II. Forensik digitaler Medien

Die digitale Transformation von Kultur und Gesellschaft lässt auch, wenig überraschend, Kriminalität, Kriminalistik und Forensik nicht unberührt. Tathandlungen, Tatwerkzeuge, Tatermittlungen und auch Tatorte verlagern sich natürlich nicht vollständig in den Computer und seine angeschlossenen Netzwerke, weisen aber doch zunehmend eine digitale, informationstechnische, komputationsbezogene Dimension auf. Der vernetzte Computer konstituiert ein ganzes Set neuartiger Tatortmedien und Medientatorte, zugleich erscheint die Forensik in vielerlei Hinsicht auch dort als computergestützte, wo es nicht direkt um Formen der Computer-, Internet-, Cyberkriminalität geht, die in der aktuellen Auflage des Standardwerks *Der rote Faden* als letztes Kapitel, unter »spezielle Kriminalistik« verhandelt werden.[1] Allein weil immer mehr Alltagshandlungen und Lebenswelten medientechnisch vermittelte sind, weil die rasante Ausbreitung, die erhöhte Portabilität und Mobilität digitaler Medien neuartige Kommunikate und Sozialitäten, ein komplex distribuiertes Regime der Datafizierung hervorgebracht hat, erscheint die forensische Informationsgewinnung entsprechend mittransformiert. Es entsteht, wie in Handbüchern aus dem erweiterten Praxisfeld der Computerforensik nachzulesen ist – die sich längst nicht mehr auf »Methoden klassischer Datenträgerforensik« reduzieren lässt, wie nachher noch auszuführen sein wird –, eine nicht immer

1 Peter Hirsch: »Internetkriminalität«. In: Horst Clages, Rolf Ackermann (Hg., 2019): *Der rote Faden. Grundsätze der Kriminalpraxis*, 14. Auflage. Heidelberg, C.F. Müller, S. 637-690.

einfach zu prozessierende Verschränkung, Überschreitung, Augmentierung: »Der steigende Grad der Digitalisierung zwingt Ermittlungsbehörden umzudenken, Wege zu finden, in der virtuellen und realen Welt zu ermitteln. Da die virtuelle Welt […] nicht losgelöst von der realen Welt existiert, ist es notwendig, die Informationen aus den Daten beider Welten zu verbinden, um ein vollständiges Bild einer Straftat zu erhalten.«[2]

Grundlage dafür ist, neben mobiler Konnektivität und einer ubiquitär und hintergründig operierenden Komputation, eine immer feinmaschigere, invasivere sensorische Durchdringung lebensweltlicher Teilbereiche, die mit der Entstehung permanent anwachsender, oftmals echtzeitlich prozessierter Datenspeicher einhergeht.[3] Dort liegen allerhand ›große Daten‹, in denen nicht nur vorgeblich deviante Muster erkennbar sein sollen – welche mittlerweile auch in die prognostischen Modellierungen des vorhersageal gorithmisch erzeugten *predictive policing* einfließen[4] –, sondern auch Daten, die, im Sinne der Forensik, als spurförmige auslesbar sind. Wie intelligent die über Modalitäten eines *ubiquitous computing* konstituierten *environments* wirklich sind, mag umstritten sein;[5] dass alltagsweltliche Umgebungen immer medientechnischer und informationsgesättigter werden, hingegen kaum. Eine Gegenwart, die immer mehr lebensweltliche Ereignisse und Handlungszusammenhänge immer unverzüglicher verdatet, immer granularer in technische Speicher zieht, in der Internetprotokolladressen, so-

2 Dirk Labudde, Michael Spranger: »Vorwort«. In: dies. (Hg., 2007): *Forensik in der digitalen Welt. Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*. Berlin, Springer Verlag, S. XI-XII. Hier: S. XI.

3 Vgl. Simon Rothöhler (2018): *Das verteilte Bild. Stream – Archiv – Ambiente.* Paderborn, Fink, S. 231ff.

4 Vgl. dazu Kapitel IV.

5 Vgl. Ulrik Ekman (Hg., 2012): *Throughout. Art and Culture Emerging with Ubiquitous Computing*. Cambridge/MA, MIT Press; ders., Jay David Bolter, Lily Diaz, et al. (Hg., 2015): *Ubiquitous Computing, Complexity and Culture*. London, Routledge; Adam Greenfield (2017): *Radical Technologies: The Design of Everyday Life*. New York, Verso und Florian Sprenger (2019): *Epistemologien des Umgebens. Zur Geschichte, Ökologie und Biopolitik künstlicher environments*. Bielefeld: transcript.

zialmediale Profile, geomediales *tracking* und *tracing*, multisensorische Modi des Registriert- und Lokalisiertwerdens nahezu ununterbrochen mitlaufen, bedeutet aus Sicht der Forensik zunächst schlicht: ein dramatisch erhöhtes, potenziell auch fallbezogen informatives Spurenaufkommen.

Man kann, wie immer die kulturellen, gesellschaftlichen, technischen Zäsuren im Detail zu ziehen wären, durchaus von einem Paradigmenwechsel, vielleicht sogar von einer Eskalation sprechen: Wo nahezu alle Praktiken datenproduktiv und insofern tendenziell Datenpraktiken werden, wo noch die nebensächlichsten, alltäglichsten Handlungen ein diskretes informationstechnisches Datum generieren, das irgendwie, irgendwo in den cloudförmig distribuierten Speicherarchitekturen[6] (und, wie wir dank Edward Snowden wissen, in nachrichtendienstlich aggregierten Mirror-Archiven) tatsächlich auch physisch liegt, haben Tatbeteiligte, Tatwerkzeuge, Tatabläufe nicht selten individuelle, vielfältig prozessierbare Adressen. Was sich im Zuge der Digitalisierung ausbreitet, sind Automatismen der Identifizierung, Registrierung und Adressierung, die nicht zuletzt auch neue Formen medienforensischen Rückwärtslesens ermöglichen.

Das bedeutet zunächst auch: Die Spurenlage wird distribuierter, realräumlich schwerer eingrenzbar: »Gerade das Internet und seine Dienste verändern in vielfacher Weise die Anforderung an die Spurensicherung. Der Tatort der Zukunft ist global.«[7] In aller Regel sind digitale Spuren medientechnisch infrastrukturierte. Forensik muss dann in letzter Instanz digitale Transportwege, IT-Systeme und Netzwerke lesen können, um Tatabläufen auf die Spur zu kommen. Die Rekonstruktion von Datenbewegungen, die Handlungszusammenhänge zuschreibbar, nachvollziehbar werden lassen sollen, erfordert deshalb

6 Tung Hui-Hu (2015): *A Prehistory of the Cloud*. Cambridge/MA, MIT Press.

7 Dirk Pawlaszczyk: »Digitaler Tatort, Sicherung und Verfolgung digitaler Spuren«. In: Dirk Labudde, Michael Spranger (Hg., 2007): *Forensik in der digitalen Welt. Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*. Berlin, Springer Verlag, S. 113-166. Hier: S. 164.

Zugang zu digitalen Infrastrukturen wie beispielsweise Cloud-Storage-Diensten, die in wachsendem Maße privatwirtschaftliches Eigentum sind. Das forensisch examinierte digitale Datum ist auch deshalb kein einfach zu sichernder ›Fußabdruck‹, weil dessen Informierung nicht nur von Programmen und Interfaces, sondern auch von Formaten und Datenbankstrukturen abhängt. Ohne computergestützte Hilfsmittel, hochspezialisierte Software sind digitale Spuren praktisch undechiffrierbar – ganz abgesehen von berechtigten datenschutzrechtlichen Vorbehalten, mehr oder weniger legitimen kryptografischen Digitalwerkzeugen oder dem Umstand, dass zahlreiche Datenspeicher im Kontext der expandierenden Verdatungs- und Verwertungsagenden des »Capture-Kapitalismus«[8] entstanden und insofern proprietäre, vielfach kommodifizierte sind.

Datenspuren, die potenziell forensisch auslesbar sind, entstehen in digitalen Medienkulturen überall, zu jeder Zeit – oftmals auch, aus Sicht menschlicher Handlungsträger, als *shadow data*, intentionslos, im Rücken der User:innen. Keine digitalen Spuren zu hinterlassen, ist eine Herausforderung, die enorme Medienkompetenzen verlangt. Die Verwischung von Spuren, ihre effektive, unrekonstruierbare Löschung, stellt auch für versierte Hacker:innen keine triviale Aufgabe dar. Denn Datenspuren entstehen heutzutage über eine schier endlose Reihe medientechnischer Akteure, die überdies vernetzt sind. So zeichnen nicht nur Fitnessgadgets jeden Treppenschritt, Armbanduhren Schlafrhythmen, Browser minutiöse Verlaufsprotokollgeschichten, Suchmaschinendienstleister jede Tastatureingabe, Social-Media-Plattformen jeden Klick auf jeden Like-Button, Streamdienstleister selbst noch Contentsichtungsunterbrechungen und Smartphones immerzu ihre – via *cell-identification*, *timing advance* oder *enhanced observed time difference* meist relativ genau ortbare – Position im Raum auf.

8 Till A. Heilmann: »Datenarbeit im ›Capture‹-Kapitalismus. Zur Ausweitung der Verwertungszone im Zeitalter informatorischer Überwachung«. In: *zfm – Zeitschrift für Medienwissenschaft*, H. 13, 2/2015, S. 35-47.

Zur Diagnose einer »growing sensorization of environments«,[9] zur Entstehung einer immer umfassender und differenzierter werdenden digitalen Datenspur, tragen gerade auch profane, diskret agierende Alltagsdinge bei.

Denn diese sind, ausgestattet mit miniaturisierten Mikrochips und Netzwerkzugang, mittlerweile selbst sensorisch kompetente, überaus registrierfreudige Akteure. Lautsprecher, Zahnbürsten, Garagentore, Haustüren, Backöfen, Glühbirnen sind zu vernetzten, untereinander kommunizierenden »Logjekten«[10] geworden, deren Agency sowohl mit ihrer Dauerkonnektivität als auch mit algorithmischen Routinen der Datensammlung und Datenübertragung zusammenhängt. Lorraine Dastons Hinweis, »talkativeness and thingness hang together«,[11] erfährt im Internet der Dinge – bestehend aus Dingen, deren proklamierte Intelligenz weniger in ihnen selbst als in ihrer Verbundenheit liegt[12] – eine medientechnische Objektivierung, die verständlicherweise auch von kriminalistischem Interesse ist. Dabei entstehen neue forensische Einsatzgebiete, nämlich computerforensisch examinierbare Objekte und Systeme. Als prominente Beispiele können rezente Fälle gelten, bei denen nicht lediglich rekonstruierte Bewegungsprofile von Smartphones, sozialmediale Kommunikate oder inkriminierte Bild- und Textobjekte, sondern etwa auch die bildsensorischen Akquisen smarter Kühlschränke[13] oder aufgezeichnetes Sprach- und

9 Jennifer Gabrys (2016): *Program Earth. Environmental Sensing and the Making of a Computational Planet*. Minneapolis, Minnesota UP, S. 4.

10 »Logjects are objects that have an awareness of themselves and their relations with the world and which, by default, automatically record aspects of those relations in logs.« Rob Kitchin, Martin Dodge (2011): *Code/Space. Software and Everyday Life*. Cambridge/MA, MIT Press, S. 54.

11 Daston: »Speechless«, S. 11.

12 »The real power of the concept comes not from any one of these devices; it emerges from the interaction of all of them.« Mark Weiser: »The Computer of the 21st Century«. In: *ACM SIGMOBILE Mobile Computing and Communications Review*, 3/3, 1999, S. 3-11. Hier: S. 6.

13 Adrian Lobe: »Wenn der Kühlschrank zum Kommissar wird«. In: *Neue Zürcher Zeitung*, 20.01.2017.

Geräuschmaterial, das als Assistenzsysteme vermarktete Lautsprecher doch längerfristig als gemeinhin bekannt zu speichern pflegen,[14] in Spurensicherungsberichte eingegangen sind.[15]

Immer mehr Tatorte sind so gesehen auch schlicht deshalb Medientatorte, weil kriminalistisch relevante Vorbereitungsorte, Ereignisorte, Fundorte, Feststellungsorte zunehmend von in Sensornetzwerken eingebundenen Dingen durchsetzt sind, die ihre Umgebungen observieren, capturen, informatisieren und dabei rückwärtslesbare Umgebungsdatenarchive ausbilden:

> »Products, such as clothes, vehicles, fridges, maps, houses, phones, are likely to carry a knowledge content, which not only renders them ›smart‹ but has the potential to render them capable of remembering past use and modifying themselves to facilitate future use. The physical world has become an information system formed by networks of sensors and actuators embedded in objects that have an increasingly active role in shaping the processes of their own production and are capable of creating memory architectures pertinent to their own use. In this sense, objects will become their own archive.«[16]

Je unterschiedlicher und verteilter die sensorischen Kompetenzen und Agenden, desto hochaufgelöster die darüber generierten Spurdatenbilder. Computer- oder IT-forensische Modellierung hat insofern auch die Aufgabe, die verschiedenen Datenspuren zu synchronisieren, Relationen und Lücken zu markieren. Der »objektive Befund« der Tatortsicherer bekommt es jedenfalls mit einer ganzen Reihe neuer ›Zeugen‹ zu tun, die vernetzte Geräte sind: Was weiß die smarte Glühbirne? Wie stellt sich die Lage aus Sicht des intelligenten Heizungssystems dar? Was haben die Sensoren des Kühlschranks außer nachzu-

14 Gerald Sauer: »A Murder Case Tests Alexa's Devotion to Your Privacy«. In: *wired.com*, 28.02.2017.

15 Vgl. Tim Tecklenborg, Alexandra Stupperich: »Häuser mit Smart Home«. In: *Kriminalistik*, 4, 2018.

16 Gabriella Giannachi (2016): *Archive Everything. Mapping the Everyday*. Cambridge/MA, MIT Press, S. 161.

bestellenden Milchtüten in den letzten 24 Stunden gesehen und wer befragt wie die Haustür? Einfach mal auf Verdacht an der Nachbarstür klingeln reicht jedenfalls schon lange nicht mehr. Medientechnisch betrachtet liegen die multisensorischen Spurdatenarchive der Dinge ohnehin nicht in diesen selbst, sondern in verteilten Datenbanken – und warten, sofern richterliche Beschlüsse den Strafverfolgungsbehörden entsprechende Zugriffsrechte (auch auf gespeicherte Verbindungsdaten) gewähren, auf forensisches *remote reverse engineering*.

II.I Computerisierte Verfahren und Kybernetik

Mit Blick auf die wie skizziert massiv ausgeweitete Spurenlage in digitalen Medienkulturen wäre jedoch zunächst noch zu differenzieren: zwischen digitalisierten und ›nativ‹ digitalen Spuren. Unter ersteren versteht die forensische Praxis »physische Spuren, die durch geeignete Technologien digitalisiert, analysiert und visualisiert werden können«.[17] Digitalisierte Spuren entstehen durch Vorgänge der Transcodierung, sind also grundsätzlich auch – vermittels Praktiken medienhistoriografischen Rückwärtslesens – befragbar auf die damit verbundenen »layers of transcription«, auf Akteurskonstellationen und Historizitäten digitaler Transkription.[18] So haben Verfahren und Agenden

17 Dirk Labudde: »Biometrie und die Analyse digitalisierter Spuren«. In: Dirk Labudde, Michael Spranger (Hg., 2007): *Forensik in der digitalen Welt. Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*. Berlin, Springer Verlag, S. 25-58, Hier: S. 25.

18 Lorraine Daston zufolge stellt sich die Frage nach der Transkription für alle Wissensarchive: »Long-lived scientific archives straddle media epochs and survive the transition only if the discipline succeeds in transcribing the contents from one medium to another. Astronomy is the paradigm case, with observations stretching in a chain from cuneiform tablets to papyrus rolls to parchment codices to paper books to digital database. Transcription is anything but mechanical: each moment of transcription is an occasion for commensuration of old and new disciplinary standards for reliable data – but also for loss of metadata as well as the detection of old errors or the insinuation of new ones […]. But the new, handier archives do not supplant the old ones; layers of transcription

der Digitalisierung kriminalistischer Prozesse in Deutschland eine längere Vorgeschichte, die (mindestens) bis in die vermeintlich ›prädigitalen‹ 1970er Jahre zurückreicht. Man kann sagen: Der Computer war, bevor er zum Tatwerkzeug wurde, vor allem ein Instrument der Tat- und Täteranalyse. Die kriminalistische Idee, dass mit in medientechnischer Hinsicht analogen Artefakten forensischer Tatortsicherung – man denke an fotografisch gespeicherte Reifen-, Fuß- oder Fingerabdruckspuren – digitale Datenbanken zu befüllen sind, geht hier insbesondere auf verschiedene Modernisierungsprojekte des Juristen Horst Herold zurück, der von 1971 bis 1981 das BKA leitete und dort unter anderem ein elektronisches Datenbanksystem für »Personen, Institutionen, Objekte und Sachen« (PIOS) etablierte. Ausgerichtet auf die computergestützte »Automation von Massendaten«, wird Herolds Verständnis der kriminalistischen Produktivität elektronischer Datenbanken bis heute in erster Linie mit dem im Kontext des »Deutschen Herbsts« notorisch werdenden Stichwort der »negativen Rasterfahndung«, mit Verfahren der Personenidentifizierung assoziiert.[19]

Dass Herold gleichwohl auf mehreren Ebenen über die kriminaltechnische Rationalität des Computers nachdachte, dokumentiert sein

---

simply accumulate. […] At any moment a query could send a researcher burrowing down through the layers of transcription in search of some overlooked detail that has suddenly become crucial. […] The archive is not and cannot be unchanging. But its usable past must be spliced and respliced with a mutable present in order to guarantee a usable future.« Lorraine Daston: »Introduction. Third Nature«. In: dies. (Hg., 2017): *Science in the Archive. Pasts, Presents, Futures*, Chicago, University of Chicago Press, S. 1-14. Hier: S. 10f.

19 Vgl. Hannes Mangold (2017): *Fahndung nach dem Raster. Informationsverarbeitung bei der bundesdeutschen Kriminalpolizei, 1965-1984*. Zürich, Chronos Verlag. Auch David Gugerli, der in Herold eine Art Vordenker digitaler Suchmaschinen sieht, konzentriert sich auf diesen Aspekt: »Während Ende der sechziger Jahre die Suche nach Mustern der Devianz wissenschaftlich wohlinformierte politische Maßnahmen in Aussicht stellte, erhöhte die auf ›pattern recognition‹ gestützte Systematisierung und Objektivierung polizeilicher Wissensbestände vor allem die Such- und Zugriffsmöglichkeiten auf Individuen.« David Gugerli (2009): *Suchmaschinen. Die Welt als Datenbank*. Frankfurt a.M., Suhrkamp, S. 65.

Vortrag auf der eingangs erwähnten BKA-Arbeitstagung zum »Sachbeweis«, der, so Herold, »zweifellos ein wichtiges Mittel der Verobjektivierung« sei:

> »Er wird im Rahmen kriminaltechnischer Verfahren gewonnen, unterliegt mathematischen, physikalischen, chemischen, also naturwissenschaftlichen Gesetzen und ist daher in Aufbau und Schlußfolgerung jederzeit logisch nachprüfbar. Er ist objektiv, er wertet nicht, er lügt nicht, sein Erinnerungsvermögen läßt nicht nach, er widerspricht sich nicht, wie wir dies vom Menschen kennen.«[20]

Abgesehen davon, dass die unterstellte Objektivität des »Sachbeweises« de facto von historisch variierenden (und insofern: historisierbaren) wissenschaftlichen Erkenntnisständen, von forensischen Kompetenzen des Zum-Sprechen-Bringens materieller Artefakte abhängt, ist an Herolds nachfolgenden Ausführungen vor allem interessant, welche Rolle der Computer in der »ganzheitlichen Betrachtung« der vorgetragenen kriminaltechnischen Fortschrittsgeschichte spielt, die in ein »in sich geschlossenes System der Objektivierung« münden solle, so jedenfalls die Vision.

Zunächst aber geht es um die erwähnte »Automation«: »Die Fähigkeit des Computers, mit hoher Verarbeitungsgeschwindigkeit gespeicherte Fakten mehrdimensional zu verknüpfen und mit ihnen mathematische und logische Grundfunktionen vergeßlichkeits-, ermüdungs- und stimmungsfrei durchzuführen, gibt dem Menschen ein Werkzeug in die Hand, riesige Daten- und Informationsmengen zu Ausgangsinformationen und Entscheidungen verarbeiten zu können.«[21] Dies sei bereits gegenwärtige Praxis: »Alle wesentlichen Instrumente der Kriminaltechnik sind heute bereits computerisiert und wären ohne diese Hilfestellung nicht mehr denkbar. Gaschromatografie, Massenspektrome-

20 Horst Herold: »Erwartungen von Polizei und Justiz in die Kriminaltechnik«. In: Bundeskriminalamt (Hg., 1979): *BKA-Vortragsreihe Band 24: Der Sachbeweis im Strafverfahren* (Arbeitstagung des Bundeskriminalamtes Wiesbaden vom 23. bis 26. Oktober 1978). Wiesbaden, S. 75-83. Hier: S. 77f.

21 Vgl. zum Folgenden ibid., S. 80ff.

trie, Infrarotspektografie, Elektronenmikroskop, Röntgenfeinstrukturanalyse könnten ohne Prozeßrechner nicht mehr arbeiten.« Ein praktisches Einsatzfeld bilde der computergestützte Zugriff auf den behördlich verfügbaren Datenspeicher: »Verschiedene Identifizierungen von Terroristen in diesem Jahr wären ohne computergestützte Daktyloskopie nicht möglich gewesen, da die einzelne Fingerspur in den vorhandenen Millionenbeständen nicht recherchierbar war.«

Zu diesen Beständen gehören aber auch »Sammlungen von Handschriften und Geschoßspuren«. Die medientechnische Voraussetzung für den »Einsatz computerisierter Verfahren« besteht in der digitalen Transcodierung zahlreicher Spur- und Vergleichsmaterialien, wie Herold weiter ausführt: »Im Rahmen solcher Verfahren werden Handschriften oder Geschoßspuren von einer Fernsehkamera abgetastet und die Abtastpunkte entsprechend ihrem Helligkeitswert in einer Digitalzahl kodiert. Auf diese Weise verwandelt sich jedes Bild in eine Zahlenmatrix von 250 000 Computerworten, die im Rechner gespeichert werden.« Der vorgestellte Digitalisierungsvorgang verläuft über das Einscannen ganzer »Vergleichsbibliotheken«[22] – oder medientheoretisch gesprochen: über Bilder, die (auch) Zahlen sind. Der Computer ist für Herold in erster Linie ein »Medium der Bildinformation« und sollte mit transcodierten »Fotoaufnahmen von Personen, Sachen, Beweismitteln, Waffen, Sprengkörpern, […] Tatorten« bespielt werden, weil die damit verbundenen Informationen, sobald sie als Digitalisate vorliegen, gerade auch im Hinblick auf ihre Zirkulation und Vernetzung anders prozessiert werden können: »Die Lichtbildsammlungen, die die Polizeien in aller Welt unterhalten, lassen sich in digitalisierten Werten einer Bilddatenbank abspeichern und in allen Einzelstücken

22 Heute sind diese »Vergleichsbibliotheken« forensische Teildatenbanken, auf die über das elektronische Informationssystem (INPOL) des BKA zugegriffen werden kann. Dort liegen Datensätze zu DNA-Profilen (DAD – DNA-Analysedatei), Fingerabdrücken (AFIS – Automatisches Fingerabdruckidentifizierungssystem), zu Geschoss- und Patronenhülsen (IBIS – Integrated Ballistic Identification System), zur chemischen Zusammensetzung von Automobillacken (PDQ – Paint Data Query), zu Schuhabdruckmustern (SoleMate, TreadMate) uvm. (vgl. dazu Labudde: »Biometrie«, S. 52ff.).

auf Monitoren wieder reproduzierbar machen.« Weil digitalisierte Informationen im Zuge ihrer Verdatenbankung eine Adresse erhalten, können sie vielfach versandt werden und gelangen »auf elektronischem Wege über Leitungen zum Empfänger vor Ort«.

Die Adresse ist die Voraussetzung für die Mobilität. In »großer Sach- und Geschehensnähe« soll der entstehende Informationsfluss strömen – kanalisiert durch Netzwerke, die digitalisierte Daten aggregieren und Access verteilen: »Der Zentralisation der Rechner steht dann die Dezentralisation der Apparatur gegenüber. Die Apparatur wird aus den bisherigen Zentralen gelöst und gestaffelt näher an die polizeiliche Front gerückt« – »bis an den Tatort selbst«. Dort soll, um der »Verwissenschaftlichung« Vorschub zu leisten und die Bedeutung des auf Zeugenaussagen beruhenden »subjektiven Tatbefundes« weiter zu reduzieren, die Forensik als »ermittelnde Kriminaltechnik, als eine Art spezialisierter Spurenfahndung« neu positioniert werden, »in strikter Beschränkung auf die Spuren und Fakten des gesamten Beziehungsgeflechts des Tatortraumes«. Der Tatort wird also, so die Idee, umfänglich informatisiert: zu einem aus digitalisierbaren Spurdaten bestehenden Datenraum, der Anschluss an das kriminalistische Rechenzentrum erhält.

Die solchermaßen »verobjektivierte« Tatortarbeit stellte sich Herold dabei dezidiert, gerade auch jenseits der spurmateriellen Analytik der Forensik, als forcierte Kybernetisierung der Kriminaltechnik vor. Die Hoffnung war, dass die computerisierten Informationsflüsse, bestehend aus Daten, die, weil digitalisiert, Adressen haben und beweglich sind, durch »Rückkopplung« evolvieren und »Techniken des Lernens« entwickeln würden: »[J]edes Lernen stellt sonach einen Regelkreislauf erfaßter, verarbeiteter und angewendeter Information dar, deren Qualität mit dem Zustrom von Informationen von Stufe zu Stufe steigt. Treibstoff solcher Prozesse der Selbststeuerung und Optimierung ist der ständige und beschleunigte Zustrom von Informationen.« Für die konkrete Tatortarbeit bedeutete dies weniger die Hoffnung auf eine Kleinstpartikel zum Sprechen bringende, disziplinär ausdifferenzierte Forensik, die »Sachbeweise« auch dort findet, sichert und analytisch aufbereitet, wo sich dem bloßen Auge kein oder nur wenig

unmittelbar wahrnehmbares Spurenaufkommen zeigt. Herolds Vision sollte vielmehr auch über den forensischen Nullpunkt hinweghelfen, den »spurlosen Tatort« (den es allerdings nach Locard nicht geben kann, sofern tatsächlich ein kriminalistisch adressierbarer »Kontakt« vorgelegen hat):

> »Denn der Begriff des Sachbeweises kann nicht auf Spuren oder sinnlich wahrnehmbare tatrelevante Gegenstände beschränkt bleiben, sondern muß auch die Ermittlung und den Nachweis allgemeiner Gesetzmäßigkeiten, die Rekonstruktion von Verhaltensweisen und spurloser Tatorte umfassen. Wenn bei einigen Erscheinungsformen des Verbrechens Spuren nicht zurückgelassen werden, so stellen sich gleichwohl Aufgaben der Rekonstruktion, z.B. das Nachvollziehen der Standorte, der Angriffsrichtung, der Abwehrhaltungen, Klima, Beleuchtung, oder Aufgaben der Bewertung von Wahrnehmungsfähigkeit oder Beobachtungsgabe.«

Dass es Herold entlang dieser Linie nicht mehr um eine kriminaltechnisch avancierte Forensik und auch nicht mehr nur um die Aufklärung begangener Verbrechen ging, sondern um eine »prognostische Durchdringung« des behördlichen Zentraldatenspeichers, deutet insofern den Übergang zu einer kriminologischen Vision an, die, da auf behavioristische Gesetzmäßigkeiten und prognostisch hochrechenbare Muster, auf Spurlosigkeit, Prävention und Zukünfte ausgerichtet, vielleicht ›smart‹ klingen mag, im Kern dann aber eigentlich keine forensische mehr ist.

II.2 Computerforensik

Über vier Jahrzehnte später erscheint die Vorstellung, dass es Tätern gelingt, keine Spuren zu hinterlassen, unwahrscheinlicher denn je. Nicht nur befördern die heute verfügbaren forensischen Prothesen und Verfahren auch aus mikroskopischen spurmateriellen Latenzen belastbare Evidenzen zutage. Auch die skizzierte sensortechnische Durchdringung der Lebenswelt reicht immer tiefer in »Umgebungen

im kleinen«[23] (Hans Gross) herein – zwar nicht direkt im stofflich-materiellen Sinn, aber doch im Hinblick auf kleinste Handlungsspurpartikel, die nun regelmäßig mit einem informationstechnischen Datum verbunden sind. Nochmals gesagt: Es ist die Ubiquität digitaler Sensoren und Datenspuren, die Vielzahl und Verteiltheit medientechnischer Akteure, die Umgebungsdaten capturen und speichern, die unobservierte, spurfreie Handlungsräume immer weiter reduziert. Statt zu versuchen, keine digitalen Spuren zu hinterlassen, kann es deshalb aus Täterperspektive zielführender sein, Tarnspuren absichtsvoll zu legen.

Die medientechnische Verteiltheit und Komplexität der Aktanten und Akteure, deren Datenproduktivität es aus Sicht der Kriminalpraxis zu sichern und zu examinieren gilt, hat spezifische Praktiken einer ›postklassischen‹ Computerforensik hervorgebracht, wie in entsprechenden Handbüchern nachzulesen ist: »Längst sind die zu sichernden Spuren nicht mehr nur auf die Festplatte eines Rechners beschränkt. In der modernen Fallarbeit müssen vielmehr immer häufiger auch Spuren im Internet, in der sprichwörtlichen Datenwolke oder in sozialen Netzen, verfolgt, gesichert und analysiert werden. Dem gegenüber steht die klassische Computerforensik, die, bezogen auf die Spurensicherung, primär auf einzelne IT-Systeme bzw. Datenträger abzielt.«[24] Dies gilt unabhängig davon, ob die zu ermittelnde Tathandlung selbst dem engeren Feld der Computer- und Internetkriminalität – Doxing, Cybermobbing, Ransomware etc. – zugerechnet wird oder nicht. Auch die allermeisten analogen Kapitalverbrechen stellen die Forensiker:innen vor die Aufgabe, die damit in Verbindung stehenden digitalen Spuren zu finden, zu sichern und zu analysieren.

Auch digitale Spuren sind aus Sicht der Forensik zunächst physische Spuren. Sie existieren, unabhängig von ihrer forensischen Intelligibilität, auf trägermedialer Basis. Weiterhin geht es also, wie unanschaulich auch immer, um materielle Veränderungen, technisch be-

23 Hans Gross (1904): *Handbuch für Untersuchungsrichter als System der Kriminalistik*. München, J. Schweitzer Verlag, S. 246.

24 Vgl. zum Folgenden Pawlaszczyk: »Digitaler Tatort«. Hier: S. 113.

schreibbar als »Magnetisierung auf der Oberfläche einer Festplatte«, »elektronische Wellen auf einem Datenkabel« oder auch »Ladezustand von Speicherzellen im Hauptspeicher«.[25] Die Forensik untersucht aber nicht einfach (oder nicht nur) die Materialität des Trägermaterials. Im Hinblick auf ihre Lesbarmachung bestehen digitale Spuren aus computerforensischer Perspektive vor allem aus diskreten Informationseinheiten. Mehr denn je entstehen und operieren Daten, die für die kriminalistische Ermittlung von Interesse sind, als bewegliche Kommunikate, die zwischen IT-Systemen übertragen werden. Oftmals sind derartige Daten flüchtig, schwer zu lokalisieren und zu sichern – zumal auf eine Weise, die *forensically sound*, gerichtsverwertbar ist. Gleichwohl gilt auch hier, wie betont wird, die Locard'sche Regel: »In jedem hinreichend komplexen digitalen System entstehen bei der Datenverarbeitung notwendigerweise digitale Spuren (digitales Austauschprinzip).«[26] Wo es immer weniger um die Sicherung einzelner Festplatten geht, wird örtliche Lokalisierung zum netzwerkanalytisch beschreibbaren Problem eines entgrenzten, tendenziell »globalen Tatorts«. Die IT-Forensik, die ohne eine Initialphase der Tatortsicherung prozedural und rechtlich nicht ohne weiteres konzeptualisierbar ist, geht deshalb von sogenannten »Hilfstatorten« aus, die in der Regel jenen »Ort [bezeichnen], an dem der Schaden eintritt«.

IT-forensische Tatortsicherung beginnt also, kurz gesagt, unabhängig davon, wo die menschlichen und nichtmenschlichen Handlungsträger, die als Tatbeteiligte in Frage kommen, realräumlich lokalisiert waren, als die Tat, medientechnisch vermittelt, ablief: »Die Spurensuche beschränkt sich längst nicht mehr nur darauf, die am Tatort gefundenen Datenträger zu sichern und auszuwerten. Wie selbstverständlich legen viele ihre Daten in Cloudspeichern ab, nutzen soziale Netzwerke, tauschen Dateien über Online-Tauschbörsen aus, kommunizieren

25 Dirk Labudde, Frank Czerner, Michael Spranger: »Einführung«. In: Dirk Labudde, Michael Spranger (Hg., 2007): *Forensik in der digitalen Welt. Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*. Berlin, Springer Verlag, S. 1-23. Hier: S. 9.

26 Pawlaszczyk: »Digitaler Tatort«, S. 115.

über Messenger-Dienste, nutzen ein Webmailkonto und bezahlen Waren und Dienstleistungen mit Kryptowährungen wie Bitcoins.«[27] Weil es nicht nur persistente, sondern auch semipersistente und flüchtige Daten zu sichern gilt, wird Forensik zeitkritisch. Dies gilt natürlich auch für die analoge, an realräumlichen Tatorten operierende Forensik, die Fußspuren in freiem Gelände besser vor einem Gewittereinbruch in den Ermittlungsspeicher zieht, um deren Integrität zu sichern. Im Regelwerk der IT-Forensik finden sich zwar keine Handlungsanleitungen zum Umgang mit plötzlichen Wetterumschwüngen, dafür aber eine in der »Securephase« strikt einzuhaltende *order of volatility*, deren Reihenfolge vorsieht, zuerst Netzwerkdaten und Prozessorregister (flüchtig), dann Haupt- und Cachespeicher (semipersistent) und schließlich Solid-State-Speicher (persistent) zu sichern. Ziel dabei ist stets die Erstellung einer bitgenauen Kopie (*forensic sound imaging*), was prinzipiell möglich ist, weil sich »digitale Spuren […] im Gegensatz zu physikalischen Spuren verlustfrei [duplizieren]« lassen.[28]

Dies wiederum ist aber auch deshalb eine besondere Herausforderung, weil die avisierte forensische Rekonstruktion vergangener Zustände von IT-Systemen durch die betriebsdynamische Volatilität sich laufend verändernder Aktualzustände erschwert wird. Bestimmte Daten, die im RAM-Speicher liegen, gehen bei kompletter Unterbrechung der Spannungsversorgung, die die Fluktuation des Systemzustands effektiv arretieren würde, verloren. Während die auf flüchtige Daten spezialisierte IT-forensische Sicherung im Modus Operandi der *live-response* (auch Online-Forensik genannt) abwägen muss, ob durch die Zustandsveränderungen eines nicht abgeschalteten Systems mehr relevante Daten verloren gehen als durch die Entscheidung, diesem sicherheitshalber die Stromzufuhr zu versagen, wird im zweiten Fall konsequenterweise von einer »Totanalyse« (*dead analysis*) und von »Post-mortem-Akquise« gesprochen. Bei dieser ›Obduktion‹ versucht die Forensik zwar ebenfalls, verlustfreie »Abbilddateien« des Systems zu generieren, operiert dann aber in einem Modus, in

27 Ibid., S. 118.

28 Ibid., S. 117.

dem die Sicherung – zu der im weiteren Verlauf auch kryptografische Hashfunktionen gehören, die die forensisch gesicherten Datenquellen, die nun Beweismittel sind, mittels eines »digitalen Fingerabdrucks« vor nachträglichen Manipulationseingriffen zu schützen versuchen –, nicht mehr zeitkritisch ist.

Während diese Vorgänge noch zum Feld der klassischen Computer- und IT-Forensik gezählt werden können, sofern die Analyse isolierter Datenträger ohne systematische Berücksichtigung angeschlossener Netzwerke und Datenströme im Mittelpunkt steht, gehen die gegenwärtig virulenten Operationsfelder doch darüber hinaus. Mit Blick auf die empirische Realität vernetzter Computer, auf die Vielzahl verbundener Endgeräte und IoT-Dinge, unterscheidet die Computerforensik pragmatisch zwischen »Internetartefakten«, die online sind (soziale Netzwerke, Foren, Webseiten, Webmails, Chatrooms, Cloudspeicher) und Offline-Daten (Log-Dateien, Systemprogramme, Software-Anwendungen, Browser-Cache, Nutzerdateien).[29] Aber auch mit Blick auf Netzwerkzugänge und Verbindungsdatenspuren sind physische Speichergeräte, sichergestellte Festplatten und Endgeräte – hier wird von *embedded and mobile forensics* gesprochen, was nicht nur Digitalgadgets wie smarte Uhren, sondern auch IoT-Geräte einbezieht[30] – weiter von Bedeutung, man denke beispielsweise an die Analyse von Systemdateien und Browsercachedaten (die sich in Profilunterordnern innerhalb von Nutzerverzeichnissen nicht nur finden, sondern auch wiederherstellen lassen).[31] Das gilt auch, wenngleich nochmals erheblich komplizierter, wenn der »erste Angriff« Datenspuren betrifft, die distribuiert in der Cloud liegen, weil Cloud-Storage-Dienste (wie Dropbox) üblicherweise über gespiegelte Kopien funktionieren, die in lokalen Systemen als Inhalte abgelegt und synchronisiert werden. Gleichwohl stellen die mit Memory- und Livesystemen arbeitenden Cloud-Dienste die Digitalforensik in der

29 Ibid., S. 117.

30 Vgl. Jens-Petter Sandvik: »Mobile and Embedded Forensics«. In: André Årnes (Hg., 2018): *Digital Forensics*. Hoboken, Wiley, S. 191-273.

31 Vgl. Pawlaszczyk: »Digitaler Tatort«, S. 143ff.

Praxis nicht selten vor das Problem, dass die dazugehörigen Server faktisch nicht erreichbar sind – etwa, aus Sicht deutscher Behörden, weil diese Server physisch in außereuropäischen Datenzentren stehen, die Justiz keinen effektiven Zugriff erzwingen kann und die entsprechenden Systeme »nicht einfach ausgebaut und in ein Labor gebracht werden können«.[32] Die Computerforensik würde ihre Untersuchungsgegenstände auch in Zeiten »globaler Tatorte« am liebsten weiterhin auf lokale Operationstische legen können, hat es aber zunehmend mit verteilten, de facto nur teilweise und remote zugänglichen Phänomenen wie *cloud computing* oder auch, noch komplizierter, mit virtuellen Servern zu tun.[33]

Digitale Spuren setzen sich also oftmals aus Daten zusammen, von denen etwaige Täter nicht nur nicht wollten, sondern auch nicht wussten, dass sie automatisch gesammelt und gespeichert werden. Der vernetzte Computer als Tatwerkzeug und Tatbeteiligter ist in trägermedialer Hinsicht enorm sensitiv. Weite Teile gegenwärtiger Lebenswelten sind so gesehen digital informierte Medientatorte, zumindest potenziell: Überaus informationsgesättigt, bestehend aus tiefen Speichern voller Geschichten, informatisieren sie unseren Alltag und laden zu forensischem *reverse engineering* ein. Unzählige Handlungspartikel werden registriert, allerhand Mikrospuren schreiben sich in nicht nur einen Speicher ein. Weil überall Mirror-Archive entstehen – man denke nur an vergleichsweise konventionelle digitale Kommunikate wie E-Mails, die auf zig Servern gleichzeitig liegen und sich im Normalbetrieb ständig vervielfachen[34] –, ist wenig unwiederbringlich gelöscht, fast nichts

32 Ibid., S. 148.

33 Diane Barrett, Gregory Kipper (2010): *Virtualization and Forensics. A Digital Forensic Investigator's Guide to Virtual Environments*. Amsterdam, Elsevier.

34 »The advent of digital culture has turned each one of us into an unwitting archivist. From the moment we used the ›save as‹ command when composing electronic documents, our archival impulses began. ›Save as‹ is a command that implies replication; and replication requires more complex archival considerations: where do I store the copy? Where is the original saved? What is the relationship between the two? Do I archive them both or do I delete the original? When our machines become networked, it gets more complicated.

für immer vergessen. Andererseits muss die Forensik vor dem Hintergrund eines immer umfangreicher, kleinteiliger, globaler werdenden digitalen Spuraufkommens gerade auch datenfilternd und datenreduzierend vorgehen, also versuchen, relevante von nichtrelevanten Daten zu separieren. Nur erstere gilt es digitalforensisch weiter auszuwerten (»Analysephase«) und dann im nächsten Schritt so aufzubereiten (»Präsentationsphase«), dass die entsprechenden Spurdaten als Informationen im Arbeitsspeicher konkreter kriminalistischer Ermittlungen oder auch vor Gericht einen Unterschied machen können – und das bedeutet meist auch: Die digitalen Spuren müssen in der rekonstruierten Modellversion mit nichtdigitalen (aber meist digitalisierbaren) Spuren korreliert werden.

II.3 Von der Tatortfotografie zu virtuellen Tatortumgebungen

»Die Fotografie im Dienste der Kriminaltechnik«, heißt es in *Der rote Faden*, »ist ein Fachgebiet mit langer Tradition.«[35] In der Tat: Eine Geschichte forensischer bzw. »forensigraphischer«[36] Tatortmedien

---

When we take that document and email it to a friend or professor, our email program automatically archives a copy of both the email we sent as well as duplicating our attachment and saving it into a ›sent items‹ folder. If that same document is sent to a listserv, then that identical archival process is happening on dozens – perhaps even thousands – of machines, this time archived as a ›received item‹ on each of those email systems. When we, as members of that listserv, open that attachment, we need to decide if – and then where to save it.« Kenneth Goldsmith: »Archiving Is The New Folk Art«. In: *https://poetryfoundation.org/harriet*, 19.04.2011.

35 Andreas Reich: »Kriminaltechnische Fotografie«. In: Horst Clages, Rolf Ackermann (Hg., 2019): *Der rote Faden. Grundsätze der Kriminalpraxis*, 14. Auflage. Heidelberg, C.F. Müller, S. 480-492. Hier: S. 480.

36 Vgl. zum Begriff der Forensigraphie und einem Ludwig Boltzmann-Forschungsprojekt in Graz, das sich vor allem mit der klinisch-forensischen Bildgebung im Kontext der Rechtsmedizin befasst: Reingard Riener-Hofer: »›Forensigraphie‹ – Treffpunkt zwischen Recht und Bildgebung«. In: dies., Christian Berg-

könnte, sofern es sich um eine Geschichte technischer Bildmedien handeln soll, im späten 19. Jahrhundert, mit fotografischen Praktiken der Spurensicherung einsetzen. Stephen Monteiro lässt seine Fotografiegeschichte kriminalistischer Tatortsicherung sogar bereits am Abend des 14. April 1865 beginnen – mit Aufnahmen, die der schottische Fotograf Alexander Gardner in der Präsidentenloge des Ford's Theater in Washington anfertigte, aus der der schwerverletzte Abraham Lincoln gerade abtransportiert worden war.[37] Susanne Regener verweist in diesem Zusammenhang auf ein *Handbuch der Kriminalistik* aus den 1970er Jahren, in dem behauptet wird, die ersten Tatortfotografien seien 1867 in der Nähe von Lausanne erstellt worden, beim Versuch, einen Doppelmord aufzuklären.[38] In europäischen Polizeiarchiven finden sich Artefakte der *crime scene photography* vermehrt seit den 1890er Jahren, als die Lichtbildaufnahme als Verfahren der Tatortdokumentation standardisiert wurde,[39] Fotolabors in die Behörde einziehen und »die Fotografie in forensischer Beziehung (das betrifft sowohl Spurensicherung als auch Erkennungsdienst) zum festen Bestandteil polizeilicher Arbeit ernannt wird«.[40]

Tatortfotografien sollen den Lokalaugenschein vor Ort objektivieren, den derart gespeicherten »objektiven Tatbefund« im Arbeitsspeicher der Kriminalpraxis abrufbar halten und diesen auch bildförmig

---

auer, Thorsten Schwark, Elisabeth Staudegger (Hg., 2017): *Forensigraphie. Möglichkeiten und Grenzen IT-gestützter klinisch-forensischer Bildgebung*. Wien, Jan Sramek Verlag, S. 1-44.

37 Stephen Monteiro: »Crime, Forensic, and Police Photography«. In: John Hannavy (Hg., 2009): *Encyclopedia of Nineteenth Century Photography*, Vol. 1. London, Routledge, S. 344-345.

38 Susanne Regener: »Verbrechen, Schönheit, Tod. Tatortfotografien«. In: *Fotogeschichte. Beiträge zur Geschichte und Ästhetik der Fotografie*, H. 78, 2000, S. 27-42. Hier: S. 29.

39 Vgl. Walter Menzel (2007): *Tatorte und Täter. Polizeiphotographie in Wien, 1890-1938*. Wien, Album Verlag, S. 21f. und Christine Karallus: »Spuren, Täter und Orte: Das Berliner Verbrecheralbum von 1886 bis 1908«. In: *Fotogeschichte. Beiträge zur Geschichte und Ästhetik der Fotografie*, H. 70, 1998, S. 45-54.

40 Regener: »Verbrechen, Schönheit, Tod«, S. 29.

vor Gericht mobilisierbar, adressierbar werden lassen. In den Gerichten des Deutschen Kaiserreichs war die Tatortfotografie schon Ende des 19. Jahrhunderts vereinzelt präsent, wurde dort aber zunächst lediglich eingesetzt, um Zeugenaussagen zu motivieren, wie Cornelia Vismann angemerkt hat: »Die Bilder sollten nicht für sich sprechen. Sie sollen die Prozessbeteiligten zum Sprechen bringen. Sie werden ihnen vorgehalten, so wie man ihnen polizeiliche Vernehmungsprotokolle oder andere Dokumente der Vergangenheit vorhalten kann, um eine Aussage anzuregen.«[41] Diese stets an menschliche Zeugnisakte rückgebundene Notwendigkeit der Versprachlichung begann sich ab 1903 aufzulösen, als verfahrenstechnisch entschieden wurde, dass die Fotografie in Hauptverhandlungen als Beweismittel eingesetzt werden darf. Die Tatortfotografie ermöglicht nun, medienfunktional gesprochen, eine spezifische Übertragung von »Realien«. Spuren, die am Tatort gesichert wurden, sollen ›objektiv‹, ohne zwingend vorgeschaltete sprachliche Evidenzbeiträge menschlicher Handlungsträger, in den Gerichtssaal transportiert werden können. Tatortfotografien sind so gesehen nicht nur Dokumente, sondern auch bewegliche Kommunikate. Sie zirkulieren als Spurbilder, distribuieren Wissensstände, verbinden kriminalistische und juristische Akteure, agieren auf unterschiedlichen Ebenen als Vermittler. In diesem Sinne spricht auch Vismann dem fotografischen »Spurenüberführungsmedium« die zentrale Funktion zu, »[a]ls Objekt des Augenscheins […] eine lineare Verbindung zwischen der Zeit der Tat und der Zeit des Gerichts [herzustellen]«.[42]

In Christine Karallus' Studie *Die Sichtbarkeit des Verbrechens*, die sich der »Historizität und Medialität der Tatortfotografie«[43] anhand der Bestände der Polizeihistorischen Sammlung Berlins aus den Jahren 1896-1917 widmet, wird dieser Paradigmenwechsel in der Geschichte technischer Bildmedien als »iconic turn« der Rechtsgeschichte

41 Vismann: *Medien der Rechtsprechung*, S. 186.

42 Ibid., S. 188f.

43 Christine Karallus (2017): *Die Sichtbarkeit des Verbrechens. Die Tatortfotografie als Beweismittel*. Berlin, Logos Verlag, S. 24.

verstanden. Nachgezeichnet wird dabei aber auch, wie durch den Medienwechsel die kriminalistische Tatortarbeit insgesamt transformiert wurde, »wie durch das Hinzutreten der Tatortaufnahmen Formen und Inhalte gebräuchlicher Tatortpraktiken, wie das Lokalaugenscheinprotokoll oder die Zeichnung, in das neue Rechtsmedium der Tatortfotografie wanderten und wie dieses wiederum auf die ›alten‹ Erfassungspraktiken zurückwirkte […]«.[44] Das fotografische Bild eines kriminalistisch zu erfassenden Spurenbildes – ein technisches Bild, das in der dazugehörigen Ideengeschichte selbst immer wieder als »objektives« Kontaktsignatur- und Inskriptionsmedium, kurzum: als Spur theoretisiert worden ist[45] – sei dabei, so Karallus, zum einen nicht einfach als Abbild zu verstehen, sei kein »Epiphänomen« des Lokalaugenscheins, sondern generiere einen »epistemischen Wert« sui generis, sofern »die Aufnahmen an der Sichtbarkeit einer Tatortsituation und seiner Spurenlage aktiven Anteil haben in dem Sinne, dass sie etwas zeigen, was es ohne sie nicht gäbe«.[46] Zum anderen sei der kriminalistische Evidenzwert der Tatortfotografie, ihr Status als Trägermedium einer »visuellen Wahrheit« – oder genauer: als Datenspeicher, der in der Kriminalpraxis weniger den Lokalaugenschein

44 Ibid., S. 22.

45 William J. Mitchell assoziiert die Fotografie sogar explizit mit der Tatortspur: »A photograph is fossilized light, and its aura of superior evidential efficacy has frequently been ascribed to the special bond between fugitive reality and permanent image that is formed at the instant of exposure. It is a direct physical imprint, like a fingerprint left at the scene of a crime or lipstick traces on your collar.« William J. Mitchell (1994): *The Reconfigured Eye. Visual Truth in the Post-Photographic Era*. Cambridge/MA, MIT Press, S. 24. Vgl. zum Spurenparadigma in der Fotografietheoriegeschichte allgemein Peter Geimer: »Das Bild als Spur. Mutmaßung über ein untotes Paradigma«. In: Sybille Krämer, Werner Kogge, Gernot Grube (Hg., 2007): *Spur. Spurenlesen als Orientierungstechnik und Wissenskunst*. Frankfurt a.M., Suhrkamp, S. 95-120. Zur Wissensgeschichte fotografischer Objektivität vgl. Lorraine Daston, Peter Galiston: »Das Bild der Objektivität«. In: Peter Geimer (Hg., 2002): *Ordnungen der Sichtbarkeit. Fotografie in Wissenschaft, Kunst und Technologie*. Frankfurt a.M.: Suhrkamp, S. 29-99.

46 Karallus: *Die Sichtbarkeit des Verbrechens*, S. 23.

selbst als seine zuvor an Schrift- und grafische Zeichenpraxen delegierte Protokollierung bildmedientechnisch übersetzt – zwar eingebunden in ein Netzwerk anderer Verfahrensweisen der Tatortsichtung und -sicherung, gleichwohl aber von diesen unterscheidbar: »Im Gegensatz zum anthropometrischen Signalement der Daktyloskopie oder der DNA-Analyse gewinnt die Tatortfotografie ihren Beweiswert nämlich nicht erst in Bezug auf bereits vorhandene Referenzdateien […], sondern in Hinblick auf ein Arrangement von Spuren, das ohne einen solchen Abgleich auf den Tathergang und den Täter verweisen soll.«[47]

Dass diese bildmediale Form der Herstellung kriminalpraktisch wie juristisch anschlussfähiger technischer Sichtbarkeiten bereits im 19. Jahrhundert in Horizonte der Informatisierung und Komputierbarkeit gerückt wurde, dass die Tatortfotografie tatsächlich kein Abbild einer *crime scene*, sondern ein Messdatenbild sein sollte, deuteten schon die verschiedenen Bemühungen Alphonse Bertillons an, die fotografische Spurensicherung vor Ort zu formalisieren und zu standardisieren. So entstanden nicht nur Regelwerke, die vorsahen, dass die Fotograf:innen sich von Überblicksaufnahmen zu Detailaufnahmen vorarbeiten sollten. Im Rückgriff auf photogrammetrische Messverfahren[48] sollten den Tatortaufnahmen Objektabstände und -größen, aber auch topografische Relationen als exakte Werte extrahierbar sein:

> »Bertillon contributed greatly to this field [of forensic photography] by devising metric photography – the inclusion of a measuring scale in photographs to provide a permanent record of the scale and relationship between objects at a crime scene. […] Metric photography became fundamental to such activities, employing wide-angle lenses and large plates to capture fine details while photographing at precise

47 Ibid., S. 33.

48 Zur Photogrammetrie und der Disziplin der Geodäsie vgl. Christian Heipke (Hg., 2017): *Photogrammetrie und Fernerkundung*. Berlin, Springer. Zur Geschichte fotografischer Vermessungsverfahren – insbesondere mit Blick auf Albrecht Meydenbauers *Königliche Messbildanstalt* – vgl. Herta Wolf: »Das Denkmälerarchiv der Fotografie«. In: dies. (Hg., 2002): *Paradigma Fotografie. Fotokritik am Ende des fotografischen Zeitalters*. Frankfurt a.M., Suhrkamp, S. 349-375.

> angles (often directly overhead) with measuring scales that permitted accurate computation of distances.«[49]

Die entsprechenden Entfernungs- und Verkürzungsskalen befanden sich materialiter oftmals an den Rändern der Fotokartons (Abb. II.1 und II.2). Die ästhetischen Effekte der Tatortbilder, die Ende des 20. Jahrhunderts zu ›post-bürokratischen‹ Zweitkarrieren, zu ihrer popkulturellen Zirkulation als True-Crime-Fundstücke[50] und zu verschiedenen Formen künstlerischer Appropriation führten,[51] fanden sich in der Kriminalpraxis von einem numerischen Rahmen eingehegt.

Wesentlich für diese frühen Formen der »Komputation« von Tatortfotografien waren dabei allerdings sehr wohl »Referenzdateien«, nämlich Metadaten, die die Bildgenese betrafen und in tabellarisch-schriftlicher Form mitgespeichert wurden. Katharina Sykora spricht bezüglich dieser Notizen und Vermerke von der erweiterten »deskriptiven« Datafizierung der Tatortfotografie, archiviert auf Rückseiten und Rändern konkreter Fotokartonmaterialien, die Angaben zur Ausrichtung der optischen Achsen, zu Standort und Positionierung des Objektivs, zum Einsatz von Hilfsmitteln wie Leiterstativen enthielten. Entscheidend aber sei, so Sykora, dass der kriminalistische Mehrwert fotoforensischer Tatortsicherung darüber noch hinausgehe:

> »Der deskriptiven Tatortfotografie geht es […] primär um die optische Fixierung und Speicherung von Fakten, die als Informationen in die Polizei- und Gerichtsakten Eingang finden, während die explorative Tatortfotografie zur Beweisführung beitragen will […]. Dazu aber muss sie einen Überschuss an visuellen Informationen über die räumlichen Umstände des Geschehens produzieren, aus dem dann nachträglich Indizien gewonnen werden können. Diese überschüssigen visuellen

49 Monteiro: »Crime, Forensic, and Police Photography«, S. 345.

50 Vgl. Katherine Biber (2019): *In Crime's Archive. The Cultural Afterlife of Evidence*. London, Routledge.

51 Vgl. Katharina Sykora (2015): *Die Tode der Fotografie II. Tod, Theorie und Fotokunst*. Paderborn, Fink.

> Daten müssen in eine systematische Ordnung gebracht werden, um dechiffrierbar zu sein.«[52]

Folgt man dieser Lesart, gewinnt die Tatortfotografie nach Maßgabe ihrer explorativen Ressourcen an kriminalistischer Handlungsmacht.

Der explorative Modus der kriminaltechnischen Komputierbarkeit fotografischer Tatortspurregistratur setzt im Zeitstrahl der Ermittlung vergleichsweise spät ein – und voraus, dass das technische Bild in bürokratische Protokolle, in Standards der Metadatierung und Archivierung eingebunden ist. Die metrischen Werkzeuge arbeiten am Rand der Bilder, als gleichsam extradiegetische Agenten der Verdatung, gegen das sich dem technischen Blick immer wieder als kontingent darbietende Chaos einer *crime scene* und sollen einen systematischen Weg aufzeigen, die »in der fotografischen Datenfülle aufbewahrten Spuren«[53] auslesbar, verwertbar zu machen. Forensische Tatortbildmedien sind so gesehen von Beginn an in Agenden der Datafizierung eingebunden, Bestandteil einer kriminaltechnischen Datenverarbeitung, die mit Bildern rechnet.

Auch die in aktuellen Handbüchern präskribierten Vorgehensweisen gehen von der Feststellung aus, dass Fotografie (und auch: Videografie) die »erste Sicherungsmethode von Spuren« darstellt: »Sie erfolgt so, dass die Spur, die entsprechende Kennzeichnung und der Maßstab auf der jeweiligen Abbildung erkennbar sind. Der Maßstab und die Kennzeichnung müssen für alle Dokumente einheitlich sein.« Digitale Medientechniken seien einerseits, heißt es weiter, »in allen Bereichen der polizeilichen Fachfotografie« längst Standard, andererseits bedeute dies nicht, dass die Praktiken vor Ort nicht mehr wiederzuerkennen seien: »Da sich im Grunde genommen an den eigentlichen fotografischen Aufnahmeverfahren nur die Art des Speichermediums geändert hat, bilden nach wie vor fundierte fotografische Grundkenntnisse ein wichtiges Fundament für die Beherrschung der im Rahmen der polizeilichen

52 Katharina Sykora (2009): *Die Tode der Fotografie I. Totenfotografien und ihr sozialer Gebrauch*. Paderborn, Fink, S. 502f.

53 Ibid., S. 508.

Aufgabenerfüllung angewendeten fotografischen Prozesse.«[54] So wird weiterhin empfohlen, sich dem Ereignisort, der »einmaligen, unwiederholbaren Ereignisortsituation«, von der Peripherie her anzunähern: »vom Allgemeinen zum Besonderen«, »von Außen nach Innen«. Ziel sei »eine anschauliche und logische Bildfolge«. Orientierungsaufnahmen (Weitwinkel- und Panoramaaufnahmen, mitunter auch Luftaufnahmen, die Hubschrauber und Drohnen liefern können) geben einen ersten Überblick und erfassen die erweiterte Umgebung des Tatorts, der in Übersichts- und Teilübersichtsaufnahmen, die die Dokumentation der Spurenlage leisten sollen, sukzessive zu erschließen ist. Relevante Spuren wiederum sind in Detailaufnahmen zu erfassen: »Es empfiehlt sich, von diesen Detailaufnahmen zwei zu fertigen, um die Lage der Spur auf dem Spurenträger zu dokumentieren und die Spur selbst abzubilden.«[55] Hier wird es handwerklich nochmals anspruchsvoller, etwa wenn »Eindruck- und Formspuren […] je nach Tiefe ihrer Oberflächenstruktur mit Schräglicht ausgeleuchtet« werden müssen (»je geringer die Eindrucktiefe, desto kleiner der Lichteinfallswinkel«), oder auch, wenn es beim Spurmaterial um »Farberscheinungen (Anlauffarben, Anhaftungen von Anstrichstoffen)« geht: »Dabei ist bei gleicher Beleuchtung eine Graukarte oder Farbtafel zur Farbabstimmung mit zu fotografieren.«[56]

Zu erwähnen ist auch, dass sich die fotografische Dokumentation der Spur nicht auf den Tatort beschränkt. Gegebenenfalls können auch kriminaltechnische Praktiken der Studiofotografie zum Einsatz kommen: »Latente oder schwach sichtbare Spuren auf transportablen Spurenträgern, Tatwerkzeugen, Kleidungsstücken, Schusswaffenspuren, Nachschließspuren in Schlössern, umstrittene Dokumente und Schreibleistungen, Mikrospuren, unbekannte Substanzen und vieles andere werden nach der Ereignisortdokumentation unter Studiobedingungen fotografisch gesichert und im Labor zum Teil individuell

54 Roll: »Kriminalistische Tatortarbeit«, S. 109.

55 Ibid.

56 Reich: »Kriminaltechnische Fotografie«, S. 483f.

bearbeitet.«[57] Grundsätzlich ist jede einzelne Spur im Tatortbefundbericht zudem näher zu beschreiben (Art der Spur, Auffindort, Spurenträger, Merkmale, Besonderheiten wie Fremdsubstanzen in der Spur und Überlagerungen) und mittels einer mitfotografierten Nummerntafel individuell zu kennzeichnen. Erst dann (und nur so) kann sie zirkulieren, eine Adresse in Aktenläufen werden. Es sind diese Ziffern, die das Spurmaterial nachhaltig bürokratisieren – und sicherstellen, dass die Spur bei aller Beweglichkeit – im polizeilichen Arbeitsspeicher der Ermittlungen wie vor Gericht – mit sich selbst identisch, adressierbar bleibt.

Bildgebende Verfahren und Praktiken der Tatortsicherung haben von Beginn an, wie Katharina Sykora zu Recht angemerkt hat, jedoch nicht nur die Funktion, »deskriptiv« zu dokumentieren, was bei der Ereignisortbegehung auch ohne technische Hilfsmittel wahrgenommen werden kann. Die »explorative« Dimension[58] hat einerseits mit jenem ›prothetisch‹ erweiterten Vermögen technischer Bildmedien zu tun, von dem Hans Gross im *Handbuch der Kriminalistik* bereits 1904 spricht:

> »Wenn nun der Weitwinkel-Apparat zwei Wände eines Zimmers […] *zugleich* faßt, so gibt dies ein Bild, welches wir noch nie gesehen haben, weil wir soviel auf einmal in der Natur niemals sehen *können*, das Bild ist fremd und wird nun als ›unrichtig‹ bezeichnet, obwohl alle Gegenstände *einzeln* richtig und deutlich wiedergegeben sind. Das Mikroskop und das Fernrohr zeigt auch mehr, als wir mit freiem Auge sehen, das Gezeigte ist aber nicht unrichtig.«[59]

Zum anderen aber hängt das »explorative« Potenzial des erstellten Tatortbefunddatenspeichers von den jeweiligen Ermittlungsständen ab,

57 Ibid., S. 486.

58 Die Begriffe »deskriptiv« und »explorativ« finden auch in *Der rote Faden* in dieser Form Verwendung (siehe ibid., S. 480).

59 Gross: *Handbuch für Untersuchungsrichter*, S. 265. Vgl. dazu Regener: »Verbrechen, Schönheit, Tod«.

hat also eine zeitliche, sich dynamisch verändernde Komponente, die mit der konstitutiven Nachträglichkeit der Forensik zusammenhängt.

Die im Grunde seit der Etablierung forensischer Bildgebung mitlaufende Vorstellung, der zufolge gerade den bildförmig gespeicherten Anteilen des Spurensicherungsberichts die Aufgabe zukommt, den Ereignisort einer Tat im Hinblick auf spätere Konsultationen fest- und zugänglich zu halten, hat mit rezenten 3D-Verfahren der sogenannten »virtuellen Tatortdokumentation« eine erweiterte medientechnische Umsetzung erfahren, die seit Mitte der Nullerjahre auch in der Praxis vermehrt zum Einsatz kommt. Verbunden damit ist eine Aufwertung des Sachgebiets »Tatortvermessung«, das nun über neuartige forensische Dokumentationsmedien verfügt. In einem der ersten Erfahrungsberichte zur Technologie im deutschsprachigen Raum, publiziert in der Fachzeitschrift des Bundes deutscher Kriminalbeamter *Der Kriminalist*, beschreibt Arnd Voßenkauf (LKA NRW) den Medienwechsel in seinem Sachverständigenbereich folgendermaßen:

> »Wir als Tatortvermessungsspezialisten waren seit einigen Jahren auf der Suche nach einer Möglichkeit, Tatortarbeit effizienter, präziser und dokumentationssicherer zu machen, als wir das bisher konnten. Bis zur Beschaffung des Laserscanners wurden Tatorte von uns photogrammetrisch (RolleiMetric), tachymetrisch (Winkel-Streckenmessung) oder ganz banal mit Zollstock, Messband und Laserdisto vermessen. Letzteres kann bekanntlich jeder Heimwerker in einem Baumarkt erwerben. Auf dieser Suche nach neuen, schnelleren und weniger bearbeitungsintensiven Methoden stießen wir schließlich auf eine innovative Technik, die bis dato nur ›polizeifremd‹ z.B. in der professionellen Vermessungstechnik und in der Architektur genutzt wurde: Das 3D-Laserscanner-Verfahren. Mit dieser Technik kann eine Räumlichkeit innerhalb kürzester Zeit mit einer ungeheuren Präzision vermessen werden.«[60]

60 Arnd Voßenkauf: »Einsatz moderner Technologien an Tat-, Unfall- und Ereignisorten – Dokumentation mittels 3D-Laserscanning«. In: *Der Kriminalist*, 5, 2006, S. 198-204. Hier: S: 198.

Dass forensische Bildgebung im Kontext der Tatortbefundsicherung einerseits auf »deskriptive« Verdatung und Vermessung, andererseits auf Möglichkeiten einer »explorativen« Re-Vision abzielt, die weder orts- noch zeitgebunden, sondern eine beliebig abrufbare Speicherperformanz ist, findet hier eine digitaltechnische Anwendung, die den Ereignisort nicht nur granularer datafiziert (und selbst Mikrobereiche zu späteren Ermittlungszeitpunkten noch hochpräzise ausmessbar werden lässt), sondern empirische Tatorte zudem als künstliche *environments* prozessier- und emergierbar macht. Wenn Tatortmedien wie vorgeschlagen insbesondere solche sind, die sich spezifisch eignen, mit der Medialität der Tatortspur epistemisch produktiv umzugehen, dann liegt das zentrale Versprechen virtueller Tatortdokumentation auf der Hand: Was eine Spur ist und was nicht, muss nicht mehr ausschließlich vor Ort, ad hoc, im Zeitraum der noch vergleichsweise unterinformierten, manchmal gar desorientierten Erstbegehung entschieden werden – respektive nur insofern, als es nur vor Ort, im Handlungszusammenhang eines realräumlich examinierten Ereignisortes möglich ist, bestimmte Spuren in ihrer stofflichen Verfasstheit, als Materialproben für forensische Laborarbeit zu sichern.

Abgesehen davon kommt die Tatortarbeit ihrem Ziel, kriminalistisch geframte Ereignisorte in die Zukunft sich fortlaufend ändernder Ermittlungsstände zu übertragen, in gewisser Weise näher. Tatorte erscheinen hier auf anschauliche Weise als durch die Zeit reisende Container, die spurmateriell inskribierte Tatabläufe enthalten – und doch beweglich, mobilisierbar bleiben. Das »gedankliche Modell« der Ermittlung, das Telos lückenloser, maximal informationsgesättigter, ›beweissicherer‹ Rekonstruktion, erhält durch diese neuartige Form forensischer Bildgebung gewissermaßen einen virtuellen Sparringspartner, der das *reverse engineering* Schritt für Schritt medientechnisch simulierbar macht. Dabei handelt es sich um einen medialen Raum, dessen digitaltechnisch konstituierte, immer wieder neu regenerierbare computergrafische Modelleigenschaften mit tatortforensisch abgesichertem Referenzanspruch operieren. Der virtuelle Raum der Forensik ist kein futuristischer Cyberspace, aber ein hochgerechneter, für spekulative Interaktionen offener – kein beliebig entworfenes Mo-

dell, sondern ein verbindlicher Handlungsraum für kriminalistisches Rückwärtslesen, der bei aller dokumentarischen Energie, die auf den Ist-Zustand von ereignisörtlich fixierten Spurmateriallagen gerichtet wird, mit zukünftigen Ermittlungsständen rechnet: ein flexibler Möglichkeitsraum voller Spuren und Geschichten.

Im Bayerischen Landeskriminalamt (BLKA) ist für die medieninnovative Seite aktueller Kriminalpraxis die Abteilung »Zentrale Fototechnik und 3D-Verfahren« (ZFT) zuständig. Ähnliche Einrichtungen finden sich auch international, beispielsweise in der Schweiz, wo seit 2012 das 3D-Zentrum Zürich (3DZZ) betrieben wird – eine Kooperation des Instituts für Rechtsmedizin der Universität Zürich, des Forensischen Instituts, der Stadtpolizei und des Unfallfotodienstes der Kantonspolizei.[61] Im BLKA arbeiten neben Bauzeichner:innen und Fotograf:innen vor allem Geomedientechniker:innen wie Ralf Breker, der in einem Aufsatz für die Zeitschrift *Kriminalistik* mit guten Gründen dafür argumentieren kann, sein Arbeitsfeld als eigenen Sachverständigenbereich weiter auszubauen.[62] Dem kriminalistischen Anspruch, »den Tatort als Gesamtheit zu dokumentieren«,[63] wird hier in apparativer Hinsicht u.a. mit terrestrischen Laserscannern (TLS), High-Dynamic-Range-Kameras und Streifenlichtscannern Rechnung getragen.

Medienpraktisch und -technisch funktioniert dies kurz gesagt so: Die Geomedientechniker:innen werden an den Tatort gerufen, bauen den nur 10 Kilogramm schweren, also aufwandlos portablen Laserscanner 5010C der Firma Z+F auf (Abb. II.3) und führen, entsprechend der kriminalistisch festgelegten »örtlichen Komponente«, eine großflächige Erfassung des relevanten Tatortbereichs durch (zum Beispiel: einer

61 Vgl. Till Sieberth, Lars Ebert, Martin Wermuth, Jörg Arnold, Erika Dobbler: »Das 3D-Zentrum Zürich«. In: *Kriminalistik. Unabhängige Zeitschrift für die kriminalistische Wissenschaft und Praxis*, 2, 2021, S. 109-115.

62 Ralf Breker: »High-End 3D-Verfahren beim Bayerischen Landeskriminalamt«. In: *Kriminalistik. Unabhängige Zeitschrift für die kriminalistische Wissenschaft und Praxis*, 8-9, 2014, S. 522-531.

63 Roll: »Kriminalistische Tatortarbeit«, S. 110.

Wohnung, in der – Brekers und Voßenkaufs Abteilungen werden üblicherweise nur bei Kapitalverbrechen aktiviert – ein Mord stattgefunden hat; es gab aber auch schon Fälle, in denen ganze Häuser, abgebrannte Sägewerke oder Straßenzüge eingescannt wurden). Der TLS tastet die Oberflächen der mit einer Messrate von rund einer Million Pixel pro Sekunde enorm hochgeschwindigkeitssensorisch erfassten Umgebung sequentiell ab (die nominale Reichweite des Scanners beträgt 187 Meter). Mit Blick auf den Messvorgang spricht man, analog zu RADAR, von Light Detection and Ranging (LIDAR).[64] Dabei sendet der Scanner einen Laserstrahl aus, der als Messsignal auf bzw. an den Oberflächen der Umgebungstopografie reflektiert. Die Reflexionen werden als Rückstreuungen sensorisch detektiert, fortlaufend erfasst und gespeichert. Der erhobene Messwert bezieht sich sowohl auf die Laufzeit des rückgestreuten Lasersignalechos als auch auf die Rückstreustärke, was zusätzliche radiometrische Informationen zur aufgenommenen Fläche enthält.[65] Generiert wird dabei eine sogenannte Punktewolke (*point cloud*), die sich aus bis zu 30 Millionen diskreten Einzelkoordinaten zusammensetzt und einen Vektorraum beschreibt: »[Wir] ›frieren‹ den Tatort sozusagen ein. Alle erfassten Objekte sind danach lagerichtig fixiert, so dass Entfernungen, Abstände, Höhen usw. jederzeit bestimmbar sind.«[66]

Der TLS-Rohscan eines Tatorts besteht aus vielen Einzelscans, die zu einer georeferenzierten Gesamtpunktewolke synthetisiert werden. In einem räumlichen Datensatz werden 2D-Rastergrafiken durch dreidimensionale Gitter, diskrete Bildpunkte durch diskrete Gitterpunkte ersetzt. Wo rastergrafische Pixel waren, operieren nun »Voxel«

64 Vgl. Jussi Parikka: »On Seeing Where There's Nothing to See: Practices of Light beyond Photography«. In: ders., Tomas Dvorak (Hg., 2021): *Photography Off the Scale. Technologies and Theories of the Mass Image. Edinburgh*. Edinburgh UP, S. 185-210.

65 Norbert Pfeiffer, Gottfried Mandlburger, Philipp Glira: »Laserscanning«. In: Heipke, Christian (Hg., 2017): *Photogrammetrie und Fernerkundung*. Berlin, Springer, S. 431-481.

66 Voßenkauf: »Einsatz moderner Technologien«, S. 199.

als basale Bildelemente eines volumengrafisch umgesetzten XYZ-Koordinatensystems. Zur 3D-Tatortdokumentation gehört aber noch ein weiterer, komplementär ablaufender bildtechnischer Vorgang. In den Rotor des Laserscanners ist eine HDR-Spiegelreflexkamera (i-Cam) eingelassen, die Panoramahochkontrastbilder aus 80 Millionen Pixeln generiert. Notwendig ist diese zusätzliche bildsensorische Operation, die zum weit in den Konsumentenbereich hineinreichenden Feld der *computational photography* gehört, weil der Laser-Rohscan keine RGB-Farbinformationen, sondern lediglich, je nach Intensität der Oberflächenreflexion, Graustufen enthält. Beide Bilddatensätze werden automatisch, über die Z+F LaserControl-Software fusioniert, was einen topografisch präzisen und farbgetreuen 3D-Bilddatensatz ergibt, der Messgenauigkeiten im Millimeterbereich erreicht und den die bildgebende Forensik gerade auch im Hinblick auf seine kriminalpraktische Operabilität als »virtuellen Tatort« bezeichnet. Mit diesem betritt, so das Versprechen, die Kriminalistik die dritte Dimension – und zwar in Form einer medientechnischen Visualisierung, die als farbgetreue Punktewolke unmittelbar wahrnehmbare, belastbare Realitätseffekte generiert und deshalb auch vor Gericht überzeugend zur Darstellung kommen kann. Es handelt sich also um ein bildgebendes Werkzeug, das sowohl zur forensischen Dokumentation von Ereignisorten, in allen Phasen kriminalistischer Ermittlung, als auch in der sachverständigen Kommunikation im Gerichtssaal einsetzbar ist.

Vordringlich geht es aber darum, die kriminalistische Temporalität des Lokalaugenscheins vor Ort dehnbar, fungibel werden zu lassen. Denn der 3D-Datensatz (man spricht hier auch von »Volumsdaten«) ermöglicht den Ermittler:innen eine nachträgliche »virtuelle Begehung« – im ersten Schritt, um einen Überblick zu erhalten, als »Flug durch den Tatort«, wie Ralf Breker ausführt: »Der Nutzer bekommt in diesem Film einen ersten detaillierten Eindruck der Tatortörtlichkeit. Der Vorteil gegenüber einem herkömmlichen Film, aufgenommen mit einer Videokamera, besteht in der Möglichkeit für den Ersteller, jede Position im Raum einzunehmen und sich vom Aufnahmestand-

ort zu lösen.«[67] Jede Position bedeutet: innerhalb wie außerhalb der Punktewolke. User:innen können stufenlos heran- und herauszoomen. Das Softwareprodukt enthält auch eine maßstabsgetreue orthografische Ansicht: »Setzt man einen Schnitt an der Decke, beispielsweise einer gescannten Wohnung, hat man freie Sicht von ›oben‹ auf den gescannten Bereich.« Die freie Perspektivwahl geht aus der umfänglichen initialen Datenakquise hervor: »Es findet keine Selektion statt, somit werden nicht nur die Daten, die der Ersteller bzw. Ermittler dargestellt haben will, visualisiert, sondern all das, was erfasst wurde.« Bei der virtuellen Tatortdokumentation handelt es sich so gesehen um eine bildtechnologische Erfassungspraxis, die auf initiale Datenfilterung weitgehend verzichtet – und genau deshalb jenes tatortfotografische Versprechen einlöst, das Greg Siegel, mit Blick auf bildforensische Unfallaufnahmen, folgendermaßen formuliert hat: »As a ›permanent‹ storage medium [the photographic image] allows a second look, and a third look – in fact it admits an unlimited quantity of additional looks, invites a virtual infinity of forensic reviews.«[68]

Die komplementären HDR-Aufnahmen ermöglichen innerhalb des technischen Workflows einerseits die Farbgebung des 3D-Datensatzes, sind aber auch im Hinblick auf das »Erkennen kleinster Details« von Bedeutung, weil die 360°-Panoramen aufgrund des hohen Dynamikumfangs selbst in sehr hellen (etwa fensternahen) und sehr dunklen Bereichen (etwa Raumecken) voller Informationen sind, die vergrößert und genauer betrachtet werden können. Virtuelle Tatorte sind künstliche *environments*, deren Speicher allerhand »Umgebungen im kleinen« (Hans Gross) enthalten; kommen hochaufgelöste Streifenlichtscannerdatensätze hinzu, etwa zur Erfassung von Profil- oder auch Verletzungsspuren, bewegt sich die bildgebende Forensik im Submillimeterbereich.

Die beliebig oft nachbegehbaren, im Walk-Through-Modus flexibel navigierbaren virtuellen Tatortvisualisierungen ermöglichen verschie-

67 Breker: »High-End 3D-Verfahren beim Bayerischen Landeskriminalamt«, S. 523. Vgl. zum Folgenden ibid., S. 524ff.

68 Greg Siegel (2014): *Forensic Media. Reconstructing Accidents in Accelerated Modernity*. Durham, Duke UP, S. 203. Vgl. zur Unfallforensik Kapitel IV.

denste digitale Anwendungen und Auswertungen. Der LKA-Beamte Arnd Voßenkauf kann schon in seinem Erfahrungsbericht aus dem Jahr 2006, als die Technologie noch relativ unausgereift bzw. experimentell war, erste Erfolge aus der Kriminalpraxis vermelden:

> »Ein unbekannter Täter schießt von außen in eine Wohnung. Das Projektil durchschlägt die Wohnzimmerscheibe und bleibt in einer Wand stecken. Die zuständigen Kollegen beauftragten uns mit einer Schussrichtungsbestimmung. Am Tatort wurden 5 Scans gemacht und vor Ort verknüpft. Über den Durchschuss der Fensterscheibe und den Einschuss in der Zimmerwand wurde eine Linie in der Punktwolke konstruiert. Diese Linie zeigte zu der gegenüberliegenden Erdgeschosswohnung. Aufgrund dieser Vermessung, die vor Ort einschließlich der Schussrichtungsbestimmung eine Stunde dauerte, konnte für die Verdächtigenwohnung ein Durchsuchungsbeschluss erwirkt werden. Bei der daraufhin erfolgten Durchsuchung fand die Sachbearbeitung die passende Waffe.«[69] (Abb.II.5)

Aus heutiger Sicht lässt sich sagen: Nicht nur ist das dreidimensionale Laserbild eines Spurenbildes über einfache, intuitiv bedienbare Interface-Funktionalitäten ganz unmittelbar ein informatisiertes Messbild geworden, das über eingebaute Software-Tools spontane Distanzmessungen und Winkelbestimmungen zulässt. Die 3D-Datensätze sind mittlerweile auch insofern integrale, das interdisziplinär zusammengetragene forensische Tatortwissen aggregierende Datenräume – also auch: digitale Ermittlungsarchive –, als die virtuellen Raumvisualisierungen diverse Datenschnittstellen enthalten können, Tatortdokumentation, Laborergebnisse und Ermittlungswissen also als Medienverbund zusammenführen. So öffnet sich beispielsweise mit einem Klick auf ein computergrafisches Blutspurmuster ein Interface, das die dazugehörige DNA-Analyse enthält. Ein weiterer Klick auf die zu Bruch gegangene Fensterscheibe führt zur Audioaufzeichnung einer Zeugenaussage. Hinter dem virtuellen Leichnam verbergen sich diverse rechtsmedizinische Befunde, mitunter auch eine Computertomografie,

69 Voßenkauf: »Einsatz moderner Technologien«, S. 200f.

die Wundspuren oder Schussbahnen durch virtuelle Körper detailgetreu visualisiert. Die am Tatort erhobenen, im Labor ausgewerteten nichtvisuellen forensischen Daten sind hier als geschichtete Ebenen eines »virtuellen Tatortfundberichts« einprogrammiert, werden, weil der virtuelle Raum ein georeferenzierter ist, nicht nur abrufbar, sondern auch verortet: »Sachverständigengutachten der Kriminaltechnik und Rechtsmedizin, die einen räumlichen Bezug aufweisen, können visualisiert werden. Beispielsweise kann ein rechtsmedizinisches Gutachten im Bereich Luminol, eine Blutspurenverteilungsmusteranalyse, die Sicht eines Zeugen und die Schussrichtungsbestimmung der Ballistik in einem Datensatz kombiniert und dem Nutzer zur Verfügung gestellt werden.« Die angesprochenen forensischen Befunde – ballistische Schussbahnen, Sichtachsenbereiche, die per Langzeitbelichtung generierten Luminolbilder (die chemische Reaktion des fluoreszierenden Wirkstoffs, der auf Hämoglobin reagiert, führt dazu, dass auch absichtsvoll verwischte, augenscheinlich entfernte Blutspuren, abgedunkelte Umgebungsbedingungen vorausgesetzt, bläulich leuchten) – können ebenso in den 3D-Scan einmodelliert, unter Umgebungslichtbedingungen als Datenschicht dazugeschaltet werden (Abb. II.6) wie auch Infrarotaufnahmen, die Spuren außerhalb des sichtbaren Lichtspektrums registrieren:

> »Der Mehrwert dieser Technik liegt auf der Hand: Luminolbehandelte oder infrarot fotografierte Blutanhaftungen (beispielsweise Schuhprofilspuren) können nun vermessungstechnisch erfasst und eventuell einem Tatverdächtigen zugeordnet werden. Der Rechtsmediziner kann die Dynamik einer Tat viel leichter rekonstruieren, wenn die Luminolspurbefunde für ihn in 3D greifbar sind. Das Luminolverfahren wird somit auch transparenter für die Justiz und erspart dem rechtsmedizinischen Sachverständigen viele unangenehme Fragen vor Gericht.«

Einerseits dokumentiert das terrestrische Laserscanning Ereignisorte also bis in Mikrobereiche hinein und leistet dabei mitunter auch eine

»bildliche Dokumentation ansonsten unsichtbarer Informationen«.[70] Andererseits bieten virtuelle Tatortumgebungen, die auch jenseits bildsensorischer Akquisen informationsgesättigte Datenräume sind, neuartige Werkzeuge kriminalistischer Heuristik. Dies betrifft sowohl die forensische Kommunikation, die Veranschaulichung und Handhabbarmachung forensischer Befunde für konkrete Ermittlungen – etwa im Fall von Blutspurenverteilungsmusteranalysen, die nun nicht mehr umständlich analog nachgebaut werden müssen, sondern direkt in der virtuellen Tatortumgebung komputier- und visualisierbar sind:

> »Blutspurenverteilungsmusteranalysen werden schon seit geraumer Zeit von Rechtsmedizinern durchgeführt. Dazu werden relevante Bluttropfen ausgewählt und ihre ballistischen Flugbahnen durch eine einfache mathematische Formel zurück zum Ursprung berechnet. Um die Ergebnisse zu dokumentieren, werden Schnüre vom Bluttropfen zum berechneten Ursprung gespannt und fotografiert. Die wesentlich elegantere, schnellere und akkuratere Lösung ist, diese ballistischen Bahnen algorithmusbasiert, dreidimensional auf Grundlage des Laserscans zu berechnen und zu visualisieren.«[71] (Abb. II.8)

Auch lassen sich Zeugenaussagen überprüfen, indem durch realräumliche Positionierungen bedingte maximale Sichtbereiche in das Modell eingerechnet werden – visualisiert als geometrische, von einer »virtuellen Kamera« (deren Position selbst an die Körpergröße der Zeug:innen anpassbar ist) ausgehende Kegelformen (Abb. II.7).

Das »gedankliche Modell zum Ereignis« ist ein virtuell materialisierbares geworden, das nicht nur ein Maximum vernetzter und verortbarer forensischer Deskriptionsdaten enthält, sondern gerade auch

---

70 Alexander Bornik: »Integrierte, computergestützte Fallanalyse auf Basis von 3D-Bildgebung«. In: Reingard Riener-Hofer, Christian Bergauer, Thorsten Schwark, Elisabeth Staudegger (Hg., 2017): *Forensigraphie. Möglichkeiten und Grenzen IT-gestützter klinisch-forensischer Bildgebung*. Wien, Jan Sramek Verlag, S. 223-252. Hier: S. 230f.

71 Breker: »High-End 3D-Verfahren beim Bayerischen Landeskriminalamt«, S. 524ff.

»explorative« Handlungsressourcen wie die virtuelle Modellierung vorgestellter Tatabläufe zur Verfügung stellt (Abb. II.9). Denn der Horizont forensischer Ereignisdokumentation ist die Ereignisrekonstruktion. Das kann auch bedeuten, dass Objekte, von deren Existenz die Kriminalist:innen nur durch Zeugenaussagen wissen, genauso in das virtuelle Modell einprogrammiert werden, wie meteorologische Informationen, die historischen Wetterdatenbanken entnehmbar sind, zu tatzeitspezifischen Lichtverhältnisberechnungen führen können.[72] Selbst Vorbehalte, offene Fragen, Hypothesen sind gewissermaßen virtualisierbar, zumindest im Virtuellen markier- und gestaltbar, wie die Gruppe des 3DZZ berichtet:

> »Bei Rekonstruktionen gilt es zu beachten, dass Unsicherheiten, die zum Beispiel aus Zeugenaussagen resultieren, gut gekennzeichnet und verständlich visualisiert werden, um nicht den Anschein ›der einen Wahrheit‹ zu erzeugen. Diese Unsicherheiten können z.B. durch Pufferzonen um Objekte herum visualisiert werden, oder durch Variationen in der Rekonstruktion, die sich durch die verschiedenen Spuren oder Spureninterpretationen ergeben können. 3D-Rekonstruktionen ermöglichen es, verschiedene Hypothesen aus dem schriftlichen Gutachten zu visualisieren und auf Plausibilität zu überprüfen. Sie bilden eine Basis für alle Parteien, die als gemeinsame Ausgangslage genutzt werden kann. Damit können Missverständnisse in der gerichtlichen Diskussion minimiert werden.«[73]

Auch Tatverdächtige, die, wenn die Kriminaltechniker:innen am Tatort eintreffen, diesen üblicherweise meist verlassen haben, können als Avatare ihrer selbst in die virtuellen Modelle transferiert werden. Der virtuelle Tatort hat eine spielerische, man könnte auch sagen ›gamifizierte‹ Seite, die nicht nur retrospektive Erkundungen, sondern auch Testläufe heuristisch vorgestellter Tatabläufe umsetzbar macht. Nicht nur können Ereignisorte und Objekte – von Schlafmitteltabletten bis zu

72 Vgl. *https://www.suncalc.org/*und *https://worldview.earthdata.nasa.gov*.

73 Sieberth et al.: »Das 3D-Zentrum Zürich«, S. 112.

ganzen Flugzeugen – lasermesstechnisch erfasst und virtuell materialisiert werden. Mittlerweile besteht auch die Option, die Tatbeteiligten selbst einzuscannen. Ganzkörperscanner wie Artec 3D sind Strukturlichtscanner – und, so Breker, die Zukunft forensischer Fototechnik:

> »[Wir] werden zukünftig mehr und mehr dazu übergehen, Tatverdächtige (wenn vorhanden) einzuscannen. Nach diversen Nachbearbeitungsschritten gibt die Artec Software ein hochgenaues texturiertes Flächenmodell (Mesh) der Person aus. Dieses kann in die Software 3ds max eingelesen und mit virtuellen Gelenken ausgestattet werden. Somit ist es also möglich, den Tatverdächtigen mit seinen der Realität entsprechenden Körperproportionen virtuell darzustellen.«[74]

Auch das 3DZZ arbeitet, in enger Kooperation mit der Rechtsmedizin der Universität Zürich, an der dreidimensionalen Vermessung tatbeteiligter Personen – Täter wie Opfer, ob sie lebendig sind oder tot. Eingesetzt wird dafür zum einen ein futuristisch anmutender Fotoautomat – ein Multi-Kamera-System namens »3D-Fotobox«, das aus 70 Canon-EOS-1200-Kameras besteht, welche in mehreren höhenversetzten Kreisen um eine in der Mitte der Fotobox platzierte Person angeordnet sind (Abb. II.10). Mit der 3D-Fotobox, die im Forensischen Institut Zürich (FOR) steht und die erkennungsdienstliche Personenidentifizierung auf ein neues Intensitätslevel biometrischer Erfassung heben soll, kann »der komplette Körper der zu untersuchenden Person mit einer simultanen Kameraauslösung 3D-dokumentiert werden«. Damit aus rechtsmedizinischer Sicht nicht genug. Hinzu kommt das Robotersystem »Virtobot«, bei dem das Skalpell durch einen Scanner ersetzt wird[75] und eine minimalinvasive virtuelle Autopsie (»Virtopsy« genannt) durchführbar ist: »Der Virtobot mit verschiedenen Modulen automatisiert unter anderem Oberflächenscans von Verstorbenen. Die In-

74 Breker: »High-End 3D-Verfahren beim Bayerischen Landeskriminalamt«, S. 528.

75 Michael Thali: »Virtuelle Autopsie (Virtopsy) in der Forensik. Vom Skalpell zum Scanner«. In: *Der Pathologe*, 32, 2011, S. 292-295 und Bornik: »Integrierte, computergestützte Fallanalyse auf Basis von 3D-Bildgebung«.

tegration mit einem Computertomografen erlaubt es, gleichzeitig mit der Oberfläche auch das Innere des Körpers hochauflösend zu dokumentieren.«[76] Auch die bildgebende Virtualisierung forensischer Medizintechniken schreitet voran[77] (Abb. II.11).

Für das »gedankliche Modell« der Kriminalpraxis bieten diese Verfahren der 3D-Dokumentation von Personen somit die Möglichkeit, eingescannte Tatverdächtige im Zuge der kriminalistischen Modellversionierung von Tatabläufen, die es vorzustellen und zu rekonstruieren gilt, ganz direkt durch den 3D-Punktewolkendatensatz einer millimetergenau gespeicherten Tatörtlichkeit zu navigieren. Eine maximal informationsgesättigte deskriptive Tatortkonservierung und ein breiter Werkzeugkasten für dreidimensionale Tatablaufvisualisierungen, die einerseits tatortforensisch (geo-)referenzialisiert sind, andererseits auf anschaulich-intuitive Weise durchgespielt werden können, finden im virtuellen Tatort so gesehen einen geteilten Möglichkeitsraum kriminalistischer Heuristik, der selbst avatarbasierte Reenactments eingescannter Tatbeteiligter zulässt. Die medialen Spannungen sind nicht unerheblich: Es handelt sich um einen virtuellen Raum, der ein historischer ist, jedenfalls als solcher verstanden werden soll, zugleich aber, medientechnisch gesehen, bei jeder Anwendung komplett neu generiert wird. Das gilt zwar für alle digitalen Objekte, selbst für ein gewöhnliches PDF, wie Lisa Gitelman gezeigt hat.[78] Im Fall der bis zur gerichtsfesten Beweisbarkeit von Tatabläufen reichenden virtuellen Tatortmodelle kann das medienmaterialistische Faktum permanenter Regenerierung aber durchaus zusätzliche Fragen aufwerfen. Denn wie

76 Sieberth et al.: »Das 3D-Zentrum Zürich«, S. 112.

77 Vgl. dazu auch Kathrin Friedrich (2018): *Medienbefunde. Digitale Bildgebung und diagnostische Radiologie*. Berlin, De Gruyter.

78 »Using a file manager application to look on your own hard drive for a PDF is something like rooting through a filing cabinet, if you could ever root through files paying attention only to file names and locations, and not to things like thickness or signs of wear. And if you can let go of the idea that the document you call to the screen is actually entirely the same (rather than just looking the same) each time you call it up.« Lisa Gitelman (2014): *Paper Knowledge. Toward a Media History of Documents*. Durham, Duke UP, S. 133.

wird garantiert, dass die visualisierte Schussbahn, die einen virtuellen Tatort durchschneidet, mit sich selbst identisch ist? Wie wird permanente Speicherstabilität erreicht und auf Anfrage nachgewiesen? Und wie garantiert, dass die informationstechnischen Kalkulationen, die der computergrafischen Visualisierung zugrunde liegen, korrekt und widerspruchsfrei sind? Man würde wohl sagen: Man vertraut der Expertise der Sachverständigen, die ihre Befunde nach den wissenschaftlichen Standards ihrer Disziplinen plausibilisieren müssen. Gleichwohl: Wieviel Handlungsmacht gutachterlichen Sachverstands wird dabei an nichtmenschliche Akteure, beispielsweise an die algorithmischen Systeme der bildgebenden Forensik delegiert? Allein weil die medialen Operationsketten, die diesen Prozessen zugrunde liegen, enorm komplex, vielgliedrig, distribuiert sind, weil auch die beteiligten Algorithmen, die eingesetzte Soft- und Hardware eine Geschichte haben, gerät der Nachweis gutachterlichen »Sachverstands« jedenfalls immer technizistischer und weitschweifiger (oder verschwindet einfach stillschweigend in einer Black Box).

Zurück zur Kriminalpraxis: Neben den bisher betrachteten Verfahren der virtuellen Tatortdokumentation, die ausschließlich von 3D-Datensätzen ausgehen, welche als solche, also lasermesstechnisch, am Ereignisort aufgenommen wurden, besteht ebenso die Möglichkeit, räumliche Strukturen aus zweidimensionalen Aufnahmen zu errechnen. Mittels verschiedener Computer-Vision-Technologien lassen sich virtuelle Modelle nämlich auch auf der Datengrundlage herkömmlichen Bildmaterials – fotografischen, videografischen, zeichnerischen; mitunter auch in Kombination – generieren. In der Praxis ermöglicht das unter anderem neuartige Auswertungen sichergestellter Videosequenzen:

> »Eine Videoaufzeichnung einer Überwachungskamera wird uns zur Verfügung gestellt. Es werden Bilder aus dieser extrahiert, in denen der Täter vollständig (d.h. von Kopf bis Fuß) zu erkennen ist. Der Tatort wird mit dem Laserscanner erfasst; über gemeinsame Punkte im extrahierten Bild aus der Videoaufnahme und dem Laserscan kann das 2D-Bild in den 3D-Raum transformiert werden. Das heißt,

> dem Bild werden die aus dem 3D-Laserscan bekannten Koordinaten zugeordnet. Das Bild kann entzerrt und sowohl die inneren als auch die äußeren Parameter der Kamera zurückgerechnet und somit Maße im Bild ermittelt werden. Nach dem gleichen Prinzip […] kann über den 3D-Punktewolkendatensatz des Tatorts und einem Bild aus dem Überwachungsvideo die Kameraposition zurückgerechnet werden. Die virtuelle Kamera im Laserscan befindet sich nun also in der gleichen Position mit den gleichen inneren bzw. äußeren Parametern der Überwachungskamera. Sind Geschädigte bzw. Tatverdächtige bekannt, können diese mit dem Artec-Scanner eingescannt werden und entsprechend ihrer Körperhaltung in die Einzelbilder (Frames) der Videoaufzeichnung in den 3D-Laserscan eingefügt werden. Man ist nun nicht mehr starr an die Kameraposition der Videokamera gebunden, sondern kann diese verlassen. Der Tatablauf kann somit in 3D aus verschiedenen Perspektiven betrachtet werden.«[79]

Eine auch in medienhistoriografischer Hinsicht nochmals komplexere Bildmaterialkonstellation hatte die fototechnische Abteilung des BLKA vor einigen Jahren zu prozessieren, als die Staatsanwaltschaft Weiden die Geomedientechniker:innen im Rahmen eines Prozesses gegen den SS-Wachmann Johann Breyer beauftragte, ein 3D-Modell des Vernichtungslagers Auschwitz-Birkenau zu erstellen[80] (Abb. II.4). Das später auch in einem weiteren derartigen Prozess (in Detmold, gegen den SS-Unterscharführer Reinhold Hanning) eingesetzte virtuelle Modell kombinierte Laserscan-Rohdaten, die Brekers Team am Ereignisort, an dem sich heute die Gedenkstätte *Auschwitz-Birkenau Memorial and Museum* befindet, in mehrtägiger Arbeit akquiriert hatten. Die vor Ort eingescannten Baracken, Wachtürme, Gleisanlagen, Rampen, Stacheldrahtzäune, Gebäude – oftmals Reststrukturen – wurden in einem aufwendigen Verfahren sowohl mit historischen Karten des polnischen Vermessungsamtes als auch mit Luftaufnahmen der Alliierten und mit im

79 Breker: »High-End 3D-Verfahren beim Bayerischen Landeskriminalamt«, S. 528.

80 Vgl. Rothöhler: *Das verteilte Bild*, S. 223ff.

Washingtoner *United States Holocaust Memorial Museum* archivierten Fotografien fusioniert, die die SS-Wachmannschaften trotz Verbots für ihre privaten Erinnerungsalben meinten aufnehmen zu müssen. Daraus für die Erstellung des virtuellen Modells zu extrahieren waren bauliche Aktualzustände, die von den ebenfalls konsultierten Planungsskizzen der NS-Täter mitunter abwichen, und auch konkrete Details wie Höhe und Blattwerkdichte bestimmter Bäume während des im Prozess verhandelten Tatzeitraums. In der Urteilsbegründung des Detmolder Gerichts wurde denn auch explizit auf den aufwendig generierten 3D-Datensatz Bezug genommen, als es darum ging, dem im Frühjahr 1944 in Auschwitz stationierten Angeklagten – der, wie üblich bei diesem Personenkreis, angab, beim besten Willen keinen industrialisierten Massenmord gesehen zu haben – konkrete Sichtachsen und Sichtbereiche zuzuordnen, die mit seinem spezifischen Dienstort in der Lagerverwaltung einhergingen.

Für die Ermittler:innen entscheidend ist, welche kriminalpraktischen Handlungsmöglichkeiten sich mit der virtuellen Tatortdokumentation eröffnen, wie der 3D-Datensatz konkret visuell umgesetzt, erfahrbar und operabel wird. Zum einen besteht natürlich weiterhin die Möglichkeit einer 2D-Visualisierung. Meist handelt es sich dabei um Bildserien, die beispielsweise verschiedene Perspektiven, die innerhalb des Modells einnehmbar sind, zeigen. Avancierter sind jedoch neuere Anwendungsszenarien, die auf Virtual-Reality-Technologien (VR) rekurrieren und die fotorealistischen Effekte der oben beschriebenen »farbgetreuen Gesamtpunktewolke« für interaktive Formen einer 3D-Tatortvisualisierung (*volume rendering*) nutzen. Der lasermesstechnisch und hochkontrastfotografisch eingefrorene historische Ereignisort einer Tat wird mittels hochauflösender VR-Headsets (im BLKA werden derzeit HTC Vive Pros eingesetzt; Abb. II.4) zu einer begehbaren, mit immersiv-gamifizierten Erfahrungsqualitäten angereicherten virtuellen Umgebung, wie Ralf Breker in seinem neuesten Beitrag für die *Kriminalistik* ausführt:

> »Die Game-Engine ›Unity‹ ist eine Entwicklungsumgebung für Computerspiele und interaktive 3D-Grafik-Anwendungen. Die offene Pro-

> grammierumgebung der Engine bietet uns die Möglichkeit, der Virtual Reality-Applikation nach Belieben Features zuzuweisen und interaktiv zu gestalten. Die programmierten Funktionen werden den Knöpfen der Controller zugewiesen und versetzen den Anwender in die Lage, mit seiner virtuellen Umgebung, in unserem Fall des Tatorts, zu interagieren.«

Im BLKA wurde hierfür eigens ein neues Medienlabor eingerichtet, das sogenannte, so viel Sci-Fi-Semantik musste offenbar sein, »Holodeck«, eine VR-Umgebung, die eine ganze Reihe zusätzlicher Funktionen für den kriminalpraktischen Alltag bereithält – so etwa die »Teleportation«:

> »Der reale Raum (Labor) in dem man sich bewegt, ist meist kleiner als der virtuelle (Tatort). Erreicht man eine Grenze des realen Raums, kann die Teleportationsfunktion verwendet werden, um in entferntere Bereiche des Tatorts zu gelangen. Die Teleportation macht den Anwender unabhängig von der realen Größe eines Raumes. Umso kleiner der reale bzw. größer der virtuelle Raum ist, desto häufiger muss diese Funktion angewendet werden.«

Derart teleportiert können die Forensiker:innen in das 3D-Bild eines konservierten historischen Spurenbildes eintreten, um »Spuren am ›echten‹ Tatort [zu analysieren und auszuwerten]; zudem könnten die Ergebnisse auf wissenschaftlicher Grundlage in Echtzeit visualisiert werden«. Die Ermittler:innen treffen dort nun auch auf greifbare, im Sinne der Modellversionierung fungibel werdende Objekte. Es besteht die »Möglichkeit virtuelle Objekte in ihrer Position und Rotation zu verändern (z.B. Verschieben eines Tisches am Tatort oder Veränderung der Position eines Autos). Im Vorfeld müssen die Objekte, die freigestellt werden sollen, definiert werden. Aus dieser Funktionalität ergibt sich z.B. die Möglichkeit zur Rekonstruktion eines Tatablaufs.« Auch können diese Objekte mitunter animiert sein, beispielsweise in Form eines durch den Tatort fahrenden Vehikels: »Ist eine virtuelle Kamera

an dem Objekt ›montiert‹, ist es möglich per Click die entsprechende Sicht einzunehmen (z.B. Mitfahren in einem Auto).«[81]

Grundsätzlich lassen sich Objekte, die als 3D-Datensatz im Arbeitsspeicher der Ermittlungen liegen, nicht nur dreidimensional visualisieren, sondern auch in stofflicher Hinsicht dreidimensional rematerialisieren – mit Hilfe von 3D-Farbdruckern. Dahinter steht einerseits eine Pragmatik, die bis auf die Gerichtsbühne reicht:

> »Der Grund, warum wir den digitalen Datensatz ausdrucken ist folgender: Im Gerichtssaal ist es möglich, anhand des 3D-Ausdrucks verschiedene Varianten eines Tatablaufs ›durchzuspielen‹. Es können mit analogen Messwerkzeugen ermittelte Messwerte eines Sachverständigen nachvollzogen werden. Außerdem erübrigt sich somit in manchen Fällen, eine virtuelle Szene mit viel Aufwand verändern zu müssen. Der 3D-Druck bietet also allen Verfahrensbeteiligten Zugriff auf ein in der Realität vielleicht nicht mehr vorhandenes Beweismittel.«[82]

Mit dreidimensional ausgedruckten Schädelmodellen lassen sich tödliche Geschossflugbahnen samt Projektil, mit dem 3D-Print einer Mordopferhand Abwehrverletzungen veranschaulichen. Auch interessant: Im BLKA werden die digitalen 3D-Modelle in dieser reanalogisierten Form konserviert. Offenbar gibt es, was den archivarischen Tradierungsauftrag der Behörde anlangt, ein gewisses Misstrauen gegenüber dem durch *data rot* und nie endende Updatezwänge, die Hard- wie Software betreffen, notorisch eingeschränkten Persistenzversprechen digitaler Datenspeicherung.

Im Zentrum steht aber, so Breker in verschiedenen Formulierungen, »die Immersion, das Eintauchen in den Tatort«, »ein von der Zeit unabhängiges ›Erfahren‹ eines Szenarios«, um »ad hoc verschiedene Varianten z.B. eines Tatablaufs durchzuspielen und diese zu bewerten«: »Die Immersion ermöglicht Empathie, die Möglichkeit des sich Hineinversetzens in eine Opfer- bzw. Täter- oder Zeugensituation.

---

81 Ralf Breker: »Virtuelle Realität: Aufbruch in eine neue Wirklichkeit«. In: *Kriminalistik*, 1, 2019, S. 43-47. Hier: S. 43f.

82 Breker: »High-End 3D-Verfahren beim Bayerischen Landeskriminalamt«, S. 531.

Alle Aussagen dieser Personen werden so nachvollziehbarer und können leichter verifiziert bzw. falsifiziert werden.« Was dabei entsteht, ist ein Handlungsraum, der nicht zuletzt auch die verschiedenen menschlichen Akteure der Kriminalpraxis neuartig verbindet, ganz konkret etwa über Remote- und Multi-User-Funktionalitäten: »Die 3D-Szenerie kann von mehr als 50 Anwendern gleichzeitig angesteuert werden und ist nicht nur in der Laborumgebung des BLKA, sondern über das Internet theoretisch von überall aus, rund um den Globus, möglich. […] Beispielsweise wäre es möglich, dass ein Staatsanwalt, ein Ermittler und ein Zeuge gemeinsam den virtualisierten ›echten‹ Tatort betreten.«[83] Während die klassische Tatrekonstruktion üblicherweise eine organisatorisch wie finanziell aufwendige, oftmals aufgrund zwischenzeitlich eingetretener baulicher, architektonischer oder landschaftlicher Veränderungen nur eingeschränkt mögliche realräumliche Rückkehr an den »Originaltatort« vorsieht, kann nun nicht nur an den virtuell übertragenen historischen Ereignisort zurückgekehrt werden, sondern diese, man könnte sagen: medienhistoriografische Zeit-Raum-Reise ist ihrerseits auch informativer dokumentierbar, wie die kostenbewussten Schweizer Kollegen des 3DZZ bilanzierend anmerken: »Mittels VR können derartige Tatortbegehungen nun direkt in den Räumlichkeiten eines Polizeipostens, dem Büro des Ermittlers, bei der Staatsanwaltschaft oder im Gerichtssaal durchgeführt werden, was zu einer wesentlich besseren Planbarkeit und niedrigeren Kosten führt. Das Sichtfeld der Protagonisten, die gemachten Aussagen und die Bewegungen werden während der virtuellen Begehung aufgezeichnet und können den Parteien zur Verfügung gestellt werden.«[84] Nicht nur die performativ nachgestellten Blickachsen, sondern auch in VR-Umgebungen benutzte Controller, die Handbewegungen ermöglichen und aufzeichnen, generieren unter virtuellen Bedingungen ein informatives Datum, auf das beim kriminalistischen *reverse engineering* nochmals zurückgekommen werden kann.

83 Breker: »Virtuelle Realität«, S. 46.

84 Sieberth et al.: »Das 3D-Zentrum Zürich«, S. 113f.

II.4 Digitalbildforensik

Ein wichtiger Teilbereich des Sachverständigengebiets Medienforensik beschäftigt sich mit der Sicherung und Analyse digitaler Bilder. Wie in der Computerforensik allgemein, gilt es hier im ersten Schritt, Datenstände einzufrieren, um sie nach ihrer forensischen Sicherstellung als Spuren möglicherweise krimineller Handlungen auslesen zu können. Nach der Secure-Phase, die mobilen Endgeräten, Festplatten, USB-Sticks, Mail-Servern, Cloud-Storage-Speichern oder auch (Visual-)Social-Media-Accounts[85] gelten kann, arbeitet die bildforensische Analyse mit Zielfragen wie diesen: Wie, wo, mit welcher bildsensorisch ausgerüsteten Apparatur ist der fragliche Bilddatensatz entstanden? Ist er nach der Akquise, jenseits der formativ in die Bildgenese involvierten algorithmischen Prozessautomatismen, verändert worden? Ergibt die forensische Examinierung Informationen zur digitalen Nutzungsgeschichte des Bildes? Wie, wann – und vielleicht sogar: wo und von wem – wurde mit ihm gehandelt?

Digitalbilder sind zum einen deshalb von besonderem forensischem Interesse, weil sie nicht nur allgegenwärtig und hochmobil, sondern zugleich relativ einfach und effektiv manipulierbar sind – beispielsweise durch populäre Photoshop-Anwendungen, die, zumindest in rudimentärer Form, meist direkt über Interfaces der Aufnahmegeräte operabel sind. Die Akquise und die Bearbeitung digitaler Bilddaten sind ohnehin zunehmend schwer unterscheidbare, weil quasi-gleichzeitig ablaufende Vorgänge – man denke an handelsübliche Filtersoftware oder das Arsenal mittlerweile ebenfalls weit verbreiteter, KI-gestützt ›selbstlernender‹ Bildoptimierungsalgorithmen.[86] ›Unbearbeitete‹ Digitalbilder

85 Vgl. Tama Leaver, Tim Highfield, Crystal Abidin (2020): *Instagram. Visual Social Media Cultures*. London, Polity Press.

86 Ein populäres Beispiel für rezente Modi einer digitalen Bildprozessierung, die sich direkt, ohne Beteiligung menschlicher Handlungsträger, in den Prozess der Bilddatenakquise einschreiben, sind etwa voreingestellte Porträtmodi auf Smartphones, die menschliche Gesichter im bildsensorisch adressierten Aufnahmefeld automatisch identifizieren und privilegieren – und dabei, wie Hito Steyerl, die hier von »relational photography« spricht, angemerkt hat, prä-

gibt es so gesehen nicht wirklich, sie sind mehr oder weniger immer, auch diesseits ihrer softwarevermittelten Phänomenalisierung auf konkreten Screens und Displays, vielfach prozessierte Effekte von Bilddatenverarbeitung.

Daraus ergibt sich eine zentrale Aufgabe der professionellen Digitalbildforensik: die gerichtsfeste Authentifizierung von Medienprodukten (auf die angesprochene Ubiquität digitaler Bilder, die eine plattformisierte ist, wird in Kapitel III näher einzugehen sein). Zum anderen aber sind Digitalbilder aus Sicht der Forensik gerade auch abseits ihres bildförmig umgesetzten ›Contents‹ hochgradig informationsgesättigte Spuren – mehr noch als ihre analogen Vorläufer. Der Grund dafür liegt in den mit digitalfotografischen Praktiken verbundenen Prozessen automatischer Datafizierung. Digitalbilder sind informativ, weil sie indexikalisch informatisiert sind – und zwar relativ unabhängig davon, was konkrete menschliche Wahrnehmungsleistungen als Bildinhalte glauben identifizieren zu können. Diese Ebene, die sichtbare Außenseite des Bilddatensatzes, das fotorealistische Bild als Wahrnehmungsgegenstand, auf dem etwas ikonisch repräsentiert, bildförmig zu sehen ist, ist natürlich aus Sicht der Kriminalpraxis alles andere als irrelevant. Gleichwohl wird beim kriminalistischen Umgang mit Digitalbildern mittlerweile ganz selbstverständlich davon ausgegangen, dass diese keine feststehenden, lediglich mit Blick auf dargestellte, abgebildete Bildinhalte zu lesenden Objekte sind, sondern dass es sich, schon im

---

diktive Effekte generieren. Das Bild ist hier also gewissermaßen algorithmisch ›bearbeitet‹, bevor es als solches vorliegt: »It is not only relational but also truly social, with countless systems and people potentially interfering with pictures before they even emerge as visible. […] You could end up airbrushed, wanted, redirected, taxed, deleted, remodeled, or replaced in your own picture. The camera turns into a social projector rather than a recorder. It shows a superposition of what it thinks you might want to look like plus what others think you should buy or be.« Hito Steyerl (2017): *Duty Free Art in the Age of Planetary Civil War*. London/New York, Verso, S. 29 [ebook]. Vgl. dazu auch: Estelle Blaschke: »Diskrete Operationen: Formen präemptiver Bildzensur in der KI-gestützten Fotografie«. In: Katja Müller-Helle (Hg., 2021): *Bildzensur. Löschung technischer Bilder. Bildwelten des Wissens, Band 16*. Berlin, De Gruyter, S. 32-41.

Moment bildsensorischer Akquisen, um ein mit möglicherweise relativ unanschaulichen, aber informativen Tiefenstrukturen assoziiertes, vielfach metadatiertes Prozessbild handelt.[87] Anders gesagt: Entstehung und Nutzung digitaler Bilder sind datenproduktiv, verlaufen über algorithmische Prozesse und Performanzen, die in verschiedenen Speicherformaten Spuren hinterlassen und deshalb in mehrerlei Hinsicht forensisch rückwärtsgelesen werden können. Digitalbilder sind Spuren, an denen sich weitere Digitalspuren anlagern: der Nutzung, der Manipulation, der Distribution oder auch der Vernetzung.

Dass die forensische Authentifizierung eines digitalen Bildes tatsächlich wenig mit der kriminalistischen Auswertung von Bildinhalten zu tun hat, betont auch Hany Farid, eine internationale Autorität im Feld der *digital image forensics*. Was auf einem Bild zu sehen, zu erkennen ist – und ohnehin: was es bedeutet –, liegt außerhalb bildforensischer Expertisen. Die forensische Authentifizierung argumentiert ihrerseits spurförmig und bezeichnet neben der im ersten Schritt festzustellenden Bildquelle (*image source identification*) – »the forensic analysis to investigate which device (or class of device) captured or formed the image under investigation«[88] – hier lediglich den Nachweis einer Abwesenheit von Bildeingriffsspuren:

> »All of the techniques are based on certain assumptions that limit their applicability, and it is critical for the reader to be cognizant of these limitations. In general, individual techniques can reveal evidence of tampering, but they cannot provide evidence of authenticity. Only in the aggregate can these techniques support (although they can never prove) authenticity.«[89]

87 Vgl. Rothöhler: *Das verteilte Bild*.

88 Aniket Roy, Rahul Dixit, Ruchira Naskar, Rajat Subhra Chakraborty (2020): *Digital Image Forensics. Theory and Implementation*. Singapore, Springer Nature, S. 3.

89 Hany Farid (2019): *Fake Photos*. Cambridge/MA, London, MIT Press, S. 4 [ebook]. Vgl. auch das dazugehörige technische Handbuch: Hany Farid (2016): *Photo Forensics*, Cambridge/MA, MIT Press.

Bildforensisch adressiert und gegebenenfalls nachgewiesen werden also Spuren digitaler Praktiken der Bildmodifikation oder gar, dramatischer formuliert, der Bildfälschung. Bleibt der bildforensische Analysevorgang diesbezüglich ohne Ergebnis, ist das Bild als unmanipuliertes authentifiziert. Mehr nicht.

Den normativen Horizont institutioneller Bildforensik bilden dabei grundsätzlich jene Regeln, unter denen fotografische, filmische, videografische Materialien vor Gericht als Beweismittel eingeführt werden können. Darauf bezieht sich auch das Koordinatensystem einer bildforensisch zu leistenden Authentifizierung, wie Farid mit Blick auf den US-amerikanischen Kontext erläutert, wo für »electronically stored information« allgemein gilt, wie es in *The Federal Rules of Evidence*, Rule 1001, Article X heißt, dass es sich, aus Sicht der Gerichtstauglichkeit, um der Wahrnehmung unmittelbar zugängliche »Originale« (mit Anführungszeichen) handeln müsse – »›original‹ means any printout – or other output readable by sight – if it accurately reflects the information. An ›original‹ of a photograph includes the negative or print from it.« Im Fall digitaler Bildmedien, so Farids Schlussfolgerung, ist für eine derartig ausgerichtete Authentifizierung der analytische Eintritt in verschiedene medientechnische Phasen des bildgebenden Prozesses von entscheidender Bedeutung: »These authentication techniques work in the absence of any type of digital watermark or signature. Instead, these techniques model the path of light through the entire image-creation process, and quantify physical, geometric, and statistical regularities in images that are disrupted by the creation of a fake.« Diesen Prozess bezeichnet Farid als »image recording pipeline«, separiert in technisch distinkte Phasen, über die Photonen in Elektronen umgewandelt, formatiert und gespeichert werden: »the interaction of light in the physical scene; the refraction of light as it passes through the camera lenses; the transformation of light to electrical signals in the camera sensor; and, finally, the conversion of electrical signals into a digital image file«. Entsprechend distribuiert ist (und gliedert sich) auch die forensische Detektion manipulativer Eingriffe: »At each stage of this image formation process, certain regularities are introduced into the final image.

The authentication techniques exploit deviations from these regularities to expose photo manipulation.«[90]

Daraus leitet sich ein breites Spektrum bildforensischer Instrumente ab, die in technischer und professioneller Hinsicht unterschiedlich voraussetzungsreich sind: von einfach zu bedienenden Reverse-Image-Search-Applikationen wie Tineye oder Google Images, mit denen sich erste Provenienz-, Zirkulations- und Versionsforschungen betreiben lassen, über die Auswertung von Metadaten, die im Fall digitaler Bilder üblicherweise im EXIF-Format gespeichert sind und u.a. Informationen zu Gerät, Belichtungszeit, Brennweite, Batterielevel und vor allem: zu Datum, Uhrzeit und zum Ort der Aufnahme enthalten – und manchmal auch Spuren eingesetzter Photo Editing Software (die in Form von Tags und zusätzlichen Zeitstempeln dokumentiert sein können) –, bis zu komplexeren Analysevorgängen der JPEG-Signatur (über die ein digitales Bild einem spezifischen Aufnahmegerättypus zugeordnet werden kann) oder auch 3D-Modellierungen, die virtuelle Kameras konstruieren und darüber Konsistenzprüfungen (beispielsweise des Schattenwurfs abgebildeter Personen und Objekte) laufen lassen. Nochmals anspruchsvoller sind Techniken, mittels derer sich herausfinden lässt, ob ein Bild nach seiner initialen Speichereinschreibung ein weiteres Mal gespeichert wurde (*double compression*), oder auch Verfahren, die direkt auf der Mikroebene der Pixelverteilung ansetzen und dort nach Spuren erfolgter Bildeingriffe fahnden. Hier geht es dann, in einem vielstufigen informationstechnischen Operationsvorgang, um eine Untersuchung der *image pipeline* in ihrer Prozessualität, wie Farid am Beispiel der *noise pattern analysis* zeigt:

> »A digital camera contains a vast array of sensor cells, each with a photo detector and an amplifier. The photo detectors measure incoming light and transform it into an electrical signal. The electrical signals are then converted into pixel values. In an ideal camera, there would be a perfect correlation between the amount of light striking the sensor cells and the pixel values of the digital image. Real devices have

90 Ibid., S. 5.

> imperfections, however, and these imperfections introduce noise in the image.«[91]

Was dabei entsteht, sind unterscheidbare Variationen, genannt *photo-response non-uniformity* (PRNU), die ein bestimmtes bildimmanentes ›Geräuschmuster‹ mit einem bestimmten Aufnahmegerät verbinden, was wiederum dem spurtheoretischen Kriterium der Individualität entspricht:

> »The PRNU associated with a particular device is not just stable; it is also distinctive. Even devices of the same make and model have different PRNUs. The stable and distinctive properties of the PRNU allow it to serve two forensic functions. The PRNU can be used to determine whether a particular image is likely to have originated from a given device. The PRNU can also be used to detect localized tampering in an image that was taken from a known device. This second use allows us to confirm the authenticity of an image taken by a photographer who has already produced a body of trusted work.«[92]

Eine zunehmend komplexere Herausforderung des forensischen Nachweises verdächtiger Inkonsistenzen – denn darum geht es im Kern: ob auf der Ebene des ikonisch umgesetzten Bildinhalts, in den unsichtbaren Mikrostrukturen der Pixeldistribution oder bezüglich der Metadatierung – besteht darin, die sich ebenfalls fortlaufend weiterentwickelnden Skills der Fälscher:innen stets mit einzukalkulieren. Das gilt auch für die tief in Pixelkorrelationen eindringende *noise pattern analysis*:

> »While an inconsistency in the sensor noise of an unsaturated image is a red flag, a lack of inconsistency is inconclusive. A forger could remove the sensor noise from the original image, alter the image, and then re-insert the sensor noise. This counterattack requires access to effective noise-removal software, but it is certainly not out of the reach of a sophisticated forger. […] We in the authentication business are in

91 Ibid., S. 260.

92 Ibid., S. 263.

> the same cat-and-mouse game as those fighting spam and computer viruses. As we develop techniques for authenticating digital images, those intent on manipulating digital images continue to adapt.«[93]

Der dynamische Antagonist dieser Form der Forensik ist der Fake. Manipulative Bildeingriffe umfassen dabei ein ebenfalls weit gefasstes Spektrum digitaler Desinformation, das, wie es in einer aktuellen Studie heißt, von *cheap fakes* bis zu *deepfakes* reicht.[94] Dort wird einerseits auf eine Reihe neuartiger Manipulationsverfahren audiovisuellen Materials eingegangen, die technisch avanciert sind und auf Künstliche Neuronale Netzwerke (KNN) zurückgreifen (Lip-synching; Face-swapping; Voice synthesis; Virtual performances). Am diametralen Ende des Spektrums befindet sich nicht die rezente Popularisierung derartiger Verfahren – man denke an die kaum mehr überblickbare Menge an FaceSwap- und LypSync-Apps –, sondern auf anderer Ebene operierende Interventionspraktiken, die ebenfalls vergleichsweise einfach umsetzbar, deshalb aber noch lange nicht weniger effizient sind: Speeding, Slowing, Cutting, In-Camera-Editing, Recontextualizing und Relabeling lauten die dazugehörigen Stichworte. Grundsätzlich hängt die (gesellschaftliche, politische) Wirksamkeit einer Fälschung in vielen Fällen nicht von ihrer technischen Perfektion, sondern von ihrer Reichweite ab. Ein ›viral gehendes‹ Fake-Video, das in kürzester Zeit millionenfach über Social-Media-Plattformen geteilt und rezipiert wird, erreicht eine Skalierung, der der Manipulationsnachweis oftmals nicht entsprechen kann.

Auch avanciertem Computer-generated Content (CGI) kommt die digitale Bildforensik meist auf die Spur – etwa wenn es darum geht, zwischen *real humans* und *rendered humans* zu unterscheiden:

> »One new technique that can make this distinction exploits the tiny periodic fluctuations in skin color that occur with each heartbeat. These changes are not captured by CGI because they are visually

93 Ibid., 270, 281.

94 Britt Paris, Joan Donovan (2019): *Deepfakes and Cheap Fakes. The Manipulation of Audio and Visual Evidence* [*https://datasociety.net*].

> imperceptible. But a remarkable group of MIT researchers has shown that this type of tiny fluctuation can be enhanced to make it more visible. Paired with some standard face-detection and tracking technology, video magnification can be used to determine whether or not a person in a video has a pulse.«[95]

Der bildforensische Umgang mit *cheap fakes* fällt mitunter gerade deshalb schwerer, weil diese per definitionem weniger technizistisch sind und nicht auf gleiche Weise digitale Bildeingriffsspuren hinterlassen: »the most accessible forms of AV manipulation are not technical but contextual. By using lookalike stand-ins, or relabeling footage of one event as another, media creators can easily manipulate an audience's interpretations. […] These types of staging and re-contextualizing are possible for nearly anyone to reproduce, and technical forensic differences are even harder to detect, because there are no pixels out of order.«[96]

Kommt die Digitalbildforensik zu dem Befund, dass sich distinkte Bildeingriffsspuren nachweisen lassen, verweigert sie dem fraglichen Bildmedienprodukt zunächst lediglich die Authentifizierung, flaggt also eine Art Vetorecht aus, das im Arbeitsspeicher konkreter Ermittlungen nicht selten neue Fragen aufwirft. In der kriminalistischen Prozessierung von Spuren geht es ohnehin nicht einfach um die bedingungslose Übernahme isolierter forensischer Teilexpertisen, sondern meist um die Aufgabe, verschiedene Spuren – technische und nichttechnische, analoge wie digitale –, deren Auswertung in den Zuständigkeitsbereich unterschiedlicher forensischer Disziplinen fällt, zueinander – und auch: zu »subjektiven« Befunden, zu Zeugenaussagen – in Bezug zu setzen. Typischerweise umfasst das Spurenbild ein Netzwerk relationaler Spuren, die man als diskrete Spurmaterialien forensisch untersuchen, aber aus Sicht der Kriminalpraxis nur in ihrer Verbundenheit intelligibel machen kann. Für Digitalbilder gilt diese konstituti-

95 Farid: *Fake Photos*, S. 274f. Vgl. dazu Simon Rothöhler: »F for Deepfake. Diese Person existiert nicht«. In: *cargo Film Medien Kultur*, 41, März 2019, S. 70-71.

96 Ibid., S. 15.

ve Relationalität, das Axiom vernetzten Rückwärtslesens auf besondere Weise, weil ihre Ubiquität – durch die Proliferation von Smartphones, durch die bildsensorische Aufrüstung des Internets der Dinge – dazu geführt hat, dass es, um Tatabläufe zu rekonstruieren, regelmäßig unvermeidlich ist, digitale Bilder zu vergleichen und auf andere digitale Datenspuren zu beziehen. Die forensische Feststellung, dass es sich nicht um gezielte Desinformation, nicht um ein gefaktes Bild handelt, ist so gesehen immer nur der Anfang der Ermittlung, wie sich auch mit Blick auf nichtinstitutionelle (para-, proto-, gegen-)forensische Praktiken in digitalen Medienkulturen zeigt, deren Authentifizierungsverfahren regelmäßig Bildassemblagen gelten und die nicht, zumindest nicht im informationstechnischen Sinn, *deep* sind, sondern distribuiert.

II.5 Forensisch-Werden der Digitalmedienforschung

Dass ein forensischer Zugriff auf digitale Medien bestimmte Vorzüge, vielleicht sogar erweiterte analytische Handlungsressourcen mit sich bringt, hat sich längst jenseits kriminaltechnischer Labore herumgesprochen – nicht nur in investigativ-zivilgesellschaftlichen oder pop- und alltagskulturellen Kontexten, sondern auch in den Medienkulturwissenschaften. Dort ist seit einiger Zeit ebenfalls eine Konjunktur zu beobachten: von Semantiken, Praktiken, Heuristiken und Methodologien, die sich (selbst) als forensische verstehen. Die dabei unternommenen Ermittlungen gelten zunächst weniger der Aufklärung einzelner Fälle als der Validierung einer epistemologischen Position, von der aus digitale Medien (noch) konzeptualisierbar sind, analysiert werden können. Verallgemeinernd ließe sich sagen, dass eine forensisch ausgerichtete Medienforschung in erster Linie auf epistemische Entzugsmechanismen digitaler Medien reagiert, auf die Schwierigkeit, diese überhaupt als Objekte des Wissens, die sich betrachten, untersuchen, theoretisieren lassen, zu konstituieren. Es ist also nicht nur die datenkapitalistische Produktivität digitaler Medien, die, da proprietär verschlüsselt und auch sonst geblackboxt, den analytischen Zugriff erschwert und

computergestützte Lektüren attraktiv erscheinen lässt, die statistisch kalkuliert und *distant* sind.

Forensische Medienforschung lässt sich vor diesem Hintergrund als Option verstehen, auf die operative Verteiltheit und prozessuale Echtzeitlichkeit, auf die vermeintliche Ephemeralität und Immaterialität digitaler Medien mit einem Alternativprogramm zu antworten. In diesem geht es nicht um Big Data und Korrelationen, sondern um kleinere Informationseinheiten und Kausalitäten. Das *close reading* distinkter medialer Operationen und Verfasstheiten ersetzt die Konstatierung einer undurchdringlichen Ubiquität der Medien. Statt mit Real Time und Prognostik befasst zu sein, setzt Forensik auf die Nachträglichkeit (Umständlichkeit, Langsamkeit) rekonstruktiven Rückwärtslesens: auf das, was medial der Fall war und nun Spur ist. Forensische Medienforschung operiert also prinzipiell qualitativ, wenngleich sich Anwendungsszenarien vorstellen lassen, bei denen, im Zuge der initialen Materialsichtung, auch auf vergleichsweise materialferne Verfahren des *data mining* zurückgegriffen wird – im Grunde wie in der kriminalistischen Medienforensik, wenn sie, um die berühmte Nadel im Heuhaufen, der ein »globaler« Medientatort ist, zu finden, relevante Digitalspuren von nichtrelevanten zu unterscheiden versucht. In diesem gleichsam vorgelagerten Prozess können via *pattern recognition* statistische Auffälligkeiten erkennbar werden und Verdachtsmomente triggern. Medienforensik ist aber gleichwohl, mit Ginzburg gesprochen, eine »individualisierende Wissenschaftsrichtung«, die »Quantifizierung nur als Hilfsfunktion [zulässt].«[97] Obwohl es also durchaus Berührungspunkte geben kann: Forensische Medienforschung interessiert sich für »das *Individuelle* an Fällen, Situationen und Dokumenten«,[98] für Kontaktsignaturen, das distinkte, identifizier- und nachverfolgbare Datum – nicht für hochgerechnete Mustererkennung, sondern für die Materialität, Geschichtlichkeit und Individualität diskreter Spuren, die mediale, mit Medien verbunden und mit Medien auslesbar sind.

97 Ginzburg: *Spurensicherung*, S. 19.

98 Ibid.

Um spurtheoretische Topoi und forensische Begrifflichkeiten kreist bereits Matthew Kirschenbaums Studie *Mechanisms: New Media and the Forensic Imagination*, die, 2008 erschienen, als eine Art Gründungstext forensischer Digitalmedienforschung gilt. Darin geht es um elektronische Datenverarbeitung, die Medienfunktion des Speicherns, vor allem aber: um das Trägermedium der Festplatte. Kirschenbaum argumentiert, wie aus heutiger Sicht gleichsam diskurshistorisierend anzumerken ist, gegen eine in den Nullerjahren noch vergleichsweise verbreitete Vorstellung, die digitale Medien als immaterielle, flüchtige, irgendwie unverbindliche denkt. Einher geht damit auch der Vorwurf – Stichwort »screen essentialism« (Nick Montfort) –, dass sich medienwissenschaftliche Ansätze der Erforschung digitaler Medien zu sehr auf die immergleichen Denkfiguren des binären Codes (»medial ideology«), auf computergrafische Oberflächen, Interface-Effekte und digitalen Content konzentrieren – mithin auf Phänomene, die dazu tendieren, die Materialität von Komputation zu dissimulieren.

Gleich das erste Kapitel von *Mechanisms* ist programmatisch mit der Locard'schen Regel überschrieben: »›Every Contact Leaves a Trace‹: Storage, Inscription, and Computer Forensics«.[99] Wie heute auch in den Infrastructure und Environmental Media Studies üblich,[100] rückt Kirschenbaum die Materialität digitaler Medien ins Zentrum, verweist dabei aber nicht auf bauliche Strukturen, realräumliche Netzwerke und mit Mediennutzung verbundene CO_2-Fußabdrücke, sondern auf militärische Protokolle der Spurenverwischung. In entsprechenden Operating Manuals des US-amerikanischen Verteidigungsministeriums kann nachgelesen werden, dass das Militär keineswegs von einer verlässlichen Flüchtigkeit digitaler Datenspeicherung ausgeht, sondern sich im Gegenteil um deren hartnäckige Persistenz sorgt. Um das Materialitätskontinuum einer Festplatte (die Anlass zu der Sorge gibt, ih-

99 Matthew Kirschenbaum (2008): *Mechanisms: New Media and the Forensic Imagination*. Cambridge/MA, MIT Press.

100 Vgl. dazu Kapitel IV und Lisa Parks, Nicole Starosielski (Hg., 2015): *Signal Traffic: Critical Studies of Media Infrastructures*. Urbana, Chicago, Springfield, University of Illinois Press.

re Daten könnten prinzipiell wiederhergestellt werden) effektiv zu unterbrechen, werden rabiate Methoden physischer Zerstörung empfohlen – »Destroy – Desintegrate, incinerate, pulverize, shred, or smelt« –, woraus Kirschenbaum folgert: »[T]here is no computation without data's representation in a corresponding physical substratum, the specifics of which very quickly get us into a messy world of matter and metal […].«[101] Wo es Materialitäten gibt, beispielsweise von Lochkarten und Magnetbändern, kann es zu Spuren kommen, die Inskriptionen und somit auch lokalisierbar sind:

> »Though normally invisible to human eyes, the magnetic recording on such a card is indisputably an inscription, as is apparent after the application of aerosolized ferrite oxide, which makes the tracks and data patterns visible […]. A computer forensics expert can visually inspect the patterns of magnetic tracks on a diskette […] and locate the starting points for the different data sectors.«[102]

Weil digitale Medien eine irreduzible materielle Seite besitzen, hinterlassen digital generierte und prozessierte Daten Spuren, die auch dann noch verortbar und rekonstruierbar sind, wenn sich Trägermedien – was in Zeiten von Cloud-Speicher-Architekturen mehr denn je gilt – tendenziell entziehen: »storage has become ever more of an abstraction«.[103] Die distribuierte, sich je nach operativer Verkettung variabel konfigurierende Materialität digitaler Medien unterscheidet Kirschenbaum dabei in eine an die symbolische Ebene (rück-)gebundene »formale« Materialität (Formate, Standards, Protokolle) – die man aus einer anderen Perspektive auch in das Feld »softer« Infrastrukturen eintragen könnte – und zum anderen, mit ersterer in Wechselwirkung stehend, in eine »forensische«:

> »[F]orensic materiality rests upon the principle of individualization (basic to modern forensic science and criminalistics), the idea that no

101 Kirschenbaum: *Mechanisms*, S. 27.

102 Ibid., S. 29f.

103 Ibid., S. 34.

> two things in the physical world are ever exactly alike. If we are able to look closely enough, in conjunction with appropriate instrumentation, we will see that this extends even to the micron-sized residue of digital inscription, where individual bit representations deposit discreet legible trails that can be seen with the aid of a technique known as magnetic force microscopy.«[104]

Um dieser zweiten, in gewisser Weise doch als tieferliegend vorgestellten Materialität auf die Spur zu kommen, entwickelt Kirschenbaum eine computerforensische Lektüre der Festplatte, die medientheoretisch hochskaliert wird und eine »maximalisierte Form der Lesbarkeit« imaginiert, in der, wie Christoph Engemann angemerkt hat, »jedes Ereignis eine Signatur [bekommt]«: »Forensik als eine besonders unbestechliche Form des Lesens.«[105] Dabei handelt es sich um eine maximal materialnahe Form des *close reading*, die den Computer grundsätzlich als hochtourige Inskriptionsmaschine versteht: »The irony is that while the protected internal environment of the hard drive is built to exclude the hairs, fibers, and other minute particulars of traditional forensic science, the platter inexorably yields up its own unique kind of physical evidence.«[106] Besonders relevant für diese Form der Beweisführung – die Kirschenbaum in die Tradition der mit Schriftstücken befassten Dokumentforensik stellt, also mit der ebenfalls materialskrupulösen, von der symbolischen Ebene weitgehend absehenden Untersuchung von Briefpapier und Tinte assoziiert; Inskriptionsmaterialien, die bereits Locard interessierten[107] – ist der Umstand, dass digitale Daten deshalb schwer zu löschen sind,[108] weil sie sich einerseits ständig vervielfältigen, zu-

104 Ibid., S. 10.

105 Christoph Engemann: »Buchbesprechung: Matthew Kirschenbaum, *Mechanisms: New Media and the Forensic Imagination*«. In: *https://zfmedienwissenschaft.de*, 12.06.2014.

106 Kirschenbaum: *Mechanisms*, S. 45.

107 Locard: *Die Kriminaluntersuchung*, S. 135-160.

108 Vgl. dazu allgemein: Matthias Bickenbach: »Löschen«. In: ders., Heiko Christians, Nikolaus Wegmann (Hg., 2014): *Historisches Wörterbuch des Mediengebrauchs*. Köln, Weimar, Wien, Böhlau, S. 429-444.

gleich aber unverwechselbare, individuelle Inskriptionsorte in konkreten physischen Speichern zugewiesen bekommen. Als Medientatort ist der Computer – gerade auch mit Blick auf seine postalische »Logik der Zustellung«[109] (Hartmut Winkler) – bereits intern enorm distribuiert.

Ersteres, die Replikationslogik, klingt aus Sicht der Forensik erst einmal wenig ergiebig, sofern Kopien im Verdacht stehen, von Originalen abzuweichen. Innerhalb von Computer-Architekturen entstehen diese Kopien aber automatisch – und sind, wo Differenz keinen Kalkulationsvorteil bringt, verlustfrei und identisch:

> »The interactions of modern productivity software and mature physical storage media such as a hard drive may finally resemble something like a quantum pinball machine, with a single simple input from the user sending files careening n-dimensionally through the internal mechanisms of the operating system, these files leaving persistent versions of themselves behind at every point they touch – like afterimages that only gradually fade – and the persistent versions themselves creating versions that multiply in like manner through the system. There is, in short, no simple way to know how many instances of a single file are residing in how many states, in how many different locations, at any given moment in the operating system.«[110]

Die autokopistische Neigung digitaler Maschinen der Datenverarbeitung interessiert auch, unter dem Terminus technicus *carving*, die professionelle Computerforensik. Zur rekonstruktiven Zusammensetzung vermeintlich gelöschter Datenfragmente können sogenannte Slackbereiche examiniert werden. Dabei handelt es sich um Speicherplätze, die zwar bereits, qua computerbefohlenem Löschvorgang, freigegeben,

---

109 In *Prozessieren. Die dritte, vernachlässigte Medienfunktion* vertritt Hartmut Winkler die These, dass der Computer ein »legitimer und unmittelbarer Spross der Telegraphie« sei, sofern die rechnerinternen Prozesse als Transportvorgänge (»interne Telegraphie«) zwischen Festplatte, Arbeitsspeicher, Prozessor und Bildschirm aufgefasst werden können. Hartmut Winkler (2015): *Prozessieren. Die dritte, vernachlässigte Medienfunktion*. Paderborn, Fink.

110 Kirschenbaum: *Mechanisms*, S. 52.

aber noch nicht überschrieben sind: »Beim Löschen einer Datei beispielsweise entfernt das Betriebssystem in der Regel lediglich den Verweis auf die Datei aus den Tabellen des Dateisystems. Der dadurch nicht länger allozierte Speicherbereich kann zu einem späteren Zeitpunkt gegebenenfalls mit neuen Daten überschrieben werden. In der Zwischenzeit sind die alten Daten aber nach wie vor vorhanden. Ähnlich verhält es sich, wenn der Datenträger formatiert wird.«[111]

Weil die medienmaterialistische Löschung eines digitalen Datums erst dann (und nur dann) vorliegt, wenn der von diesem Datum beanspruchte Speicherplatz restlos, bis in den Nanobereich physisch exakt überschrieben ist, findet die computerforensische *trace evidence* immer wieder Rückstände und Restbeträge: unvollständig überschriebene *ambient data*. Je voluminöser, preiswerter, zugänglicher die verfügbaren Speicherkapazitäten werden, desto unwahrscheinlicher erscheint vollständig kongruente Überschreibung. Das vormals weithin akzeptierte Mooresche Gesetz ist ein Freund der Forensik: Es generiert fortlaufend Speicherüberschüsse, minimiert die Notwendigkeit vollständiger Überschreibung. Aufgrund der physischen Eigenschaften digitaler Datenspeicherung – »the inability of the writing device to write in exactly the same location each time« – können forensische Instrumente, Verfahren, Methodologien überhaupt zur Anwendung kommen, wie Kirschenbaum ausführt:

> »This effect satisfies the forensic principle of individualization, which insists upon the absolute uniqueness of all physical objects. The core precepts of individualization construct a hard materiality of the kind that ought to resonate with textual scholars and others in the traditional humanities: ›No two things that happen by chance ever happen in exactly the same way; No two things are ever constructed or manufactured in exactly the same way; No two things ever wear in exactly the same way; No two things ever break in exactly the same way.‹ That the scale here is measured in mere microns does not change the fact

111 Pawlaszczyk: »Digitaler Tatort«, S. 137.

> that data recording in magnetic media finally and fundamentally is a forensically individualized process.«[112]

Grundsätzlich bleibt dabei aber zu bedenken, dass die formale und die forensische Materialität des Computers ineinander verschränkt sind, weshalb digitale Forensik – als *trace evidence*, die Komputation über Kontaktsignaturen konzeptualisiert – zwar von einem physisch nachweisbaren Verbleib von Daten in Speichermedien ausgeht (»stored data have a measurable physical presence in the world«), zugleich aber auch weiß, dass ohne die Funktionalität der formal-symbolischen Ebene kein digitalforensischer Analysezugriff vorstellbar ist, der in der »realen Welt« einen relevanten Unterschied macht:

> »A skilled investigator is able to leverage the features of the software operating system (OS) along with the physical properties of the machine's storage media. But a comparison of digital evidence to hair, fibers, and paint chips will take us only so far. Specialists recognize that the characteristics of digital data are different from those of other forms of physical evidence […]. […] we must remember that there is, finally, no direct access to data without mediation through complex instrumentation or layers of interpretative software.«[113]

Computerforensik ist mit Remanenzen, mit fossilen Daten befasst: spurförmig abgelagerte Überreste, *shadow* und *ambient data*, die, weit unterhalb der Wahrnehmungsschwelle empirischer Mediennutzer:innen, persistieren – und dennoch (oder gerade deshalb) wiederhergestellt, rekonstruiert, mittels Software interpretiert und über Interfaces operabel werden können. Wobei: Wahrgenommen werden diese Rückstände mittlerweile sehr wohl, wenn auch nicht forensisch-konkretistisch, sondern eher diffus, wie sich an einer Verschiebung der »anxieties«[114] im kulturellen ›Imaginären‹ ablesen lässt. Spätestens

112 Kirschenbaum: *Mechanisms*, S. 63.

113 Matthew Kirschenbaum, Richard Ovenden, Gabriela Redwine (2010): *Digital Forensics and Born-Digital Collections.* Washington, Council on Library and Information Resources, S. 6.

114 Kirschenbaum: *Mechanisms*, S. 70.

seit den Enthüllungen Edward Snowdens gelten verbreitete Speicherpersistenzsorgen weniger Phänomenen wie *data rot* und *data loss* als der effektiven Unlöschbarkeit all jener Tracking- und Tracing-Spuren, die einigermaßen unaufkündbar zum digitalen Alltag gehören. Wo vormals Speicherverlustsorgen vorherrschten, dominiert nun die Skepsis gegenüber der Ubiquität unvermeidlich mitlaufender »digital footprints«[115] – gegenüber Speichern, die nicht vergessen, und Spuren, die langfristig auffindbar, auslesbar bleiben.

Im diskurshistorischen Rückblick durchaus nicht unähnlich wie Sybille Krämer, die die geisteswissenschaftliche Renaissance des Spurkonzepts vor gut eineinhalb Dekaden gegen die »Beschwörung einer Referenzlosigkeit der Zeichen«, gegen von ihr im Einzugsbereich des »sogenannten postmodernen Denkens« verortete Vorstellungen der »Dematerialisierung, Derealisierung, Entkörperung, Informatisierung, Virtualisierung, Simulationseuphorie« in Stellung bringen wollte, resoniert auch Kirschenbaums forensisches *close reading* der Festplatte mit der epistemologischen Suche nach einem »Ariadnefaden […], der uns aus der ›reinen‹ Zeichenwelt hinausführt«.[116] Um im Bild zu bleiben: Dass sich der digitale ›Irrgarten‹ – ein protokollogisch geknüpftes, hochgradig durchrationalisiertes Netzwerk, das aus User-Perspektive, so sich diese von den slicken Anwenderoberflächen abwendet, tatsächlich labyrinthisch anmuten kann – nicht einfach zugunsten medienmaterialistischer Selbstevidenzen auflöst, nur weil sich in der computerforensischen Kasuistik prinzipiell medienmaterialistische Durchgänge, Verbindungen, Kausalitäten finden lassen, verweist dann allerdings schon auf die Notwendigkeit, forensische Geltungsansprüche, die sich auf individuelle Spurmaterialien, konkrete Medientatorte, einzelne Fälle konzentrieren, nicht voreilig (oder gar digitalphobisch) zu extrapolieren. Denn eine medienmaterialistische Grundlegung des Digitalen, der Nachweis, dass es bei informationstechnischen Prozessen der Datenverarbeitung, wie reversibel und

115 Vgl. Susan Schuppli: »Walk-Back Technology: Dusting for Fingerprints and Tracking Digital Footprints«. In: *Photographies*, 6/1, 2013, S. 159-167.

116 Krämer, »Was also ist eine Spur?«, S. 12f.

unverbindlich sie auch scheinen mögen, prinzipiell zu physischen Inskriptionen und Materialeinsätzen kommt, übersetzt sich nicht automatisch in das, was Forensik in erster Linie ist: das Versprechen, Spuren nicht nur zu sichten und zu sichern, sondern auch fallbezogen intelligibel zu machen. Grundsätzlich lässt sich insofern sagen, dass jedwede computergestützte Medienforensik als qualitative digitale Methode verstanden werden kann – einer »Doppelung von Methode und Gegenstand« folgend, die nicht weiter erstaunlich, sondern eher gewöhnlich ist: »Das Wissen über digitale Kulturen wird in vielen Fällen mit Mitteln und Methoden generiert, welche solche Kulturen selbst zur Verfügung stellen.«[117]

Dass es Medienforensik nicht mehr mit einzelnen Rechenmaschinen und Festplatten, sondern mit vernetzten Computern und distribuierten Speichermedien zu tun hat, ist der Ausgangspunkt einer medienwissenschaftlichen Fallstudie von Matthew Fuller und Nikita Mazurov, die mittels forensischer Konzepte und Instrumente eine Perspektive auf die Komplexität digitaler Daten*übertragung* zu gewinnen versucht. Dabei geht es weniger um die materielle Faktualität von Inskription (wenngleich diese vorausgesetzt wird) als um Zirkulation, nicht um die Materialität von Datenspuren, sondern um eine forensische Analyse der medienlogistischen Mobilität, die digitale Spurbildung ermöglicht und infrastrukturiert. Komplex, unübersichtlich, analytisch schwer adressierbar ist dieser entgrenzte Übertragungsmedientatort, weil »die Übertragung der Daten jenseits ihrer Inhalte zum Dauerzustand unserer Umgebungen«[118] geworden ist. Dass digitale Objekte überaus beweglich, mit minimalem Aufwand kopier- und teilbar sind, eröffnet im Fall proprietärer Bilddaten, deren

117 Christoph Engemann, Till A. Heilmann, Florian Sprenger: »Wege und Ziele. Die unstete Methode der Medienwissenschaft«. In: *zfm – Zeitschrift für Medienwissenschaft*, H. 20, 1/2019, S. 151-161. Hier: S. 156.

118 Christoph Engemann, Florian Sprenger: »Im Netz der Dinge. Zur Einleitung«. In: dies. (Hg., 2015): *Das Internet der Dinge. Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*. Bielefeld, transcript, S. 7-58. Hier: S. 28.

»Urheber« über Patente und Lizenzbestimmungen Eigentums- und Verwertungsrechte geltend machen können, zugleich ein kommerzielles Einsatzfeld für forensische Praktiken. Denn die Permanenz von Datendistribution, der »Dauerzustand« des Sendens und Empfangens, ergibt ein dynamisches, sich quasi-echtzeitlich rekonfigurierendes, fortlaufend neu aggregierendes Spurenbild, das zwar nicht einfach arretiert und tatortforensisch »eingefroren«, gleichwohl aber kasuistisch rückwärtsgelesen werden kann.

Fuller und Mazurov befassen sich am Beispiel eines geleakten Oscar Academy Award Screeners – Quentin Tarantinos The Hateful Eight, der 2015 vor seinem offiziellen Kinostart über einschlägige BitTorrent-Seiten in raubkopierter Version in die Zirkulation gebracht worden war – mit dem medienforensischen Status einer steganografischen Copyright-Markierung digitaler Objekte – genauer: mit darüber operationalisierten Verfahren des sogenannten *traitor tracing*. Die massive Ausweitung der Spurenlage im Digitalen, die gerade auch die informationstechnisch datafizierten digitalen Übertragungen selbst betrifft, bei denen jeder Verbindungsaufbau – die Konnektivität selbst – diskrete, prinzipiell rekonstruierbare Spuren hinterlässt (zum Beispiel verbindungsprotokolltechnisch metadatierte), macht forensische Auswertung nicht unbedingt trivialer. Nicht die Flüchtigkeit digitaler Datenspuren ist das Problem, sondern ihre hochdynamische, quasi-echtzeitliche Evolution und Proliferation. Weil sich Forensik tendenziell nicht für Big Data interessiert, mehr Daten zwar mehr Mustererkennung ermöglichen, aber nicht unbedingt zu einem zielgenaueren forensischen *reverse engineering* konkreter Handlungen führen, weil es Forensik überdies nicht um korrelative Datenverarbeitung, sondern um die Spezifität ›kleiner Daten‹ geht, die als individuelle, unverwechselbare Spuren prozessiert werden, entstehen hier zunächst erhöhte Anforderungen forensischer Datenselektion, -filterung und -reduktion.

Im rekonstruierten Fall handelt es sich konkret um ein »digitales Wasserzeichen«, ein dateiintern hinterlegtes, encodiertes Muster, das nicht nur Datensätze authentifizierbar und Datenquellen identifizierbar, sondern auch Datenspuren einfacher und zielführender nachver-

folgbar machen soll: »[T]he proliferation of forensics includes the development of forms of technology that pre-structure objects in order to make them more susceptible to tracing.«[119] Die informationstechnische Bauweise dieser Objekte, das in ihnen prozessierte, auf die Erschwerung oder gar Blockade nichtautorisierter Zirkulation angewandte forensische Wissen, bietet aus medienwissenschaftlicher Sicht einen heuristischen Eintrittspunkt in die transmissionsintensive Verfasstheit digitaler Medienkulturen. Kurz gesagt: Fuller und Mazurov blicken mit (gegen-)forensischen Methoden[120] auf die Distributionsgeschichte eines Datensatzes, der forensisch (vor)informiert ist. Der imprägnierte proprietäre Bilddatensatz rechnet also damit, zum Sachbeweis – genauer: zur Adresse eines weitläufigen Übertragungsmedientatorts – zu werden, antizipiert und befördert Spurbildung und bereitet die Verfolgung und Identifizierung involvierter Akteure vor.

Das allgemeine Ziel, Praktiken der Bilddatendistribution zu detektieren, die eine kriminelle Handlung darstellen, findet sich grundsätzlich nicht nur im Kontext von Copyright und Digital Rights Management (DRM). So hat Hany Farid mit der *robust image hashing technology* PhotoDNA ein bildforensisches Verfahren entwickelt, um fotografisches und videografisches Material, das mit sexueller Gewalt assoziiert ist, bereits im Moment eines versuchten Plattform-Uploads zu identifizieren, filtertechnisch zu blockieren und strafrechtlich verfolgbar zu machen. Voraussetzung dafür ist, einen bestimmten, bereits kriminalistisch markierten, also bekannten Bilddatensatz (selbst wenn er, durch den Bildausschnitt manipulierendes *image cropping*, softwaretechnisch verändert wurde) »robust«, mittels eines effizient und automatisiert komputierbaren (und deshalb leicht skalierbaren) »digital footprint« zu erkennen – egal, wo er auftaucht oder wer versucht,

119 Matthew Fuller, Nikita Mazurov: »A Counter-Forensic Audit Trail: Disassembling the Case of The Hateful Eight«. In: *Theory, Culture and Society*, 36/6, 2019, S. 171-196. Hier: S. 174.

120 Um die »gegenforensische« Theorie und Praxis von Forensic Architecture, auf die sich Fuller/Mazurov beziehen, wird es im nächsten Kapitel (III) gehen.

ihn erneut in die Zirkulation zu bringen. Genau diese Form der informationstechnischen Identifizierbarmachung durch Individualisierung leisten Hashing-Algorithmen: »[They] work by extracting a distinct digital signature from known harmful or illegal content and comparing these signatures against content at the point of upload. Flagged content can then be instantaneously removed and reported.«[121] Das inkriminierte Bildmaterial erhält hier zwar kein »digitales Wasserzeichen«, ist aber, nachdem der individuelle Hashwert kalkuliert und in einer kriminalistischen Datenbank hinterlegt wurde, mit einer algorithmisch adressierbaren DNA-Probe verbunden, einem Fingerabdruck, der jeden Kontakt in digitalen Übertragungskanälen signiert. Mit ähnlichen Verfahren arbeitet aber mittlerweile auch die automatisierte digitale Rechteverwaltung – etwa das »digital fingerprint system« der Plattform YouTube, das »Content ID« heißt und dafür Sorge tragen soll, dass der Anbieter nicht von Rechteinhabern, die ihren Content anders bewirtschaftet sehen wollen, verklagt wird.

Zurück zur Fallstudie von Fuller/Mazurov: Im Gestus einer kriminalistischen Ermittlung – »the counter-forensics audit trail is […] a thriller in itself«[122] – werden Dokumente (wie die 170 000 durch Wikileaks in Umlauf gebrachten internen Sony-Pictures-E-Mails), Patente von Forensic Coding Technology (die Generierung digitaler Wasserzeichen ist, hier schließt sich der Kreis, ihrerseits proprietär geschützt) und schließlich auch der piratisierte Datensatz selbst (*The.Hateful.Eight.2015.DVDScr.XVID.AC3.HQ.Hive-CM8*) bis auf die Mikroartefaktebene computerforensisch analysiert, um Funktionalität und Praxis des *traitor tracing* gegenforensisch zu exponieren:

> »A counter-forensic audit trail is […] a record constructed to disassemble black-boxed forensic events to discover how they may have

121 Hany Farid: »Fostering a Healthier Internet to Protect Consumers« (House Committee on Energy and Commerce). In: *https://congress.gov*, 16.09.2019. Vgl. dazu auch Simon Rothöhler: »Calm Images. The invisible visual culture of digital image distribution«. In: Olga Moskatova (Hg., 2021): *Images on the Move. Materiality – Networks – Formats*. Bielefeld, transcript, S. 73-86.

122 Fuller, Mazurov: »Counter-Forensic Audit Trail«, S. 189.

> occurred (and thus how they may be stymied in the future) […]. While covert and imperceptible watermarks may strive for unobservability in the service of facilitating streamlined traitor tracing, the role of counter-forensics is to render these processes observable and detectable so as to facilitate the unlinking of any ›traitor‹ from the leaked content. A subsequent aim of counter-forensics […] is to contest the forensic claim of being resistant to counter-forensics. In other words, by rendering the forensic trace function detectable or perceptible, paving the way for its removal or manipulation, counter-forensics contests the efficacy of forensic claims of detectability – effectively deploying forensic practices in the service of their own undoing.«[123]

Wo Forensik, wie Fuller und Mazurov zu Recht feststellen, in verschiedenen Anwendungskontexten »proliferiert«, zu einer von diversen Akteuren angewandten soziotechnischen Vorgehensweise wird, die auf die aufwandlose Verbreitung digitaler Daten und auf die Persistenz digitaler Datenspurbildung reagiert, ist Forensik wenn nicht die einzige, so doch eine naheliegende methodologische Option: des Rückwärtslesens von Praktiken, Prozessen und Techniken des Rückwärtslesens.

Dass seit einiger Zeit auch die Medienwissenschaft vermehrt von forensischen Methoden, den damit verbundenen Denkfiguren, Konzepten, Argumentationsweisen Gebrauch macht, hat, wie eingangs gesagt, vor allem mit der Komplexität und Verteiltheit jener großtechnischen Systeme, Netzwerke, Infrastrukturen zu tun, die der Operativität digitaler Medienkulturen zugrunde liegt. Immer häufiger sind es lediglich kleine Ausschnitte, mikroskopische Details, residuale Fragmente, die zum Gegenstand medienwissenschaftlicher Analytik werden. Hinzu kommt, dass weite Teile der solchermaßen in den Blick genommenen Medientatorte proprietär geblackboxt und selbst mit Informatik-Expertisen, die jenen professioneller Coder:innen entsprechen, nur sehr eingeschränkt auslesbar sind. Eine Heuristik, die, wo die wirklich ›großen Daten‹ ohnehin unerreichbar, da privatwirtschaftlich

123 Ibid., S. 180, 182f.

kommodifiziertes Konzerneigentum sind, von Details und Restbeträgen ausgeht, die mit dem arbeiten muss, was übriggeblieben ist, rechnet nicht lediglich defätistisch mit dem eigenen Zuspätkommen, sondern versetzt sich zugleich in die Lage, aus dieser Konstellation materialnahe Epistemologien der Nachträglichkeit zu entwickeln. Eine Heuristik, die darauf abzielt, aus unklar zusammenhängenden, verstreut auftauchenden, zunächst vielleicht sogar rätselhaft anmutenden Spurpartikeln Modelle größerer Zusammenhänge, Versionen indizienbasiert zusammengesetzter Abläufe zu gewinnen, muss nicht auf *crime labs* beschränkt bleiben und kann auch in anderen Anwendungskontexten epistemischen Mehrwert generieren.

Die Forensik ist, wie gezeigt, auf verschiedenen Ebenen in medienwissenschaftliche Diskurse und Arbeitsformen eingesickert, hält sich aber nicht nur in diesem relativen Off der Institution auf. Es scheint, als sei Forensik eine proliferierende kulturelle Praktik geworden. Zu beobachten ist jedenfalls, dass mit (quasi-)forensischen Methoden und Semantiken plausibilisierte Geltungsansprüche vermehrt auftauchen – gerade auch jenseits eines klar abgegrenzten Handlungsraums kriminaltechnisch regulierter Praktiken. Forensische Handlungen, Verfahren, Instrumente, die vormals ausschließlich in institutionalisierten Laboren, deren Operationen rechtlich codiert sind, ihren privilegierten Ort fanden, haben sich in neue Zusammenhänge und Kontexte eingetragen. Gegen- und anti-forensische Tendenzen digitaler Medienkulturen sind ebenfalls Teil einer vollständigen Lagebeschreibung. Was der Fall und beobachtbar ist, ist eine Diffusion, die den harten Kern kriminalistischer Forensik je nach Standpunkt aufweicht, unverbindlicher, problematischer, anfälliger für gezielte Störungen und Instrumentalisierungen macht – oder, diametral perspektiviert: die Forensik zivilgesellschaftlich anschlussfähiger, offener für kritische Inversionen und emanzipatorische Praktiken werden lässt. Wahrscheinlich findet beides zugleich statt – und ergibt einen Prozess, der nicht einfach komplementär, sondern in vielerlei Hinsicht verwickelt und widersprüchlich ist. Der in jedem Fall naheliegenden Diagnose, dass die Ausbreitung forensischer Praktiken über den (methodologischen) Sonderfall eines Forensisch-Werdens digitaler

Medienforschung hinausreicht, insofern es sich bei diesem Phänomen nicht nur um einen durchaus innovativen analytischen Zugriff auf digitale Medien, sondern auch um ein verändertes Verhältnis zu ihnen handelt, ist – weil gerade dieser Befund wiederum Gegenstand forensischer Medienforschung werden kann und sollte – das folgende Kapitel gewidmet.

Abb. II.1: Photographie métrique | 09.08.1913
Quelle: Polizeipräsidium Paris

Abb. II.2: Photographie métrique prise verticalment | Encadrement perspectomètre | 27.08.1905
Quelle: Polizeipräsidium Paris

Abb. II.3: Z+F IMAGER® 5010C, 3D Laserscanner (Zoller+Fröhlich)
Quelle: BLKA, Spiegel TV

Abb. II.4: Headset HTC Vive Pro
Quelle: BLKA, *Kriminalistik* 1/2019

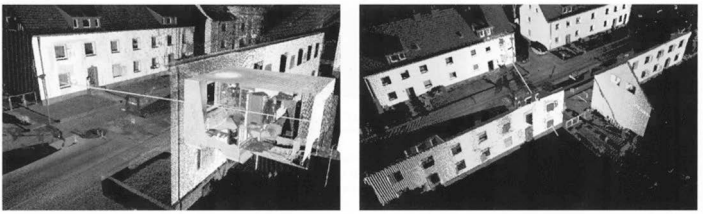

Abb. II.5: Tatörtlichkeit mit Schusswinkel-Rekonstruktion
Quelle: LKA NRW, *der kriminalist* 05/2006

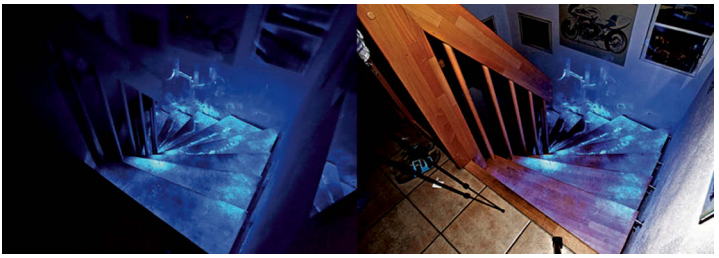

Abb. II.6: Integration von 2D-Luminolaufnahmen in den Laserscan: Fluoreszierendes Luminol (links) und verrechnetes Bild im Scan (rechts)
Quelle: BLKA, Zoller+Fröhlich

Abb. II.7: Darstellung des Sichtbereichs
Quelle: BLKA, Zoller+Fröhlich

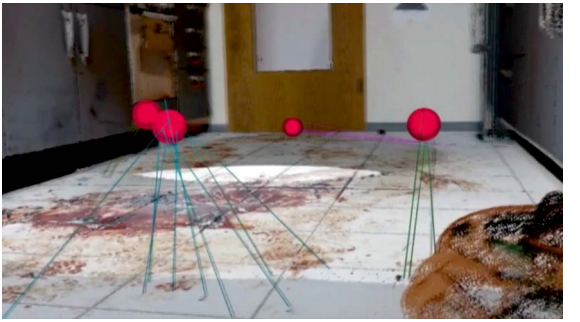

Abb. II.8: Ballistische Flugbahnen von Bluttropfen
Quelle: BLKA, Spiegel TV

Abb. II.9: Tathergangsrekonstruktion: Kombination aus Laserscans des Tatorts und Oberflächen- und CT-Scans des verstorbenen Opfers
Quelle: 3DZZ, *Kriminalistik* 2/2021

Abb. II.10: Multikamerasystem 3D-Fotobox, Forensisches Institut Zürich
Quelle: 3DZZ, *Kriminalistik* 2/2021

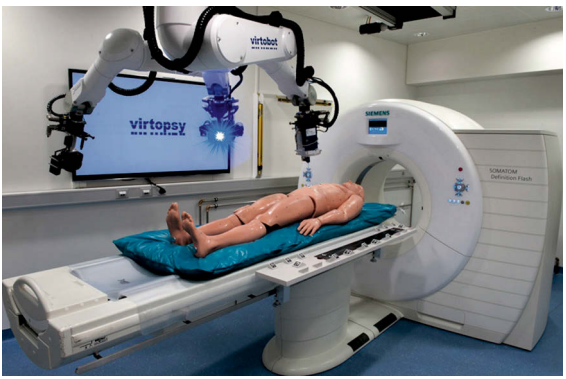

Abb. II.11: Virtobotsystem, IRM-UZH
Quelle: 3DZZ, *Kriminalistik* 2/2021