.

Locard, Edmond (1930). *Die Kriminaluntersuchung und ihre wissenschaftlichen Methoden*. 2. Auflage. Berlin: Kameradschaft Verlagsgesellschaft.

Ludewig, Franziska und Günther Epple (2020). „Open Source Intelligence (OSINT) zur Einsatzbewältigung der Polizei“. In: *Kriminalistik* Heft 7, S. 457–461.

Lyle, James, Steven Mead und Kelsey Rider (2007). „Disk Drive I/O Commands and Write Blocking“. In: *Advances in Digital Forensics III*. Hrsg. von Philip Craiger und Sujeet Shenoi. New York: Springer, S. 163–177.

Mabey, Mike u. a. (2018). „Challenges, Opportunities and a Framework for Web Environment Forensics“. In: *Advances in Digital Forensics XIV*. Hrsg. von Gilbert Peterson und Sujeet Shenoi. Cham: Springer International Publishing, S. 11–33.

Mahnken, Julia Katherina (2020). *Welche Auswirkungen hat die digitale Transformation für die Aufgaben und Ausrichtung der Kriminalpolizei?* Bochum: Bisher unveröffentlichte Masterarbeit, Ruhr-Universität Bochum.

Manske, Mirko (2020). „Crime-as-a-Service: Die Neun Säulen - Eine Phänomenbeschreibung“. In: *Kriminalistik* Heft 4, S. 235–239.

Martini, Ben, Quang Do und Kim-Kwang Raymond Choo (2015). „Mobile cloud forensics“. In: *The Cloud Security Ecosystem*. Hrsg. von Ryan Ko und Kim-Kwang Raymond Choo. Syngress, an Imprint of Elsevier, S. 309–345.

Meier, Stefan (2016). „Digitale Forensik in Unternehmen“. Diss. Universität Regensburg.

Meinel, Christoph und Harald Sack (2012). *Internetworking*. X.media.press. Berlin, Heidelberg: Springer Berlin Heidelberg.

Metropolnews (2020). *Polizei beschlagnahmt Krypto im Wert von 30 Millionen US-Dollar vom Betreiber einer Streamingseite*. URL: https://www.metropolnews.info/mp479992/polizei-beschlagnahmt-krypto-im-wert-von-30-millionen-us-dollar-vom-betreiber-einer-streamingseite (besucht am 09. 12. 2020).

Meyer-Goßner, Lutz und Bertram Schmitt (2018). *Strafprozessordnung - mit GVG und Nebengesetzen*. München: Verlag C. H. Beck oHG.

Ministerium des Innern und für Sport Rheinland-Pfalz (2020). *Bekämpfungsstrategie gegen Cyberkriminelle*. URL: https://www.polizei.rlp.de/de/aufgaben/kriminalitaet/kriminalitaetsbekaempfung/cybercrime/rund-um-cybercrime/bekaempfungsstrategie (besucht am 03. 12. 2020).

Ministerium für Inneres Digitalisierung und Migration Baden-Württemberg (2020a). *Über uns - Polizeipräsidium Aaalen*. URL: https://ppaalen.polizei-bw.de/ueber-uns (besucht am 06. 11. 2020).

– (2020b). *Virtuelle Kriminalität Cybercrime*. URL: https://im.baden-wuerttemberg.de/de/sicherheit/polizei/kriminalitaetsbekaempfung/cybercrime (besucht am 03. 12. 2020).

Mohr, Jörg, Hrsg. (2015). *Modulhandbuch für den Bachelorstudiengang (B.A.) Kriminalvollzugsdienst im Bundeskriminalamt*. Wiesbaden: Hochschule des Bundes für öffentliche Verwaltung.

Momsen, Carsten (2015). „Digitale Beweismittel aus Sicht der Strafverteidigung“. In: *Cybercrime and Cyberinvestigations*. Hrsg. von Eric Hilgendorf und Susanne Beck. 1. Auflage. Baden-Baden: Nomos Verlagsgesellschaft, S. 67–91.

Müller, René (2013). „Recovering Traces: Windows“. In: *Grundlagen der IT-Forensik, Bericht 2013-01*. Hrsg. von Gabi Dreo u. a. Neubiberg: Universität der Bundeswehr München, Institut für technische Informatik, S. 33–52.

Mundt, Thomas (2020). *Projekt EMERGE IoT - Entwicklung von Kompetenzen, Methoden und Werkzeugen für zukunftsorientierte Ermittlungen und Ermittlungsunterstützung im Internet of Things*. URL: https://www.emerge-iot.de (besucht am 10. 11. 2020).

National Museum of American History (2004). *Vote: The Machinery of Democracy - Florida 2000*. URL: https://americanhistory.si.edu/vote/florida.html (besucht am 17. 10. 2020).

Niedersächsisches Ministerium für Inneres und Sport (2020). *Cybercrime*. URL: https://www.mi.niedersachsen.de/startseite/themen/innere_sicherheit/polizei_niedersachsen/kriminalitatsbekampfung/cybercrime/cybercrime-139122.html (besucht am 03. 12. 2020).

NIJ (2019). *Digital Evidence and Forensics*. URL: https://nij.ojp.gov/digital-evidence-and-forensics (besucht am 01. 11. 2020).

NIST (2013). *Federal Inf. Process. Stds. (NIST FIPS) - 186-4: Digital Signature Standard (DSS)*. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf (besucht am 29. 10. 2020).

Pawlaszczyk, Dirk (2017). „Digitaler Tatort, Sicherung und Verfolgung digitaler Spuren“. In: *Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*. Hrsg. von Dirk Labudde und Michael Spranger. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 113–166.

Perske, Jörn (2020). *Polizei-Nachwuchs hat wenig Interesse an Cyberkriminalistik*. URL: https://www.hessenschau.de/panorama/studiengang-verschoben-polizei-nachwuchs-hat-wenig-interesse-an-cyberkriminalistik,polizei-cyberkriminalistik-100.html (besucht am 09. 11. 2020).

Pientka, Monika und Norbert Wolf (2017). *Kriminalwissenschaften I*. 3. Auflage. München: Verlag C. H. Beck oHG.

Plank, Holger (2017). *Gesamte Strafrechtswissenschaft - Ein fallanalytischer Diskurs am Beispiel eines Kriminalromans, Reihe Bochumer Schriften zur Rechtsdogmatik und Kriminalpolitik, Band 40*. Holzkirchen: Felix-Verlag.

– (2020). „Bedürfen Cyberstrafrecht und Cyberkriminologie der Fortentwicklung? Eine Betrachtung im Spannungsfeld von Dogmatik, Kriminalpolitik und evidenzbasierten Kriminalwissenschaften“. In: *Kriminalistik und Kriminologie*

in der VUCA-Welt – Herausforderungen, Entwicklungen und Perspektiven, Band 105 der Rothenburger Beiträge. Hrsg. von Ralph Berthel. Rothenburg/Oberlausitz, S. 1–74.

Polizeiakademie Niedersachsen, Hrsg. (2019). *Modulhandbuch Bachelorstudiengang Polizeivollzugsdienst (B.A.)* Nienburg/Weser: Polizeiakademie Niedersachsen.

Pollitt, Mark M. (2007). „An Ad Hoc Review of Digital Forensic Models“. In: *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*. IEEE, S. 43–54.

Reiser, Hans P., Noëlle Rakotondravony und Johannes Köstler (2017). *Mikromodul 8003: Grundlagen von Cloud-Forensik*. 1. Auflage. Passau: Universität Passau, Fakultät für Informatik und Mathematik.

Rohleder, Bernhard (2020). *Das intelligente Zuhause: Smart Home 2020*. Berlin: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.

Rosenstiel, Lutz von (2004). „Rollen in Organisationen aus psychologischer Sicht“. In: *Strategisches Kompetenzmanagement. Von der Strategie zur Kompetenzentwicklung in der Praxis*. Hrsg. von Lutz von Rosenstiel, Dirk Pieler und Peter Glas. Wiesbaden: Gabler, S. 94–113.

Rossberger, Robert (2019). „Digitale Transformation: Kultur, Strategie und Technologie“. In: *Gestaltung und Management der digitalen Transformation : Ökonomische, kulturelle, gesellschaftliche und technologische Perspektiven*. Hrsg. von Ronny Alexander Fürst. Wiesbaden: Springer Fachmedien Wiesbaden, S. 19–36.

Rückert, Christian (2020). „Herausforderungen der Digitalisierung für das Strafverfahren“. In: *Digitalisierung und Strafverfahren - Beiträge zum Strafrecht*. Hrsg. von Jochen Bung u. a. Band 5. Baden-Baden: Nomos Verlagsgesellschaft, S. 9–38.

Rüdiger, Thomas-Gabriel und Petra Saskia Bayerl, Hrsg. (2018). *Digitale Polizeiarbeit*. Wiesbaden: Springer Fachmedien Wiesbaden.

Salim, Ahmad S. und Asmaa A. Abdalla (2019). „The determination of identity and uniqueness of color laser printouts of Ricoh® brand by Adobe® Creative Cloud Photoshop® 2018“. In: *Egyptian Journal of Forensic Sciences* 9.1, S. 40.

Schäfer, Christian und Christiane Schnell (2020). „Professionalisierung durch Akademisierung?“ In: *Kriminalistik* Heft 5, S. 341–346.

Schmitz, Lothar u. a. (2005). „Langzeitarchivierung“. In: *Informatik-Spektrum* 28.6, S. 489–492.

Schneider, Bernhard (2015). „Big Data und die vierte technische Revolution - Fluch oder Segen für die Polizeiarbeit?“ In: *der kriminalist* Heft 4, S. 17–20.

Schulz, André (2018). *Aufgaben und Tätigkeiten von Kriminalist*innen in Deutschland - Eine empirische Bestandsaufnahme und Bewertung, Bochumer Schriften zur Rechtsdogmatik und Kriminalpolitik ; Band 48*. Holzkirchen: Felix-Verlag.

Schulze, Ronald und Dirk Pawlaszczyk (2018). „Digitales Gold - Bitcoins als neue Herausforderungen in der polizeilichen Fallarbeit“. In: *der kriminalist* Heft 1-2, S. 30–31.

Schümchen, Werner (2006). „Fachhochschulen (Polizeiausbildung)“. In: *Wörterbuch zur Inneren Sicherheit*. Hrsg. von Hans-Jürgen Lange. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 78–87.

Süptitz, Thomas, Christine Utz und Torsten Eymann (2013). „State-of-the-Art: Ermittlungen in der Cloud“. In: *Datenschutz und Datensicherheit - DuD* 37.5, S. 307–312.

Taylor, M. u. a. (2010). „Digital evidence in cloud computing systems“. In: *Computer Law & Security Review* 26.3, S. 304–308.

Tecklenborg, Tim und Alexandra Stupperich (2018). „Häuser mit Smart Home“. In: *Kriminalistik* Heft 4, S. 203–207.

Voigt, Kai-Ingo u. a. (2018). „Industrie 4.0 aus Perspektive der nachhaltigen industriellen Wertschöpfung“. In: *Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht: 2. Band: Wissenschaft und Recht*. Hrsg. von Christian Bär, Thomas Grädler und Robert Mayr. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 331–343.

Wackernagel, Udo und Christian Graßie (2021). „Die Beauftragung von IT-Forensikern im Ermittlungsverfahren : Zulässige Sachverständigenbeauftragung oder unzulässiges Outsourcing originärer Ermittlungstätigkeit?“ In: *Neue Zeitschrift für Strafrecht (NStZ)* Heft 1, S. 12–18.

Wang, Qian, Michael D. Myers und David Sundaram (2013). „Digital Natives and Digital Immigrants“. In: *Business & Information Systems Engineering* Heft 6, S. 409–419.

Watson, Steve und Ali Dehghantanha (2016). „Digital forensics: the missing piece of the Internet of Things promise“. In: *Computer Fraud & Security* 2016.6, S. 5–8.

Weinert, Franz (2002). *Leistungsmessungen in Schulen*. Weinheim: Beltz.

Wenzel, Henning (2016). „Rechtliche Grundlagen der IT-Forensik“. In: *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)* Heft 3, S. 85–93.

Wieczorek, Niklas (2018). *LKA plant Einheit für Digitale Spuren*. URL: https://www.kn-online.de/Nachrichten/Schleswig-Holstein/Cybercrime-LKA-Schleswig-Holstein-will-Kompetenzzentrum-Digitale-Spuren (besucht am 12. 11. 2020).

Wigger, Ernst (1965). *Kriminaltechnischer Leitfaden*. Schriftenreihe des Bundeskriminalamtes 61-69. Wiesbaden: Bundeskriminalamt 1965/1-3.

Wirth, Ingo (2010). *Kriminalistik Lexikon*. Heidelberg: Kriminalistik Verlag.

Witt, Kurt-Ulrich (2014). „Asymmetrische Verschlüsselung“. In: *Algebraische und zahlentheoretische Grundlagen für die Informatik*. Wiesbaden: Springer Fachmedien Wiesbaden, S. 165–180.

Zhang, Jian und Andrew Moore (2007). „Traffic Trace Artifacts due to Monitoring Via Port Mirroring“. In: *2007 Workshop on End-to-End Monitoring Techniques and Services*. IEEE, S. 1–8.

Ziercke, Jörg (2014). „Kriminalistik 2.0 - Effektive Strafverfolgung im Zeitalter des Internet aus Sicht des BKA“. In: *Kriminalistik* 1.Heft 1, S. 10–17.

Zink, Wolfgang, Kerstin Zimmermann und Mario Müller-Dofel, Hrsg. (2020). *Öffentliche Akzeptanz digitaler Technologien für die deutsche Polizei*. Frankfurt am Main: PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft.

Zirk, Wolfgang und Gottfried Vordermaier (1998). *Kriminaltechnik und Spurenkunde: Lehrbuch für Ausbildung und Praxis*. Hrsg. von Rainer Schulte. FH-Schriftenreihe Polizei. Stuttgart: Richard Boorberg Verlag.

Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, alle Ausführungen, die anderen Schriften wörtlich oder sinngemäß entnommen wurden, kenntlich gemacht sind und der Leistungsnachweis in gleicher oder ähnlicher Fassung noch nicht Bestandteil einer Studien- oder Prüfungsleistung war.

Sundhagen, 15. 07. 2021