Dr. Uwe Ewald

Digitale Beweismittel und neue Wege der Strafverteidigung

Welche Herausforderungen stellt die Ausweitung informationstechnologischer Überwachungs- und Ermittlungsmethoden an die Strafverteidigung?[1]

> »The justice system is known for many things, but efficiency is not one of them. Neither is being up-to-speed with technology. One joke goes that the unofficial IT slogan of the courts is, 'Yesterday's technology, tomorrow!«[2]

I. Vorbemerkung

Der Begriff der ›Digitalisierung‹ wird in verschiedenen Bedeutungen verwandt.[3] Grundsätzlich beschreibt er einen tiefgreifenden Transformationsvorgang (›digitale Revolution‹), der die analogen, meist sinnlich-unmittelbar wahrnehmbaren Formen der Informations- und

1 Seit dem 42. Strafverteidigertag in Münster im März 2018 sind im Bereich der Digitalisierung der Gefahrenabwehr und Strafverfolgung weitere bemerkenswerte Entwicklungen u.a. zur Veränderung der Sicherheitsarchitektur, zu eEvidence und zu technologischen Fortschritten zu beobachten gewesen, welche die Herausforderungen an die Strafverteidigung im Umgang mit digitalen Beweismitteln weiter zugespitzt und deutlich gemacht haben. Diese schriftliche Fassung meines Vortrages bezieht deshalb auch einige dieser seit März 2018 eingetretenen Veränderungen ein, verbleibt aber im Übrigen in der Anlage und Struktur des Vortrages. Wesentliche Inhalte des Beitrages sind in Seminaren und Software-Trainings mit Strafverteidiger*innen präsentiert und diskutiert worden, so u.a. in Seminaren beim Republikanischen Anwältinnen- und Anwälteverein e.V. (RAV) im November 2017 und im Mai 2018. Den Seminarteilnehmer*innen sei für die aktive Debatte und produktive Hinweise gedankt.

2 In freier Übersetzung: Die Justiz ist für vieles bekannt, aber nicht für Effizienz und ebenso wenig dafür, technologisch aufgeschlossen zu sein. Ein Witz geht so: Der inoffizielle IT-Slogan der Gerichte ist: »Die Technologie von gestern ist gerade gut genug für morgen!« https://www.law.com/legaltechnews/sites/legaltechnews/2017/12/20/dutch-blockchain-company-legalthings-aims-to-update-criminal-justice/?slreturn=20180524061128, zuletzt besucht: 24. Juni 2018.

3 *Specht*, Ph., Die 50 wichtigsten Themen der Digitalisierung: Künstliche Intelligenz, Blockchain, Bitcoin Virtual Reality und vieles mehr verständlich erklärt, München: Redline Verlag 2018

Wissensverarbeitung in vielen Lebensbereichen mit digitalen Formen verbindet oder durch diese ersetzt. Digitale Informationsverarbeitung ist damit an den Gebrauch von Hard- und Software gebunden, mithin der direkten sinnlichen Wahrnehmung nicht zugänglich. Dieser Übergang von der analogen zur digitalen Informationsverarbeitung führt nahezu zwangsläufig (jedenfalls zunächst) zu einer ›digitalen Kluft‹ (›digital divide‹), der diejenigen *mit* Zugang und Fähigkeiten in der Beherrschung der notwenigen Hard- und Software von denjenigen *ohne* Zugang und Fähigkeiten unterscheidet.[4] Diese Effekte sind auch bei der zunehmenden digitalen Erfassung und Verarbeitung von Informationen im Rahmen des strafrechtlichen Beweisverfahrens zu beobachten.

Strafverteidigung ist zunehmend mit massenhaften digitalen Beweismitteln[5] konfrontiert. Besonders in sogenannten Umfangsverfahren zur organisierten (häufig grenzüberschreitenden) Kriminalität stützen sich die Ermittlungen auf den sogenannten ›digitalen Fußabdruck‹, der im Zuge der Tatbegehung vermeintlich hinterlassen wurde. Sie steht damit vor einer Herausforderung im Übergang von der analogen zur digitalen Daten- und Informationsverarbeitung im Beweisverfahren, die als unvermeidbare Folge der Digitalisierung von polizeilicher Gefahrenabwehr und Strafverfolgung durch Strafverteidigerinnen und Strafverteidiger zu bewältigen ist, jedenfalls dann, wenn Verteidigung unter Wahrung des Prinzips der Waffengleichheit in einem fairen Verfahren stattfinden soll.

Im Zusammenhang mit der Vorlage neuer EU-Rechtsvorschriften zu eEvidence[6] schätzt die Europäische Kommission ein, dass »bei mehr als der Hälfte aller Ermittlungen ein grenzüberschreitender Antrag auf Zugang zu elektronischen Beweismitteln gestellt (wird).

4 *Valadez*, J. R., & *Durán*, R. P., Redefining the Digital Divide: Beyond Access to Computers and the Internet. The High School Journal, 90(3), 2007, S. 31-44. doi:10.1353/hsj.2007.0013

5 Die Begriffe ›digitale Beweismittel‹ und ›eEvidence‹ werden in diesem Artikel synonym verwendet. Siehe aber Punkt II.3 zur Terminologie und Systematik der Begriffe ›eEvidence‹, ›digitale Beweismittel‹ und ›digitalisierte Beweismittel‹.

6 Vorschlag für eine ›Verordnung des Europäischen Parlamentes und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen‹, COM(2018) 225 final, 17.04.2018; Vorschlag für eine ›Verordnung des Europäischen Parlamentes und des Rates für zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren‹, COM(2018)0226 final, 17.04.2018

Für rund 85 Prozent der strafrechtlichen Ermittlungen werden elektronische Beweismittel benötigt, und in zwei Dritteln dieser Ermittlungen ist es notwendig, Beweismittel von Online-Dienstanbietern anzufordern, die sich in einem anderen Land befinden.«[7] Es bedarf vor diesem Hintergrund keiner besonderen Fantasie zu antizipieren, dass eEvidence als Massendaten zukünftig zur Normalität des Strafverteidigeralltags gehören wird.

Gleichwohl wird bei aller rasanten Entwicklung im technologischen Bereich und bei der Produktion digitaler Daten, die als Beweismittel im Strafverfahren eingebracht werden, Neuland betreten. Die prozessrechtlichen und praktischen Konturen im Umgang mit digitalen Beweismitteln durch die Prozessbeteiligten, sei es beispielsweise bei der Herausgabe von Smartphone-Images im Rahmen des Akteneinsichtsrechts oder bei der Überprüfung der Zulässigkeit, Zuverlässigkeit und des Beweiswertes digitaler Beweismittel, sind erst im Entstehen begriffen.[8] Ohne Übertreibung lässt sich feststellen, dass die Zuwendung von Politik und Gesetzgebung aber auch der Berufsvertretungen von Richtern, Staatsanwälten und auch Rechtsanwälten – so auch der Strafverteidigervereinigungen – trotz der bereits praktisch wirkenden Zwänge im Beweisverfahren unzureichend ist und die technologische Entwicklung die Strafjustiz – jedenfalls weitgehend[9] – vor sich hertreibt.[10]

In der heute gegebenen Situation ist kaum bestreitbar, dass technologiegetriebene Digitalisierung von Innerer Sicherheit und Strafjustiz das Verstehen und Bewerten der digitalen Beweismittel be- bzw. verhindert, die Unabhängigkeit der Justiz berührt und die Waffengleichheit für die Strafverteidigung untergräbt.

7 Europäische Kommission-Factsheet (2018a), Häufig gestellte Fragen: Neue EU-Vorschriften für die Beschaffung von elektronischem Beweismaterial, Brüssel, 17. April 2018, http://europa.eu/rapid/press-release_MEMO-18-3345_de.pdf, zuletzt besucht: 24.06.2018

8 *Weiß*, U., Elektronische Dokumente in der Hauptverhandlung nach neuem Strafverfahrensrecht. Wistra, 6, 2018, S. 245-251

9 scip, *Labs 9*, Zürich: Scip AG 2018

10 *Franzen*, R., Stellungnahme der Neuen Richtervereinigung (Landesverband Sachsen) zum Entwurf eines Gesetzes zur organisatorischen Verselbständigung der Leitstelle für Informationstechnologie der sächsischen Justiz vom 29.12.2017. Drucksache des Sächsischen Landtages, Nr. 6/12504, S. 26-31; *Quattrocolo*, S., & *Pagallo*, U., Fair Trial and the Equality of Arms in an Algorithmic Society. In: Padua Lima, M. L., Ghirardi, J. G. (Eds.), Global Law - Legal Answers for Concrete Challenges (pp. 246-276). Porto, Portugal: Editorial Juruá, 2018

Dazu ist hinter den z.T. schillernden Formen des Digitalen zu begreifen, dass wir am Anfang einer Entwicklung stehen, die darauf hinausläuft, eine nicht-humane Form künstlichen Denkens zu erzeugen, die auch in der politischen und justiziellen Entscheidungsfindung insbesondere zu komplexen Sachverhalten die menschlichen Möglichkeiten übertreffen wird. Damit ist die Grundfrage nach der Selbstbestimmung des Menschen (kleiner geht es leider nicht) und letztlich danach gestellt, ob und wenn ›ja‹ in welchem Ausmaß die Entscheidungsgewalt über existenzielle Fragen, wozu sicher die Rechtsprechung gehört, ›delegiert‹ werden sollen.

Wem das zu dystopisch oder unreal erscheint, hilft vielleicht die Lektüre von z.B. *Harald Welzer* (2017), *Yvonne Hofstetter* (2016) oder *Richard David Precht* (2018)[11] oder ein Blick in gegenwärtige Entwicklungen von Künstlicher Intelligenz in ihrer Verbindung zu Legal Tech und Sicherheitsszenarien, um etwas Nachdenklichkeit hervorzurufen. Wer die kritischen Ansichten von Yvonne Hofstetter oder Harald Welzer, die – sicher in provozierender Absicht – ›Das Ende der Demokratie‹ oder die ›Smarte Diktatur‹ als mögliche Folge der Digitalisierung der Gesellschaft sehen, einfach als ›Verschwörungstheorie‹ abtut, macht es sich gewiss zu leicht.

Aber richtig ist auch: Noch ist es trotz aller Anfänge nicht so weit. Daraus ergibt sich die Chance, sich auf diese Entwicklungen effektiv einzustellen und die Vorteile und Risiken computer- und softwaregestützter Verarbeitung von elektronischen Massendaten im Rahmen des Strafverfahrens zu verstehen und eigene Kompetenzen zu entwickeln.

Ein gerade erschienener Beitrag von *Serena Quattrocolo* und *Ugo Pagallo* (2018)[12] beschäftigt sich mit den möglichen Folgen der Digitalisierung auf das Strafverfahren und insbesondere eine aus Sicht der Autoren mit den Techniken der digitalen Beweiserhebung nahezu zwangsläufig verbundene Gefahr der Verletzung von Artikel 6 Abs. 1 EMRK.

11 *Welzer*, H., Die smarte Diktatur. Der Angriff auf unsere Freiheit, Berlin: Fischer 2017; *Hofstetter*, Y., Das Ende der Demokratie: Wie die künstliche Intelligenz die Politik übernimmt und uns entmündigt. München: C. Bertelsmann 2016; *Precht*, R. D., Jäger, Hirten, Kritiker: Eine Utopie für die digitale Gesellschaft. München: Goldmann 2018

12 *Quattrocolo* & *Pagallo*, 2018 (Fn. 10)

Nach *Quattrocolo* und *Pagollo* greift der Gebrauch von Techniken der digitalen Massendaten-Analyse und Künstlicher Intelligenz im Bereich der Strafrechtsanwendung tief in die bisherige Art der Herstellung individueller strafrechtlicher Verantwortlichkeit ein und berührt insbesondere das individuelle Recht auf ein faires Verfahren und Waffengleichheit nach Artikel 6 Abs. 1 der EMRK. Es wird insbesondere auf die Wissens-Asymmetrie zwischen Anklage und Verteidigung hingewiesen, die aus dem ungleichen Zugang zu digitalen Beweismitteln und deren Verarbeitung resultiert. *Quattrocolo* und *Pagollo* gehen dabei so weit, die Offenlegung des Quellcodes von Software, mit der digitale Beweismittel erzeugt wurden, als ein Mittel der Herstellung der Waffengleichheit zu fordern.

Die Frage, ob die computergestützte Erzeugung von beweiserheblichen Daten zu einer Verletzung von Artikel 6 Abs. 1 EMRK führt, muss sicher nicht allein an der Überprüfung des Quellcods der verwendeten Software festgemacht werden. Es geht vielmehr um die Nachvollziehbarkeit der mit Software-Hilfe erzeugten beweiserheblichen Befunde unter methodischen Gesichtspunkten der Reliabilität, Validität, Objektivität und Plausibilität. Und diese Nachvollziehbarkeit kann auch auf anderem Wege (in der Regel sogar einfacher) als durch Offenlegung und Expertenanalyse von Quellcodes sichergestellt werden (siehe Punkt II.3).

Derzeit ist ein *Ungleichgewicht zwischen Anklage und Verteidigung* festzustellen, das als ›digitale Kluft‹ in den jeweiligen Kompetenzen und Möglichkeiten der Verarbeitung elektronischer Beweismittel bezeichnet werden könnte. Während sich die Staatsanwaltschaft mithilfe der massiven digital-forensischen Infrastruktur der Polizei nicht nur digitale Massendaten als beweisrelevante Informationsbasis in großem Umfang verschafft und auch über den behördlichen Zugang zu Experten und damit grundsätzlich über die Kompetenz der Auswertung verfügt, erlangt die Strafverteidigung über Akteneinsicht und Inaugenscheinnahme Kenntnis von Daten und Datenträgern bzw. deren Inhalten, wenn ihrem Ersuchen stattgegeben wird. Schließlich im Besitz der elektronischen Massendaten, stellt sich die Frage einer effektiven Aufbereitung und Auswertung, für deren Lösung bislang – betrachtet man die Gesamtsituation – noch keine befriedigende Antwort gefunden wurde, mehr noch, es droht die Gefahr, dass sich die

›digitale Kluft‹ zwischen Anklage und Verteidigung ausweitet und die Strafverteidigung hoffnungslos ›abgehängt‹ wird. Die Frage ist also: »Kann David mit Goliath Waffengleichheit herstellen – und wenn ja, auf welche Weise?«

Um diese Frage in wesentlichen Zügen zu reflektieren, beschäftigt sich dieser Beitrag zunächst in Punkt II mit einigen Hintergründen und den ›treibenden Kräften‹ der Digitalisierung im Bereich polizeilicher Gefahrenabwehr und Ermittlungstätigkeit und daraus folgenden Konsequenzen für den Übergang zur digitalen Informationsverarbeitung im Strafverfahren. In Punkt III werden dann analytische und informationstechnische Herausforderungen für die Strafverteidigung betrachtet, die sich als neue Kompetenzen digitaler Informationsverarbeitung im Beweisverfahren im Umgang mit Hard- und Software darstellen lassen. Punkt IV wird im Sinne eines Ausblicks kurz auf mögliche Szenarien des zukünftigen Umgangs mit digitalen Beweismitteln aus Sicht der Strafverteidigung eingehen.

II. Digitalisierung von Innerer Sicherheit und Strafverfolgung

1. Kontext & Hintergründe

Eine immer noch verbreitete Ansicht scheint darauf hinaus zu laufen, es handele sich bei der Digitalisierung im Bereich von Gefahrenabwehr und Strafverfolgung um eine weitgehend technologische Angelegenheit, welche die bisherige analoge Datenverarbeitung besonders im Beweisverfahren eben schneller und effizienter und auch kostengünstiger und energiesparender (der wohl zurzeit größte Trugschluss) nun mit Computer und Software in digitaler Weise durchführen lässt bzw. bereits bestehende Praktiken nur effektiver und kostensparender fortgeführt werden. Und im übrigen könne man sich der technischen Entwicklung ohnehin nicht entziehen und müsse sich ihr anpassen.[13]

Um die Dimensionen des Konzepts und der Praxis der ›„digitalen Beweismittel‹ in ihrer Tiefe wenigstens annähernd zu erfassen, kommt man nicht umhin, Kontext und einige Hintergründe zu den Grundzügen der Digitalisierung im Bereich Inneres und Strafjustiz[14][15] zu beleuchten. Am Ende wird es um die entscheidende Frage gehen, welche Effekte die Digitalisierung im Bereich von Sicherheit und Strafjustiz auf die informationellen Entscheidungsgrundlagen und die Unabhängigkeit und Selbständigkeit von Gericht, Staatsanwaltschaft und Verteidigung hat und wie die Strafverteidigung die Rechte von Beschuldigten und Angeklagten in ihrer physischen und auch digitalen Existenz (›physical and digital self‹) durch fachgerechte Überprüfung der Rechtmäßigkeit, Zuverlässigkeit und des Beweiswertes elektronischer Beweismittel schützen kann.

Wenn Strafverteidigung dem Staat in seiner Definitionsmacht der ›Abweichung‹ und einem darauf fußenden Sanktionsanspruch aus gutem Grund Grenzen setzt – *welche Folgen hat dann die Veränderung*

13 Ein Disput im Plenum des Sächsischen Landtags am 13. Dezember 2017 zwischen dem Abgeordneten der Fraktion DIE LINKE, Klaus Bartl und dem damaligen Staatsminister des Innern, Markus Ulbich, macht dieses verbreitete Missverständnis auf Seiten politischer Entscheidungsträger hinsichtlich der Risiken von Digitalisierung für eine rechtsstaatliche Strafjustiz deutlich. Bartl hatte angezweifelt, dass sich mit der Einrichtung des Gemeinsamen Kompetenz- und Dienstleistungszentrums (GKDZ) zur Zentralisierung der Telekommunikationsüberwachung in fünf Bundesländern unter Beteiligung von Sachsen »mit dieser hoch institutionalisierten digitalen Verfahrensbearbeitung keine Unterschiede qualitativer Art für die Beteiligten am Strafverfahren im Verhältnis zur analogen Aktenführung im Zuge der Ermittlungen zu Strafverfahren eintreten«. Darauf Ulbig: »Telekommunikationsüberwachung, wie wir sie – so viel zu Ihrem Thema, Herr Bartl – bereits jetzt in den jeweiligen Landeskriminalämtern und danach auch im GKDZ betreiben, dient der Aufklärung schwerer Straftaten; ... Ich habe bei dieser Diskussion, die Sie jetzt geführt haben, überhaupt nicht verstanden, wo Sie das Problem haben; (Albrecht Pallas, SPD: Das wundert mich jetzt nicht!) denn die Arbeit, die jetzt vom LKA erledigt wird, wird in Zukunft genauso im GKDZ stattfinden... Bei der Einrichtung des GKDZ geht es aber nicht darum, auf dem neuesten Stand der Technik zu sein, sondern wir müssen auch mit den Technologien von morgen Schritt halten.« (Plenarprotokoll, 2017).

14 Mit dem Verweis auf »Inneres und Strafjustiz« wird die von der Europäischen Union bezeichnete »Area of Freedom, Security and Justice« umschrieben.

15 *Monroy*, M., Diskussion zu ›elektronischen Beweismitteln‹. In: CILIP 116, 2018 https://www.cilip.de/2018/06/24/diskussion-zu-elektronischen-beweismitteln/, zuletzt besucht: 26. Juni 2018; *ders.*, SIS II wächst kontinuierlich. In: CILIP 116, 2018, https://www.cilip.de/2018/06/24/sis-ii-waechst-kontinuierlich/, zuletzt besucht: 26. Juni 2018

der Arbeitsweise des strafenden Staates vom Analogen zum Digitalen für die Verteidigung?

Die Digitalisierung des ›Raums der Freiheit, der Sicherheit und des Rechts‹ und damit auch des Strafverfahrens bedeutet einen Paradigmenwechsel der Informationsverarbeitung vom traditionellen (primär) analogen ›Aktenstudium‹[16] hin zur (primär) computer- und softwaregestützten Datenverarbeitung mit Blick auf

- die *Erfassung, Speicherung und Aufbereitung* fallrelevanter digitaler und digitalisierter (Massen-)Daten (elektronischer Daten),
- deren ebenso computergestützten *Analyse und Verdichtung* zu beweiserheblichen Informationen/Befunden und schließlich
- die Verarbeitung dieser Informationen und *Präsentation* (Verschriftlichung/Visualisierung) als Beweisergebnis (›prozessuale Wahrheit‹).

Die zunehmende Anwendung von Informations- und Kommunikationstechnologien bei der Begehung von Straftaten auf der einen wie bei ihrer Verfolgung auf der anderen Seite wirft die bereits genannten kritischen Bedenken in Bezug auf die Aufrechterhaltung rechtsstaatlicher Grundsätze wie z.B. des fairen Verfahrens und der Waffengleichheit auf, verbunden mit der grundsätzlichen Frage, ob der David der Strafverteidigung dem digital aufgerüsteten Goliath auf Seiten der Sicherheits- und Ermittlungsbehörden überhaupt noch auf Augenhöhe begegnen und folglich seine Verteidigerpflichten erfüllen kann.

Es wird hier die klare Auffassung vertreten, dass Strafverteidigung diese Herausforderung bewältigen kann, *wenn* die Unausweichlichkeit einer Kompetenzverschiebung in der Arbeitsweise der Strafverteidigung erkannt wird. D.h. Strafverteidiger und Strafverteidigerinnen sind (sicher auch arbeitsteilig und in unterschiedlichem Maße) einerseits gefordert, ein hinreichendes Verständnis von der neuen, digitalen Art der Informationsverarbeitung sowohl als Moment der Tatbegehung als auch im Hinblick auf die Gefahrenabwehr und Strafverfolgung zu entwickeln; andererseits müssen sie sich selbst in die Lage

16 Selbstredend ist auch Informationsverarbeitung im vordigitalen Zeitalter mehr als das Studium von Akten, aber sie basiert in jedem Fall wesentlich – ob z.B. durch Vernehmung von Zeugen und Beschuldigten oder die Inaugenscheinnahme von Tatmitteln – auf der sinnlich-unmittelbaren Wahrnehmung von Informationen.

versetzen, Methoden der digitalen Datenverarbeitung anzuwenden – entweder in selbständiger Arbeit oder in Zusammenarbeit mit Experten im Bereich der digitalen Forensik bzw. Massendatenanalyse.

Im Grunde sprechen wir hier von einem Prozess lebenslangen beruflichen Lernens und eines Wandels zum ›DigiTorney‹ (digital attorney). Würde diese Zuwendung zu den digitalen Herausforderungen nicht stattfinden, liefe die Strafverteidigung (eine in Ansätzen bereits zu beobachtende) Gefahr, die Präsentation von auf elektronische Daten gestützten Beweismitteln durch die Staatsanwaltschaft nicht mehr ausreichend in ihrem Zustandekommen zu verstehen und ihre Integrität und Authentizität und damit ihren Beweiswert nicht mehr unabhängig überprüfen zu können – nicht zu reden von dem eintretenden Verlust der Fähigkeit, punktuell eigene Analysen der in das Strafverfahren eingeführten digitalen Daten durchführen zu können.

Der strategische Charakter der Veränderungen wird sichtbar, wenn man sich verdeutlicht, dass sich nicht nur die Methoden und Techniken der Informationsverarbeitung im Ermittlungs- und Strafverfahren verändern, sondern die Grundlagen und Prinzipien der Entscheidungen zu ›Abweichung‹ und ›Sanktion‹ infolge der Digitalisierung verschoben werden.

Die am Beispiel neuer Polizeigesetze in Bayern und weiteren Bundesländern konkret gewordene massive Veränderung der Sicherheitsarchitektur in Deutschland,[17] eingebettet in die neue interne Sicherheitsstrategie der Europäischen Union[18] macht diese qualitativen Verschiebungen deutlich, die nur vor dem Hintergrund der Digitalisierung und der daraus resultierenden Möglichkeiten von Überwachung und Risikoeinschätzung bzw. Risikoprognose zu verstehen sind.

17 Löffelmann, M., Die Zukunft der deutschen Sicherheitsarchitektur – Vorbild Bayern?, in: Zeitschrift für das Gesamte Sicherheitsrecht. Europäisches und Deutsches Sicherheitsrecht/Sicherheitspolitik, 3/2018, 85-91, S. 85*ff*.

18 Europäische Union, Die Europäische Sicherheitsagenda. MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN. COM(2015) 185 final, 2015

Zunächst kann in diesem Zusammenhang von zwei sich wechselseitig verstärkenden Trends ausgegangen werden:

(1) Durch-Digitalisierung aller Lebensbereiche

Als Folge des rasanten technologischen Fortschritts und der nahezu ungebremsten Einführung von ITK (Informations- und Kommunikationstechnik) nach dem Prinzip der technologischen Machbarkeit und unter dem Mantra der Vereinfachung und Lösung von Problemen durch Digitalisierung und Big Data (›das neue Öl‹) kommt es zum massiven Auf- und Ausbau einer ITK-Infrastruktur mit entsprechenden Experten und in der Folge zu einer permanenten exponentiell anwachsenden Anhäufung von personenbezogenen Massendaten.[19] Diese ›digitale Identität‹ (›digital self‹), deren Entstehen am Ende durch niemanden zu verhindern ist, enthält auch den ›digitalen Fussabdruck‹ von Verhalten, das als Straftat angeklagt wird.

(2) Entstehen einer daten-getriebenen Sicherheitsarchitektur

Es wird eine »›Vernachrichtendienstlichung‹ des Polizeirechts und des Strafverfahrensrechts« antizipiert und eine Entgrenzung polizeilicher Befugnisse und Ausweitung von Überwachung in das Vorfeld einer Gefährdung (›drohende Gefahr‹) in der Weise festgestellt, dass Polizei als Datenbeschaffer (z.T. in Echtzeit) im Rahmen der Gefahrenabwehr mit fließenden Grenzen zur Verwendung der Daten im Ermittlungs- und Beweisverfahren agiert.[20]

Auf der Digital Investigation Conference 2018[21] wurde mit Blick auf die wahrscheinlichen Entwicklungen in den nächsten zehn bis fünfzehn Jahren von KPMG, einer der ›Big Four‹-Wirtschaftsprüfungsgesellschaften, die selbst digitale Forensik und Datenanalyse betreiben,[22] ein Szenario vorgestellt, das (A) die radikale Transformation durch Digitalisierung in allen Lebensbereichen in den nächsten 15 Jahre beschreibt, welche (B) in der Folge zu völlig neuen Formen der polizeilichen Ermittlungsarbeit – und damit von digitalen Beweismitteln – führen wird.

(A) Strategische Technologien werden nach dieser Prognose komplexe soziale und technische Prozesse steuern und datenmäßig erfassen. Von ›digital twins‹, ›IoT platforms‹ und ›smart cities‹ über ›neuromorphic hardware‹, zu ›Brain Computer Interface‹ und ›human augmentation‹ wird eine Entwicklung stattfinden, in der die Grenzen zwischen dem ›Physischen‹, dem ›Virtuellen‹ und dem ›Biologischen‹ verschwimmen und damit auch die Wahrnehmung von und polizeiliche Ermittlungsarbeit zu wesentlichen Bereichen strafbaren Verhaltens, das sich in eben diesen ›Räumen‹ abspielt, zunehmend betreffen.

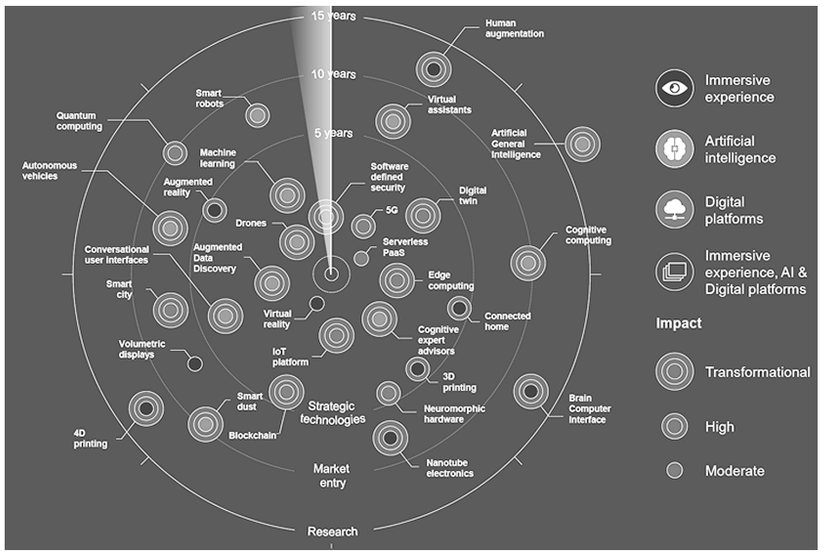
19 Wer immer noch Zweifel daran hat, dass sich dieser Trend der Durch-Digitalisierung aller Lebensbereiche tatsächlich durchsetzt und keiner Wahnvorstellung von Digitalisierungsgegnern entspringt, werfe einen Blick auf ›i.Con Smart Condom‹ (https://britishcondoms.uk/i-con-smart-condoms.html - zuletzt besucht: 26. Juni 2018) – »Welcome to the future of wearable technology in the bedroom.«

20 *Löffelmann* 2018 (Fn. 17), S. 86*ff.*

21 DIC - Digital Investigation Conference 2018, http://www.digitalinvestigationsconference.ch/zurich/agenda/index.html zuletzt besucht: 26.06.2018

22 Siehe KPMG ›Forensic Investigations‹, »Unabhängige unternehmensinterne Ermittlungen bei Verdacht wirtschaftskrimineller Handlungen auf Basis erprobter Methoden.« https://home.kpmg.com/de/de/home/dienstleistungen/audit/forensic/forensic-investigations.html - zuletzt besucht: 26. Juni 2018. Die ›Big Four‹ Deloitte, Ernst & Young (EY), KPMG und PricewaterhouseCoopers (PwC) besitzen im Bereich der Digitalisierung von Polizei und Justiz europaweit eine erhebliche Gestaltungsmacht. Z.B. ist PwC maßgeblich in die Digitalisierung der Justiz von Großbritannien involviert.

Grafik 1: IKT-Entwicklung der nächsten 15 Jahre – potenziell digitale Beweismittel



Quelle: KPMG (2018)

Auf Legal Tech-Konferenzen[23] und Veranstaltungen zu digitaler Polizeiarbeit[24] ist seit mehreren Jahren eine sich zunehmend intensivierende Debatte zwischen Polizei, verantwortlichen Regierungsstellen und der IT-Wirtschaft festzustellen. Wie eine Studie belegt, hat sich auch der Anteil der IT-Privatwirtschaft an der EU-geförderten Sicherheitsforschung ständig erhöht.[25]

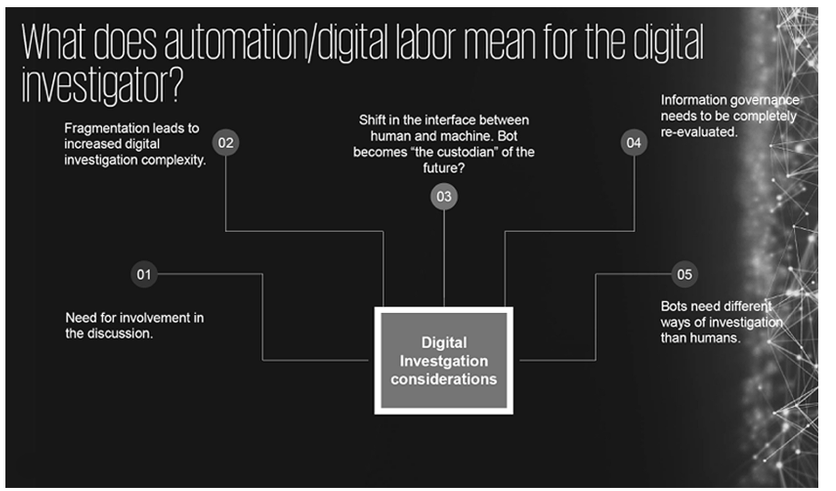
23 Z.B. LEGAL ®EVOLUTION, »Die größte Kongressmesse für Legal Innovation in Europa«, https://legal-revolution.com/de/, zuletzt besucht: 26. Juni 2018.

24 Z.B. Spezialmesse zur Digitalisierung der Inneren Sicherheit!, http://www.gpecdigital.com/de/, zuletzt besucht: 26. Juni 2018. »Für wen ist die GPEC® digital? Einfache Rechnung: Digital + Innere Sicherheit. Ihre Behörde kämpft für Innere Sicherheit im digitalen Wandel? Sie schaffen als Unternehmen Sicherheitsprodukte mit digitaler Struktur? Sie streiten als Experte für innovative Ansätze? Schlagworte wie Cybersecurity, Smart Policing und Smart Cities, KI-basierte Technologie, Intelligente Überwachung, Datenhaus Polizei, Critical & Mobile Communications und Vernetzung von Mensch und Fahrzeug sind für Sie keine Worthülsen, sondern Ihr tägliches Einsatzgebiet? Dann willkommen auf der GPEC® digital 2019!« Oder die ›Digital Investigations Conference‹ (DIC), Zürich, http://www.digitalinvestigationsconference.ch/zurich/, zuletzt besucht: 26. Juni 2018.

25 *Jones*, C., Market forces: The development of the EU security-industrial complex. London, UK: Transnational Institute, Statewatch, 2017

(B) Die wesentlichen Folgen für die Ermittlungstätigkeit und Beweiserhebung zu kriminellem Verhalten wird – so die Vorhersage – einerseits in einem enormen Anwachsen sowohl des Umfangs als auch der Komplexität digitaler Ermittlungstätigkeit und damit in deren Ergebnis digitaler Beweismittel führen[26]; andererseits wird durch ein verändertes Verhältnis von Mensch und Maschine, den (intelligenten) Maschinen (Bots = Roboter/Software) bei der Aufklärung von Straftaten eine zentrale Rolle zukommen, was zu einem Umdenken in der Informationsverarbeitung bei der Strafverfolgung führen wird.

Grafik 2: Zukünftige Perspektiven digitaler Ermittlungstätigkeit der Polizei



Quelle: KPMG (2018)

Als Folge dieses Digitalisierungstrends ist neben dem Anwachsen von Big Data eEvidence eine zunehmend computergestützte Einschätzung von Gefahrensituationen und ›Gefährdern‹ (der potenzielle ›Gefährder‹ wird primär zum Objekt der Erkenntnis (Scoring), nicht die ›akute Gefahr‹ bzw. strafbare Handlungen und ihre kausale Zuordnung zu Personen), die Grundlage juristischer Entscheidungen, die sich zudem auf eine informationstechnologische Infrastruktur bezieht (siehe oben »Emerging technology radar«), welche ohne Expertenwissen nicht zu verstehen ist.

26 Siehe neuere Trends in der Car- und Drone-Forensik zur Sammlung digitaler Beweismittel.

Vor diesem Hintergrund der IT-Entwicklung darf man sich schon fragen, inwieweit die Digitalisierung des Erkenntnisverfahrens ein politisch-justiziell ›gesteuerter‹ und in seinen wesentlichen Wirkungen bewusst wahrgenommener und gewollter Prozess oder aber ein sich weitgehend selbststeuernder, technologie-getriebener Mechanismus ist, der von dem Glauben getragen ist, auf diesem Wege sei am Ende nicht nur im Einzelfall ein Ermittlungserfolg zu erzielen, sondern tatsächlich ein Mehr an Sicherheit *und* Freiheit (d.h. insbesondere Schutz von Grundrechten) zu erreichen. Es wird also nicht gefragt, welche Sicherheit soll mit welchen Mitteln (darunter Möglichkeiten der Digitalisierung) erreicht werden, sondern die technischen Möglichkeiten der Digitalisierung werden unmittelbar als zentrales Mittel der Lösung von erheblichen Sicherheitsproblemen dargestellt – im Zweifel unter Einschränkung von Grundrechten.

Evgeny Morozov hat diese Sichtweise im Sinne einer »eigenständigen Rechtfertigungsordnung«[27] als »Solutionism«[28] bezeichnet, einer Perspektive, in der die Digitalisierung – etwas vereinfacht ausgedrückt – als effektive Antwort auf Probleme verstanden wird, ohne dass nach den Ursachen dieser Probleme gefragt werden muss. Mit Blick auf Gefahrenabwehr und Strafverfolgung scheint Digitalisierung so die in Echtzeit wahrgenommene Gefährdung und das Einschreiten idealerweise noch vor Eintreten einer akuten Gefahr zu ermöglichen und zudem basierend auf digitalen Massendaten sichere Beweise für eine Verurteilung zu liefern.

In Filmen wie ›Citizenfour‹ und ›Pre-Crime‹ werden diese bedrohlichen Entwicklungen bereits eindringlich dargestellt; gleichwohl kann man sich des Eindrucks nicht erwehren, dass sie überwiegend als virtuelles Spektakel eines ›digitalen Wahnsinns‹ auf der Leinwand missverstanden werden und nicht als ein (wahrscheinlich noch untertriebenes) Abbild tatsächlicher Vorgänge, von denen wir bereits betroffen sind. Aber: Hinter diesem ›digitalen Wahnsinn‹ gibt es ein Design, ein Muster, einen ›Plan‹.

27 *Nachtwey*, O. & *Seidl*, T., Die Ethik der Sulution und der Geist des digitalen Kapitalismus, in: Institut für Sozialforschung (Hrsg.) IFS Working Paper #11, Frankfurt am Main 2017, S. 1

28 *Morozov*, E., To Save Everything, Click Here. Technology, Solutionism and the Urge to Fix Problems that Don't Exist. New York: Public Affairs, 2013

2. Die treibenden Kräfte – EU-Multi-Level-Governance, IT-Wirtschaft und Veränderung der Sicherheitsarchitektur

Um die Grundzüge der Digitalisierung des Strafverfahrens, die damit verbundenen Risiken für seine rechtsstaatlichen Prinzipien und letztlich Wege der Bewahrung von Waffengleichheit durch effektive Strafverteidigung im Umgang mit digitalen Massen-Beweismitteln zu verstehen, muss man zunächst nach Europa schauen – auch wenn es am Ende doch eigentlich (nur) darum geht, eine effektive Verteidigung beim Umgang mit digitalen Beweismitteln im konkreten Strafverfahren am Landgericht X in Deutschland zu gewährleisten.

These: Die treibende politische, rechtsetzende und exekutive Macht der Digitalisierung in den Bereichen von Sicherheit und Strafjustiz ist die Europäische Union. Der wesentliche Hebel zur Umsetzung der politischen Ziele einer digitalisierten Sicherheits- und Justizpolitik ist die Herstellung von Interoperabilität der EU-weit zum Einsatz kommenden IKT- Infrastruktur und entsprechender Softwarelösungen. Das Verstehen der Digitalisierung des Strafverfahrens muss deshalb hier ansetzen.[29]

Die Europäische Ermittlungsanordnung[30] (EEA) bietet ein hervorragendes Beispiel dafür, diese Zusammenhänge im Konkreten nachzuvollziehen. Mit Blick auf die Digitalisierung des Ermittlungs- und Strafverfahrens ist die Begründung des Gesetzentwurfs[31] (dem dann so auch vom Bundesrat zugestimmt wurde) auf S. 23 f. mit den Ausführungen zu Art. 7 (Vorgaben für die Übermittlung eines EEA

29 Um es hier an Deutlichkeit nicht fehlen zu lassen: Es ist nicht die politische Debatte um die in der Folge von Digitalisierung eintretende massive Veränderung von sozialer und strafrechtlicher Kontrolle und rechtsstaatlichen Prinzipien, in deren Ergebnis eine Grundentscheidung dahingehend gefällt wird, ob diese Folgen gewollt sind. Vielmehr wird - vor dem Hintergrund (hypertrophierter?) Terrorismusbedrohung und von Gefahren durch die grenzüberschreitende organisierte Kriminalität - über das weitgehend unwidersprochene Mantra der Notwendigkeit informationstechnischer Modernisierung zur Vollendung der ›Sicherheitsunion‹ (wesentlich über EU-Rechtsetzung) eine technologische und institutionelle Infrastruktur geschaffen, über deren Einführung Entscheidungsträger zu substanziellen Veränderungen veranlasst werden. In Kürze: IKT im Bereich AFSJ droht tendenziell Politik und Justiz zu ›entmündigen‹.

30 Umsetzung in Deutschland durch das ›Vierte Gesetz zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen‹ vom 5. Januar 2017 (Bundesgesetzblatt Jahrgang 2017 Teil I, Nr. 2, ausgegeben zu Bonn am 10. Januar 2017).

31 Deutscher Bundestag, 18. Wahlperiode, Drucksache 18/9757, 26.09.2016.

durch die Anordnungsbehörde) interessant. Voraussetzung für das Funktionieren der EEA ist danach das Zusammenwirken verschiedener Institutionen und Agenturen auf europäischer, Landes- und regionaler Ebene. Neben der Prüfung der rechtlichen Voraussetzungen besteht mit Blick auf die Verarbeitung digitaler Informationen und Beweismittel das Hauptproblem darin, die Authentizität und Integrität der übermittelten Daten zu gewährleisten. Dazu sind elektronische Signaturen erforderlich wie auch informationstechnische Vorkehrungen durch die Einrichtung entsprechender elektronischer Übertragungswege und Sicherheitssysteme zu treffen sind, welche die Identität des Absenders gewährleisten. Für die Bundesrepublik Deutschland gehört als zentraler Bestandteil zu diesen informationstechnischen Systemen das Elektronische Gerichts- und Verwaltungspostfach (EGVP).[32]

Um nun die EEA grenzüberschreitend innerhalb der EU zu übermitteln, ist die Anbindung des EGVP in eine EU-weite Infrastruktur zu gewährleisten. Diese wird über das im Aufbau befindliche Projekt des e-CODEX angeboten.[33] Mit dem Arbeitsprogramm der Europäischen Kommission für 2018 wurde der mit der EEA eingeschlagene Weg mit einem neuen Gesetzgebungsvorschlag erweitert.[34] Hierbei handelt es sich um Vorschläge für zwei Verordnungen,[35] welche die Vereinfachung des Zugangs zu eEvidence (hier bezogen auf elektronische Inhalte, die bei Internetdiensten in anderen Mitgliedstaaten oder Drittstaaten gespeichert sind) regeln sollen. Die Einbindung der

32 Anmerkung: Teil des EGVP ist das besondere elektronische Anwaltspostfach (beA).

33 Siehe: https://www.e-codex.eu - zur Beschreibung des Projekts und Video-Präsentation; https://www.e-codex.eu/partners/contact; https://www.e-codex.eu/node/129, zuletzt besucht: 26. Juni 2018. eCodex wird später als meCodex fortgeführt.

34 Anhang 1 zum ›Arbeitsprogramm der Kommission 2018‹, Nr. 16, »Vorschlag zur Verbesserung des grenzüberschreitenden Zugangs von Strafverfolgungsbehörden zu elektronischen Beweismitteln«. Neben Maßnahmen zur Vollendung des digitalen Binnenmarktes werden auch Bestimmungen im Bereich eGovernance überarbeitet (REFIT), und es wird die erweiterte Nutzung öffentlicher Daten angestrebt. Siehe auch Vorschlag zu einer Verordnung über die ›EU-Cybersicherheitsagentur (ENISA)‹ (Zertifizierung der Cybersicherheit).

35 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen COM(2018)0226 final; Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, COM(2018)0226 final.

entsprechenden nationalen Justiz-IT-Systeme in die EU-weite Infrastruktur wird für Deutschland maßgeblich durch das Ministerium der Justiz von Nordrhein-Westfalen getestet.[36]

Neben der Kommission sind auf EU-Ebene insbesondere das Europäische Justizielle Netzwerk (EJN) und Eurojust involviert. EJN-Kontaktstellen (auf Bundesebene am Bundesamt für Justiz, auf Länderebene überwiegend bei den Generalsstaatsanwaltschaften angesiedelt) besitzen einen Zugang zur sicheren Telekommunikationsverbindung des EJN. Eine direkte Verbindung zwischen der Anordnungsbehörde und der Vollstreckungsbehörde (gegebenenfalls unter Einbindung der genannten Zentralbehörden) ist ebenfalls vorgesehen.

Inwieweit zu einem späteren Zeitpunkt das besondere elektronische Anwaltspostfach (beA) als Teil des EGVP über Schnittstellen in dieses informationstechnische System eingebunden wird, ist bislang – soweit zu sehen ist – noch nicht substantiell thematisiert. In Bezug auf die technischen Standards des beA scheint die Interoperabilität jedoch gegeben zu sein.

Vor dem Hintergrund der Tatsache, dass Formen der schweren und organisierten Kriminalität regelmäßig grenzüberschreitender Natur sind,[37] bedarf es keiner besonderen Weitsicht festzustellen, dass die hier mit den europäischen Entwicklungen gesetzten Perspektiven und Standards im Zuge der technisch für das letztendliche Funktionieren dieser Infrastruktur notwendige Harmonisierung vollständig auf die nationalen Systeme durchgreifen wird.

Die hier über das Beispiel der Europäischen Ermittlungsanordnung und die Nachfolgeregelungen zur Erlangung von elektronischen Beweismitteln für den Justizbereich in Kürze nachgezeichneten Entwicklungen sind im Bereich der EU-weiten informationstechnischen Verbindung von Sicherheits- und Polizeibehörden bereits wesentlich weiter entwickelt und praktisch getestet.

36 Siehe: http://www.justiz.nrw.de/WebPortal_en/index.php, zuletzt besucht: 26. Juni 2018.

37 Siehe SOCTA2017, https://www.europol.europa.eu/socta/2017/, zuletzt besucht: 26. Juni 2018

Der Rat der Europäischen Union hat im Februar 2017 das Netzwerk der bestehenden IKT-Infrastruktur im Bereich der öffentlichen Sicherheit nachgezeichnet (siehe Grafik 3).[38]

Mit euLISA und ENISA entwickelt die EU mächtige Agenturen für das Management, die Kontrolle sowie die Entwicklung der IT-Systeme im Bereich von AFSJ insbesondere zur Gewährleistung deren Interoperabilität, darin eingeschlossen - so die Planung - das grenzüberschreitende EU-Justizportal eCodex.[39]

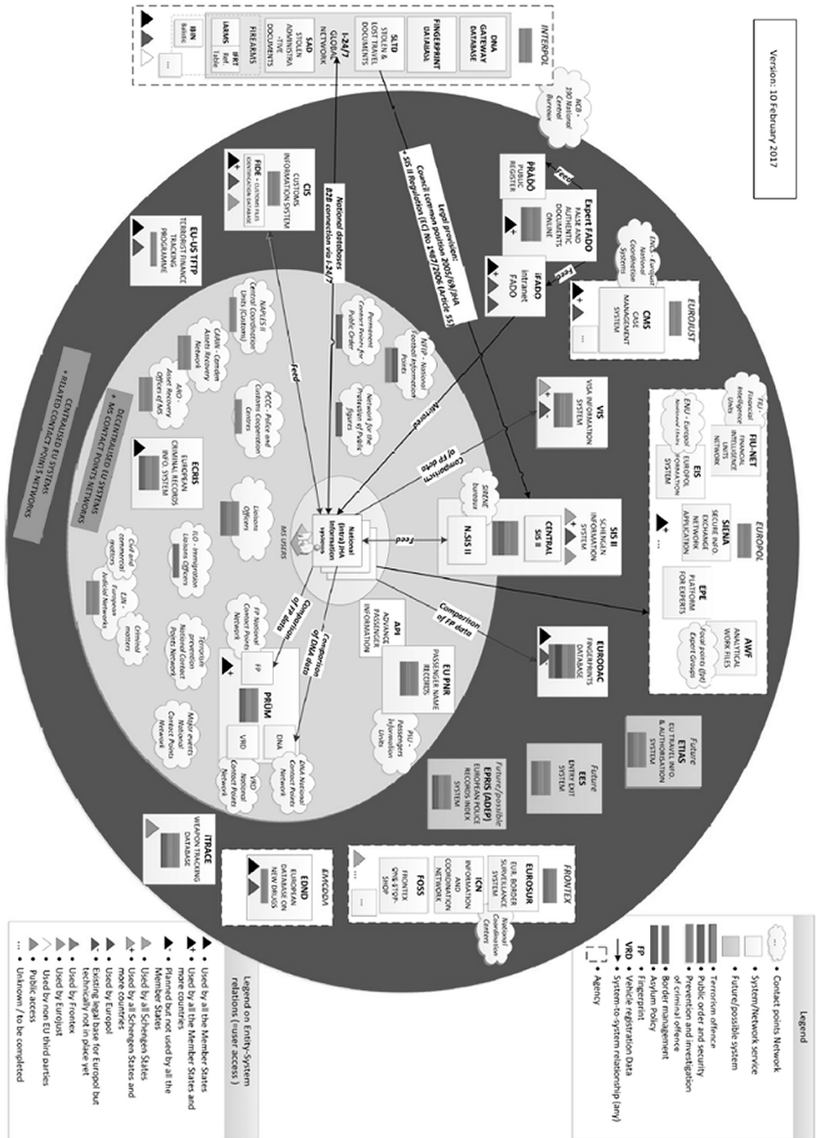
Die grundlegenden politischen Entscheidungen für die Fortsetzung dieser digitalen Sicherheitsintegration sind auf EU-Ebene bereits gefallen. Am 24. Oktober 2017 hat die Europäische Kommission ihr Arbeitsprogramm für 2018 vorgestellt[40], das die bislang bereits konsequent verfolgte Perspektive eines harmonisierten Informationsaustausches im Bereich ASFJ fortsetzt. Zwei Initiativen sind hier hervorzuheben: zum einen ein Vorschlag zu einem Gesetzesvorhaben zur Verknüpfung der EU-Informationssysteme für Sicherheits-, Grenz- und Migrationsmanagement und zum anderen als langfristige Maßnahme (»Zukunftsmaßnahmen«) die Erweiterung der Zuständigkeit der Europäischen Staatsanwaltschaft auf grenzüberschreitende terroristische Straftaten (angestrebter Zeithorizont 2025). Damit soll die »Vollendung der Sicherheitsunion« – als Priorität unter den Schwerpunkten der Kommission – insbesondere »zur Verbesserung des grenzübergreifenden Zugriffs der Strafverfolgungsbehörden auf

38 Council of the European Union. Overview of the information exchange environment in the justice and home affairs area, Brussels, 15 February 2017, 6253/17. »In the context of the implementation of the Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area (9368/1/16 REV 1) and the ongoing work in the High Level Expert group on information systems and interoperability, the General Secretariat of the Council has made an attempt to map the existing (and some future) information exchange instruments, networks and databases in the JHA field.«

39 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Ratsbeschlusses 2007/533/JI sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011, COM/2017/0352 final

40 Siehe Arbeitsprogramm der Kommission 2018, COM(2017) 650 final. https://ec.europa.eu/info/publications/2018-commission-work-programme-key-documents_en, zuletzt besucht: 26. Juni 2018

Grafik 3: Überblick zur EU-Infrastruktur des Informationsaustausches im Bereich öffentlicher Sicherheit



elektronische Beweismittel und Finanzdaten«[41] erreicht werden. Parallel wird der personen- und sachbezogene freie Datenaustausch im EU-Binnenmarkt und in der EU-Außenwirtschaft vorangetrieben (betrifft das Thema Umgebungsintelligenz, auch relevant für Gefahrenabwehr und Strafverfolgung).

Wie unschwer zu erkennen ist, sind in diesem System der AFSJ-IT-Infrastruktur die EU-Ebene, die Mitgliedsstaats-Ebene und die regionale (Länder-) Ebene *interoperabel* miteinander verbunden. Zwar spielen auch in diesem ITK-Gesamtsystem hierarchische Elemente der Über- und Unterordnung entlang der Linie ›EU-Bund-Länder‹ eine funktional bedingte Rolle (etwa dem Grundgedanken des Subsidiaritätsprinzips folgend), wenn es jedoch um die Frage des Datenaustausches (input/output) geht, können mit diesem Netzwerk verbundene Akteure auf allen Ebenen (mit unterschiedlichen Befugnissen) Daten einspeisen oder abrufen. Interoperabilität auf der technischen Seite geht am Ende mit Universalität der Nutzung der Daten (jedenfalls tendenziell) einher. Die Frage ist, ob das so gewollt ist.

Die polizeilichen Vorgangsbearbeitungssysteme und Dateien auf Bundes- und Landesebene spielen hierbei in Deutschland eine entscheidende Rolle;[42] auch aus der Sicht der Auswertung elektronischer Beweismittel in konkreten Strafverfahren ist das System und der Austausch von (überwiegend, aber nicht nur) personenbezogenen Daten im Verbundsystem polizeilicher Datenbanken von zentraler Bedeutung. Die weitere Operationalisierung und Konkretisierung dieses Systems wird auch in Deutschland massiv vorangetrieben,[43] da die derzeitige ITK-Infrastruktur föderal extrem zerklüftet ist und selbst vorhandene Informationen im operativen Betrieb nicht oder nur mit übermäßigen Aufwand zu finden sind.

41 Siehe Arbeitsprogramm der Kommission 2018, S. 9

42 Siehe »Vorgangsbearbeitungssysteme in deutschen Polizeibehörden« https://police-it.org/vorgangsbearbeitungssysteme-in-deutschen-polizeibehoerden , zuletzt besucht: 26. Juni 2018.

43 Der Kriminalist, die Fachzeitschrift des Bundes Deutscher Kriminalbeamter, berichtet in seiner November-Ausgabe 2017 auf Seite 31 ff. vom weiteren Ausbau des Polizeilichen Information- und Analyseverbundes (PIAV), der durch die Saarbrücker Erklärung der Innenminister von Bund und Ländern und das Programm Polizei 2020 noch einmal bekräftigt worden ist. Das PIAV wird durch den Fonds für die Innere Sicherheit der Europäischen Union kofinanziert.

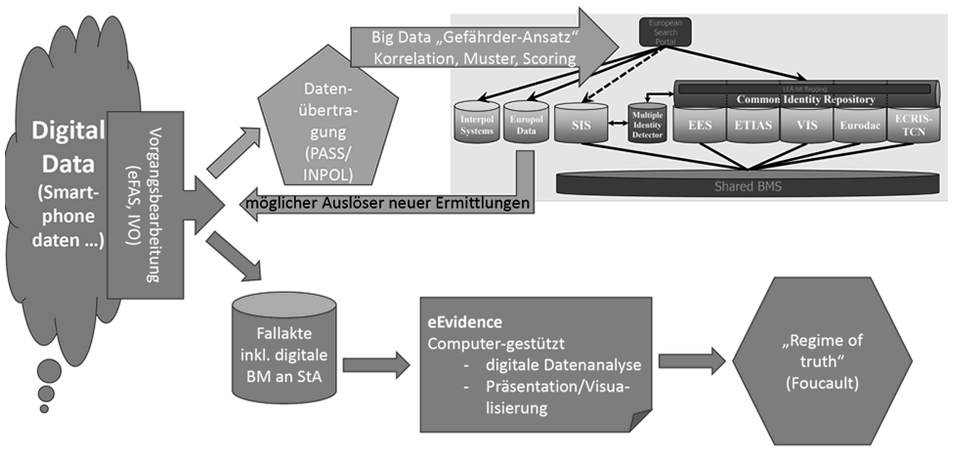
Was nun haben diese Groß- und Teilsysteme der IKT-Sicherheits- und Justizinfrastruktur mit der Verarbeitung von Massen-eBM in einem konkreten Strafverfahren zu tun?

Der zentrale Zweck dieser AFSJ-IKT-Infrastruktur besteht in der effektiven Unterstützung der Gefahrenabwehr und Strafverfolgung. ›Predictive policing‹ kann als Beispiel für den Bereich der Gefahrenabwehr gelten. Für beide Bereiche stehen beispielhaft der Verbund von Vorgangsbearbeitungssystemen der Vollzugspolizeien auf Länderebene (z.B. für Berlin POLIKS, für Sachsen IVO), auf Bundesebene das System INPOL und auf EU-Ebene die Verbunddateien VIS und SIS II. Diese ITK-Systeme sind über Schnittstellen miteinander verbunden und tauschen (überwiegend) personenbezogene Daten in Bezug auf laufende Ermittlungsverfahren oder zu Gefährdungslagen aus. Aufgrund dieser Daten werden hoheitliche Maßnahmen von Ermittlungsbehörden gerechtfertigt und ergriffen, die in Grundrechte eingreifen können.

Wie das False-Positive-Beispiel aus Anlass des G-20-Gipfels 2017 in Hamburg zeigt, ist die Kenntnis des Zustandekommens und die Möglichkeit der Überprüfung des Wahrheitsgehalts und der Validität der aus BKA-Datenbanken stammenden Informationen zu einer möglichen Gefährlichkeit von Personen (die in diesem Fall unberechtigterweise zum Entzug der Akkreditierung von Journalisten geführt hat) Voraussetzung dafür, die Grundlage dieser ungerechtfertigten Eingriffe erfolgreich anzugreifen. Ähnliche Fälle sind auch mit Blick auf das Schengen-Informationssystem bekannt.

Eine weitere und wesentliche Verbindung dieser Datenbanksysteme mit der Beweiserhebung in konkreten Strafverfahren ergibt sich aus der Tatsache, dass Informationen aus Ermittlungsverfahren in diese Systeme eingespeist werden. Mit anderen Worten: Sie sind – in unterschiedlichem Maße – Teil des Systems elektronischer Datenverarbeitung, das Informationen produziert, die als elektronische Beweismittel in Beweismittelordnern ›auftauchen‹. Informationen aus diesen Datenbanken werden routinemäßig in polizeiliche Fallbearbeitungssystemen übernommen und auch über Schnittstellen in staatsanwaltschaftliche und auch gerichtliche elektronische Akten übermittelt.

Grafik 4: Herstellung von Big Data eEvidence



Grafik 4 stellt in einfacher Form die Erzeugung, die Verarbeitung und das Recycling von Daten in den digitalen Datensystemen auf den verschiedenen Ebenen des EU-Multi-Level-Governance-Systems im Bereich innerer Sicherheit und Strafjustiz dar.

Im Zusammenhang mit der Wahrnehmung von sicherheitsrelevanten ›Vorgängen‹ werden digitale Daten aus verfügbaren Quellen (Wolke) erfasst und in sogenannte Vorgangsbearbeitungssysteme eingegeben. Das Integrierte Vorgangsbearbeitungssystems (IVO) wurde in Sachsen für die Landespolizei entwickelt. Über die Schnittstelle des Elektronischen Fallbearbeitungs- und Analysesystems (eFAS), einer Variante des Fallbearbeitungssystems RSCase und PASS, das Polizeiliche Auskunftssystem, können Daten nach bestimmten Kriterien von Befugten in die Bundesdatenbank INPOL eingespeist werden. INPOL wiederum besitzt eine Schnittstelle mit dem Schengener Informationssystem SIS II. SIS ist Teil eines interoperablen Verbundes von sieben weiteren EU-weiten polizeilichen Datenbanken, die zukünftig über das ESP (European Search Portal) von einzelnen Polizei- und Grenzbeamten über eine einheitliche Nutzeroberfläche abgefragt

werden können.[44] Sollte sich hier bei der Überprüfung ein Treffer ergeben, kann daraus wiederum ein neuer Vorgang entstehen, der dann weitere Ermittlungen in Gang setzten könnte, welche sich wiederum auf Informationen stützen, die mit Hilfe der beschriebenen Datensystemen erzeugt wurden und für den Fall der Einleitung eines Strafverfahrens als digitale Beweismittel eingeführt werden. Diese gesamte hier beschriebene Linie (obere Ebene) basiert wesentlich auf Entscheidungen der Polizei.

Die untere Ebene der Grafik 4 beschreibt den grundsätzlichen Weg, den digitale Daten nach ihrer Erfassung nehmen, wenn hinreichender Tatverdacht festgestellt wird und die Fallakte inklusive der digitalen Beweismittel an die Staatsanwaltschaft weitergegeben wird, die dann Eingang in die Beweisaufnahme in der Hauptverhandlung finden können.

Bei grenzüberschreitender Kriminalität und vor dem Hintergrund der Europäischen Ermittlungsanordnung und den eEvidence-Verordnungen stellen die in Grafik 3 dargestellten digitalen Informationssysteme eine zunehmend interoperable Einheit des Austausches von Daten dar, die potenziell als digitale Beweismittel im Strafverfahren in Erscheinung treten können.

Wenngleich die verschiedenen Datensysteme (Erfassung, Weiterleitung, Abfrage, Auswertung, Mehrfach- und Weiterverwendung) in der Perspektive der Gefahrenabwehr (obere Ebene) und der Strafverfolgung (untere Ebene) hinsichtlich zuständiger Behörden und Jurisdiktionen klar der EU-, Mitgliedstaats- und regionalen Ebene (für Deutschland die Bundesländer) zugeordnet werden können, bildet sich hier in technischer Hinsicht ein interoperables Gesamtsystem heraus, dessen Standards wesentlich durch die EU-Agentur euLISA erarbeitet und

44 Zur Umsetzung der Interoperabilität wurden im Dezember 2017 zwei Verordnungsvorschläge von der Europäischen Kommission eingebracht: Vorschlages für eine ›Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Grenzen und Visa) und zur Änderung der Entscheidung 2004/512/EG des Rates, der Verordnung (EG) Nr. 767/2008, des Beschlusses 2008/633/JI des Rates, der Verordnung (EU) 2016/399 und der Verordnung (EU) 2017/2226, COM(2017) 793 final‹ (Bundesrat-Drucksache: 45/18) und Vorschlages für eine ›Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration), COM(2017) 794 final‹ (Bundesrat-Drucksache: 46/18)

durchgesetzt werden.[45] euLISA wird zukünftig nicht nur die polizeilich genutzten IT-Großsysteme betreuen und entwickeln, sondern auch das IT-Großsystem für den EU-weiten Austausch der Justiz, eCodex.

Aus der Debatte zu den derzeit im Aufbau befindlichen Gemeinsamen Kompetenz- und Dienstleistungszentren (GKDZ) Nord und Ost ist klar zu entnehmen, dass insbesondere eine Verbindung zwischen elektronischen Daten, die aus Überwachungsmaßnahmen stammen, und der elektronischen Strafakte, die 2020 flächendeckend eingeführt sein soll,[46] angedacht ist.[47] Anhand des GKDZ-Konzepts zu Aufnahme, Sicherung, Aufbereitung und (in gewissem Umfang mögliche) Recherche der über TKÜ-Maßnahmen erfassten elektronischen Daten lässt sich darstellen, welche Standards und Abläufe der elektronischen Datenverarbeitung (zunächst mit Fokus auf die TKÜ) zukünftig Anwendung finden sollen und in welcher Form der Datenaustausch vor dem Hintergrund des interoperablen Gesamtsystems im Bereich öffentlicher Sicherheit und Strafjustiz auch mit Blick auf die Einbeziehung der Strafverteidigung in der Zukunft gestaltet werden kann – z.B. mit Einführung der elektronischen Akte in Strafsachen.

Es liegt also fern von aller Utopie, schon heute davon auszugehen, dass in der Zukunft beweiserhebliche Daten als Extrakt aus den verschiedenen polizeilichen elektronischen Datensystemen in der elektronischen Strafakte nicht nur der Staatsanwaltschaft zur Verfügung stehen, sondern auch für Strafverteidiger und Strafverteidigerrinnen über das beA zur Verfügung gestellt werden und im Netzwerk von eCODEX und EGVP kommuniziert werden.

Da es sich bei diesen Daten zumindest im Bereich der Cyberkriminalität und großer Umfangsverfahren der organisierten grenzüberschreitenden Kriminalität überwiegend nicht nur um digitalisierte Daten aus gescannten Dokumenten handelt, sondern um Daten originär digitalen Ursprungs, die mittels IK-Technologie vom Smartphone über TKÜ-Daten bis zur IP- und geheimen online-Überwachungen erhoben werden, ist hier ein grundlegendes Verstehen der Strukturen und Abläufe, von Grundproblemen digitale Forensik sowie der computergestützten Massendaten-Analyse unverzichtbar, wenn effektiv verteidigt werden soll.

Die Tatsache, dass der Mythos von der Objektivität und Zuverlässigkeit elektronischer Systeme und elektronischer Daten bereits heute widerlegt ist (siehe auch weiter unten), unterstreicht, wie notwendig die Entwicklung der Fähigkeit der Strafverteidigung zu einer eigenständigen und unabhängigen Überprüfung von Objektivität, Plausibilität, Reliabilität und Validität von Daten ist, auf die gerichtsfeste Beweise gestützt werden sollen.

Das Konzept der elektronischen Beweismittel (electronic oder digital evidence – eEvidence) bietet für das Verständnis des Übergangs von der analogen zur digitalen Informationsverarbeitung im Strafverfahren einen effektiven Zugang zu einem systematischen Verständnis der einzelnen Ebenen und Elemente, die aus Verteidigersicht letztlich bei der Beweiserhebung im Strafverfahren eine Rolle spielen können und zu deren Beherrschung neue Kompetenzen entwickelt werden müssen.

3. eEvidence – digitale Informationsverarbeitung im Strafverfahren

Ohne Übertreibung kann man feststellen, dass mit der Digitalisierung im Bereich der Strafjustiz nicht nur ein Paradigmawechsel mit Blick auf die Formen und Methoden der Verarbeitung beweiserheblicher Informationen auf allen Stufen des Strafverfahrens verbunden ist, sondern die Beherrschung oder Nichtbeherrschung dieser Methoden durch Richter, Staatsanwälte und Strafverteidiger darüber entscheiden wird, ob die Grundlagen rechtsstaatlicher Strafjustiz und die Standards des Strafprozessrechts im Bereich der Beweiserhebung zukünftig erhalten bleiben und gefestigt oder aber in einer Weise verändert werden, die die Frage aufwirft, ob es sich bei der Beweiserhebung, Beweiswürdigung

45 Siehe Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Ratsbeschlusses 2007/533/JI sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011, COM (2017) 0352 final

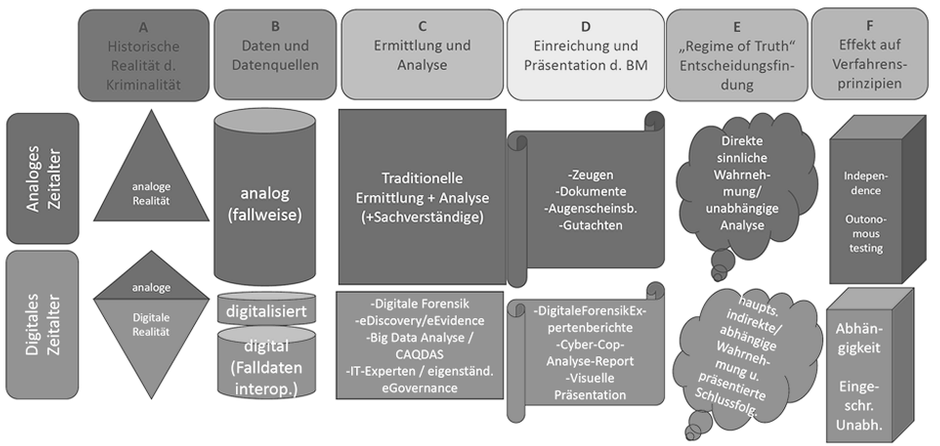
46 Zur Elektronischen Strafakte siehe: Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Einführung der elektronischen Akte in Strafsachen und zur weiteren Förderung des elektronischen Rechtsverkehrs, Drucksache 18/9416, 17.08.2016

47 So das Ergebnis einer Anhörung zum Staatsvertrag zwischen den Ländern Berlin, Brandenburg, Sachsen-Anhalt, Sachsen und Thüringen zur Einrichtung eines GKDZ am 26. Oktober 2017 vor dem Innenausschuss des Sächsischen Landtages.

und letztlich Urteilsfindung um einen eigenständigen und unabhängigen Entscheidungsvorgang geht.

Ermittlungsergebnisse als Resultat der Analyse digitaler Beweismittel werden üblicherweise auf der polizeilichen Ebene im Zusammenwirken von IT-Forensikern (Extraktion der Daten) auf der einen und IT-Ermittlern und Sachbearbeitern (verfahrensbezogene Aufbereitung und Analyse) auf der anderen Seite ›hergestellt‹.[48] Das führt im Vergleich zu ›analogen Zeiten‹ zu neuen Methoden und Organisationsformen innerhalb der polizeilichen Ermittlungsarbeit, die auch für die am Strafverfahren beteiligten Juristen und die Informationsverarbeitung im Strafverfahren auch und gerade unter dem Aspekt der Kontrolle möglicher Fehlerquellen und der Einschätzung des Beweiswertes von eEvidence von entscheidender Bedeutung sein können.

Grafik 5: Digitalisierung und Wandel der Informationsverarbeitung in Strafjustiz



Im *analogen Zeitalter* waren strafbare Handlungen (A), die Daten und Datenquellen, aus denen ihre Existenz geschlossen wurde (B) ebenso analog wie auch die Methoden polizeilicher Ermittlung (C), die sich auf einen oder überschaubare Fallkomplexe beziehen, wie

48 *Büchele*, Ch., Veränderte Kriminalitätsformen erfordern veränderte Organisationsformen. In: der kriminalist, 7-8/2018, 18-22, S. 21

auch die Präsentation entsprechender Beweismittel (D) analog waren. Die an der ›Wahrheitsfindung‹ beteiligten Juristen konnten Beweise direkt-sinnlich wahrnehmen und einer eigenen Analyse unterziehen. Mit Rückgriff auf *Michel Foucault* und seinen Ansatz vom »Wahrheitsregime« kann die Beweisaufnahme in öffentlicher Verhandlung als ein Diskursraum von Akteuren verstanden werden (E), welche die ›prozessuale Wahrheit‹ diskursiv nach bestimmten Prozessregeln konstruieren.[49] Die für Gericht, Staatsanwaltschaft und Strafverteidigung gleichermaßen gegebene Möglichkeit der direkt-sinnliche Wahrnehmung der analogen Beweismittel bildet die Basis für ihre im rechtsstaatlichen Verfahren notwendige Eigenständigkeit und Unabhängigkeit (F).

Diese Voraussetzungen juristischer Entscheidung bei der ›Wahrheitsfindung‹ ändern sich im *digitalen Zeitalter* erheblich. Zum einen findet Kriminalität nicht mehr allein analog, sondern im oder mit Hilfe des Digitalen statt (›digitaler Fussabdruck‹) (A), so dass Daten und Datenquellen zur Rekonstruktion der Tathandlungen (B) wie die Ermittlungsmethoden und –techniken analog und (zunehmend) digital sind (C). Beweiserhebliche Daten sind dabei durch Verbundsysteme für die Ermittler nicht auf einen oder wenige Fälle begrenzt, sondern können sich auf den gesamten digitalen Datenbestand (siehe Grafik 3) beziehen. Aus diesen Möglichkeiten ergeben sich völlig neue Analyse- und Ermittlungsansätze (eDiscovery, Computer Aided Qualitative Data Analysis Software), die eine bis dahin unbekannte Expertengruppe digitaler Forensiker und Datenanalysten (Cybercops) mit einer relativ eigenständigen eGovernance-Struktur im Hintergrund (GKDZ, eJustice) entstehen lässt, deren Kompetenz und Service benötigt wird, um die Einreichung und Präsentation von eEvidence (D) im Beweisverfahren überhaupt zu ermöglichen. Das hat für die juristische Analyse und Bewertung der Beweismittel und die darauf basierende Entscheidungsfindung weitreichende Folgen: Durch die fehlende Möglichkeit, digitale Beweismittel direkt-sinnlich wahrzunehmen, sind die am juristischen Diskurs Beteiligten auf die Vermittlung durch Experten angewiesen (E). Eigenständigkeit und

49 *Foucault*, M., & *Hemminger*, A., Die Regierung der Lebenden Vorlesungen am Collège de France 1979-1980. Berlin: Suhrkamp, 2014

Unabhängigkeit bei der Auswertung und Bewertung digitaler Beweise sind mindestens eingeschränkt (F).

Dieser am Ende die Unabhängigkeit und Eigenständigkeit der am strafrechtlichen Entscheidungsprozess beteiligten Juristen bedrohenden Kompetenzverschiebung, insbesondere auch die Grundsätze des fairen Verfahrens und der Waffengleichheit (be)treffend, kann aus Sicht der Strafjustiz nur auf zwei Wegen begegnet werden:

- zum einen dadurch, dass sich Richter, Staatsanwälte und Strafverteidiger das notwendige Wissen zur digitalen Verarbeitung von eEvidence insoweit erarbeiten, dass sie die Informationsverarbeitung auf Seiten der IT-Experten hinsichtlich der Zuverlässigkeit ihrer Methoden erfassen können und damit weiterhin eigenständig in der Lage sind, die Validität von Informationen zum Beweis von Anklagevorwürfen substanziell einzuschätzen;
- zum anderen (und das dürfte insbesondere für die Strafverteidiger zutreffen), indem die digitale Informationsverarbeitung nicht vollständig den Ermittlungsbehörden, IT-Experten im Bereich von eGovernance und eJustiz oder dem LegalTech-Bereich überlassen wird, sondern eigene Möglichkeiten zur digitalen Informationsverarbeitung massenhafter digitaler und digitalisierter Beweismittel entwickelt werden. Diese können zum einen darin bestehen, eigene Kompetenzen bei der Auswertung digitaler Beweismittel (d.h. Anwendung entsprechender Hard- und Software) zu entwickeln oder den Weg des Outsourcings zu gehen und externe Experten zu beauftragen oder Kompetenzzentren zu bilden.

Kurz: Die Juristen im Strafverfahren werden zukünftig nicht umhin kommen, sich die neue, ›digitale Art und Weise von Lesen und Schreiben‹ anzueignen, wollen sie nicht in unvertretbare Abhängigkeiten geraten und ihre Unabhängigkeit in der juristischen Entscheidungsfindung durch Abgabe entsprechender Kompetenzen und Funktionen der Verarbeitung von Beweisinformationen an IT-Experten verlieren.

Das *Konzept des ›elektronischen Beweismittels‹* (eEvidence) gibt hinreichende Orientierung, auf welchen Ebenen Kompetenzen für die digitale Informationsverarbeitung im Strafverfahren zu betrachten

sind. Die Debatte zu Standards des Umgangs mit elektronischen Beweismitteln befindet sich in Deutschland sowohl, was den akademischen Diskurs anlangt, als auch die legislative und juristische Praxis betrifft, in den Anfängen, wie allein ein Literaturvergleich zu diesem Thema mit dem englischsprachigen Raum zeigt.[50]

Vor dem Hintergrund der seit mehr als zehn Jahren im angloamerikanischen Raum andauernden Debatte zu eDiscovery und eEvidence, wie sie in besonderer Weise in den SEDONA-Regeln bzw. in der Arbeit der ›Scientific Working Group on Digital Evidence‹ reflektiert wird,[51] hat die EU für ihre Mitgliedstaaten auch hier eine Vorreiterrolle mit dem zunächst 2016 abgeschlossenen Projekt ›EVIDENCE – European Informatics Data Exchange Framework for Courts and Evidence‹ eingenommen.[52]

Aus den mit dem *EU-EVIDENCE-Projekt* bearbeiteten Inhalten lassen sich acht Themenkomplexe ableiten. Die in den Themenkomplexen abgebildeten Inhalte sind dabei nicht trennscharf voneinander abgegrenzt, sondern weisen wesentliche Überschneidungen auf. Es sei auch angemerkt, dass die gebildeten Schwerpunkte nicht primär im Ergebnis theoretisch-konzeptionellen oder juristischen Nachdenkens über ›Wesen und Erscheinung‹ digitaler Beweismittel entstanden sind, sondern induktiv aus den in der Arbeit der verschiedenen Teil-Projektgruppen entstandenen Inhalte ›erzeugt‹ worden sind.[53] Für die weitere Arbeit an dieser Systematik wird es selbstredend erforderlich sein, den Nachholbedarf an konzeptioneller Arbeit

50 Vgl. *Momsen*, C., Digitale Beweismittel aus der Sicht der Strafverteidigung, in: S. Beck, B.-D. Meier, C. Momsen (Hrsg.), Neue Herausforderungen der Digitalisierung für Strafrecht, Strafprozessrecht und Kriminologie, Baden-Baden 2015; *Heinson*, D., IT-Forensik: Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen, Tübingen 2015; *Sammons*, J., The Basics of Digital Forensics. The Primer for Getting Started in Digital Forensics, 2nd Edition, Amsterdam 2015; *Mason*, St., *Seng*, D., Electronic Evidence, 4th Edition, London 2017; *Sommer*, P., Digital Evidence Handbook, Virtual City Associates, London 2017; *Nelson*, S. D., *Olson*, B. A., *Simek*, J. W., The Electronic Evidence and Discovery Handbook. Forms, Checklists, and Guidelines. American Law Association, Library of Congress Cataloging-in-Publication Data, 2006, S. 32; *Furneaux*, N., Investigating cryptocurrencies: Understanding, extracting, and analyzing blockchain evidence. Indianapolis: John Wiley & Sons 2018.

51 Siehe: https://www.swgde.org/faq/view, zuletzt besucht: 26. Juni 2018.

52 Siehe: http://www.evidenceproject.eu, zuletzt besucht: 26. Juni 2018.

53 siehe »Media Kit« des EU-EVIDENCE-Projekts

zu befriedigen. Für einen ersten pragmatischen aber in jedem Fall praxisorientierten Zugriff leistet diese Kategorisierung insbesondere wegen ihrer Unterstützung in den jeweiligen Teilprojekten des EU-EVIDENCE-Projekts gute Dienste.

Thematische Komplexe des EU-EVIDENCE-Projekts

Erstens: *Kriminalitätsformen*, die in ihrer Begehungsweise oder/und durch die Besonderheiten ihrer polizeilichen Ermittlung signifikant mit elektronischen Beweismitteln verbunden sind.

Zweitens: *Zuordnung der digitalen Beweismittel (eBM) nach ihren Quellen* als digitale und nicht-digitale Quellen. Diese Unterscheidung ist für die Einschätzung der Verwahrkette (Chain of Custody) und der konkret anzuwendenden Standards bei der kritischen Überprüfung der Authentizität und Integrität elektronischer Beweismittel von Bedeutung.

Drittens: *Art der Erzeugung digitaler Beweismittel*, hier geht es insbesondere um den ›Urheber‹ der Produktion digitaler Daten – Mensch oder Maschine –, die als Beweismittel infrage kommen. Auch hier gelten dann entsprechend unterschiedliche Kriterien und Standards, die es zu überprüfen gilt.

Viertens: *Verarbeitung von eBM,* umfasst die informationstechnischen sowie digital forensischen Bereiche. Diese reichen von der Erzeugung elektronischer Daten bis hin zur Archivierung und sind notwendigerweise selbst an die Nutzung von neuen Technologien und Methoden gebunden. Ihr Verstehen und Erlernen und ihre (in unterschiedlichem Maße zu entwickelnde) Beherrschung stellt einen, wenn nicht *den* wesentlichen Teil der Kompetenzverschiebung bei der Informationsverarbeitung im Rahmen der Strafverteidigung dar.

Fünftens: *Prozessuale Voraussetzungen*, deren Erfüllung zu prüfen ist, um am Ende den Beweiswert digitaler Daten einschätzen zu können, bzw. die so genannte ›Forensic Readiness‹ kritisch zu hinterfragen. Dieser Bereich ist eng mit der Beherrschung des unter Viertens beschriebenen Gegenstandes verbunden.

Sechstens: *Digitale Forensik*, wie im Vergleich der Ausdifferenzierung der acht Themenkomplexe in der Mindmap zu sehen ist, vermittelt sich das Thema der digitalen Forensik in einer sehr verzweigten Teilstruktur. Dies bedeutet nicht zwangsläufig, dass alle anderen Bereiche weniger komplex oder weniger differenziert sind, sondern weist vor dem Hintergrund der induktiven Erzeugung der Mindmap zunächst nur darauf hin, dass jedenfalls das EU-Projekt in diesem Bereich eindeutig einen herausragenden Schwerpunkt bestimmt hat. Es wird sich in der Zukunft zeigen müssen, wo die sinnvolle Grenze für die Ausweitung der Strafverteidigerkompetenzen liegt. Es ist nicht zu erwarten, dass angesichts der in Rede stehenden hochkomplexen technischen Prozesse, die bis in die Grundlagen der Informationstechnologie hineingehen, eine substanzielle eigene digitale forensische Kompetenz der Verteidiger entwickelt werden muss. Gleichwohl muss und wird es möglich sein, die Qualität digitaler Forensik als Strafjurist selbst oder mithilfe von Experten soweit zu verstehen, dass eine juristische Argumentation zur Zulässigkeit und zum Beweiswert digitaler Daten möglich ist.

Siebtens: *Normen und Regeln*, welche den Umgang mit elektronischen Beweismitteln unter dem Aspekt der Datensicherheit und des Datenschutzes bestimmen. Hier spielen gesetzliche Regelungen auf EU-, Bundes- und Landesebene sowie technische Standards eine Rolle.

Achtens: *Akteure und Interessenvertreter*, die an der Verarbeitung digitaler Daten im Bereich von Sicherheit und Justiz beteiligt sind. Eine Übersicht zum Netzwerk von professionellen und nicht professionellen Akteuren, die bei der Erzeugung bzw. Verarbeitung digitaler Beweismittel eine Rolle spielen, erleichtert das Verständnis der von ihnen angewandten Technologien und Methoden. Gegebenenfalls lassen sich in diesen Netzwerken auch Experten oder Sachverständige finden, die bei fehlender eigener Sachkompetenz zu Rate gezogen werden können.

Begriffliches: »Elektronische« oder »digitale« Beweismittel?

Die grundlegende begriffliche Unterscheidung elektronischer Beweismittel bezieht sich auf die Frage, ob die in elektronischer Form vorliegende Information digital erzeugt worden ist oder durch Digitalisierung von einem analogen in einen elektronischen Zustand versetzt worden ist. In dieser Sichtweise wäre der Begriff »elektronisches

Beweismittel« der Überbegriff für die beiden grundlegenden Arten »digitales Beweismittel« und »digitalisiertes Beweismittel«.

Diese Unterscheidung besitzt nicht nur formalen oder semantischen Charakter, sondern ihr kommt für die Aufbereitung und insbesondere Analyse der Daten als potenzielle Beweismittel in einem Strafverfahren nicht unerhebliche Bedeutung zu. Geht man von einem ganzheitlichen analytischen Ansatz aus, sollten alle verfügbaren elektronischen Daten, also digitalisierte analoge wie auch digitale Daten, für die Analyse in einem ganzheitlichen analytischen Projekt (Datenbank) gespeichert und gepflegt werden. Erst damit werden Dokumentendaten gemeinsam mit Daten, die originär digitaler Natur sind und zum Beispiel aus einer TKÜ-Maßnahmen stammen, auswertbar. Die Zusammenführung dieser beiden grundlegenden Arten elektronischer Beweismittel in einem analytischen Projekt ist nicht nur möglich, sondern anzustreben, stellt aber den digitalen Strafverteidiger vor gewisse Herausforderungen bei der Anlage und Einrichtung des Ausgangsprojektes.

Daten, Information, Wissen

In der Datenanalyse werden verschiedene Verarbeitungsstufen durchlaufen, die den Charakter der Ausgangsdaten (oder Rohdaten) verändern. Diese stufenweisen Veränderungen werden im allgemeinen mit den Begriffen »Daten«, »Information« und »Wissen« reflektiert.

Am Beispiel der Verarbeitung von Daten, die über TKÜ-Maßnahmen erfasst worden sind, lässt sich dieser stufenweise Prozess nachvollziehbar darstellen. Zunächst werden die im Prozess der unmittelbaren Kommunikation erzeugten Rohdaten vom Provider erfasst und auf der Grundlage der gerichtlichen Anordnung an zentrale Auswertungsstellen des LKA oder (zukünftig auch) an das Gemeinsame Kommunikations- und Dienstleistungs-Zentrum (GKDZ) weitergeleitet. Das auf dieser Stufe vorhandene Rohdatenformat ist selten für eine direkte Analyse brauchbar und muss entsprechend qualifiziert werden (Datenreinigung, Datenaufbereitung, Transformation in ein analysefähiges Format). Aus den Daten der ersten Stufe werden analysefähige Informationen (häufig strukturierte Daten).

Im Zuge der mit diesen digitalen Informationen durchgeführten in der Regel auf die Prüfung von analytischen Fragen oder Hypothesen gerichteten Auswertung/Analyse werden Befunde erzeugt (A hat zu einer bestimmten Zeit mit B bestimmte Inhalte kommuniziert; A und B gehören zu einem Kommunikationsnetzwerk von X Personen, die mit der vorgeworfenen Tat in Verbindung stehen). Dieses Wissen, soweit es als zuverlässig hergestellt und valide eingeschätzt wird, bildet die Grundlage für die juristische Subsumtion des Sachverhalts.

Die Unterscheidung dieser Stufen auch in Verbindung mit dem korrekten Gebrauch dieser Begrifflichkeit kann helfen, Standards und Kriterien, die auf jeder dieser Stufen unterschiedlich sein können, entsprechend zuzuordnen, und bei Fragen an Ermittler oder Sachverständige diese verschiedenen Ebenen sachlich auseinanderzuhalten.

Besonderheiten digitaler Beweismittel

Grundsatz: Die Präsentation digitaler Beweismittel bedeutet per se, dass ein Umwandlungsprozess (der immer auch Selektion und Interpretation beinhaltet) der Daten stattgefunden hat.

Einzelaspekte:

- Durch Auflösung der festen Bindung von Daten und Trägermedium werden tendenziell zeitliche und räumliche Beschränkungen der Übertragung aufgehoben mit der Kehrseite, dass komplexe Vorgänge und Zwischenstufen der Verarbeitung zwischen den originär erzeugten digitalen Daten/Informationen und den beim Nutzer eintreffenden oder präsentierten Daten/Informationen notwendig sind, die in der Regel zu (technischen) Veränderungen an den ursprünglichen Daten führen.
- Im Vergleich zu analogen Daten ist die Vielfalt der Datenarten und das Vorhandensein (mehr oder weniger umfangreicher) Metadaten bei elektronischen und besonders digitalen Daten erheblich ausgeprägter.
- Diese Vielgestaltigkeit der Wandlung bei der Transformation und Übertragung digitaler Daten in sinnlich wahrnehmbare Informationen, der Beteiligung diverser Hard- und Software, häufig unter Mitwirkung einer Vielzahl von Personen, erzeugt notwendigerweise das Risiko und die Wahrscheinlichkeit bewusster

oder unbewusster Manipulationen.

- Im Bereich der bewussten Manipulation digitaler Daten hat sich ein ganzer ›Geschäftszweig‹ herausgebildet, die sogenannte Anti-Forensik, die zudem in Teilen relativ einfach erlernt werden kann (Beispiel Fake-E-Mails).
- So lange zuverlässige elektronische Sicherungsverfahren (siehe LegalTech, Blockchain, Hashwert...) nicht zum Standard in der Praxis der Verarbeitung digitaler Beweismittel geworden sind, ist die Nachvollziehbarkeit von Transformationsschritten oder die Reproduzierbarkeit von Umwandlungsschritten nicht gegeben und es ist schwer oder unmöglich, die Validität digitaler Daten und damit den Beweiswert sicher einzuschätzen.
- Die Nachvollziehbarkeit der Transformationsschritte elektronischer Beweismittel ist besonders hinsichtlich der Bestimmung von Zeitangaben, Orten, Urhebern (z.B. IPs, Fake-IPs...) von Bedeutung (Authentizität, Integrität der eBM).
- Die Erstellung einer zuverlässigen Verwahrkette (Chain of Custody) ist bei elektronischen Daten ein wesentlich komplexerer und ebenfalls an die Anwendung von IKT/forensische Informatik gebundener Vorgang; oftmals wird die Dokumentation der Verwahrkette und die Nachvollziehbarkeit der Selektion und Herstellung beweisrelevanter digitaler Daten nicht ausreichend dargestellt. Aus diesem Umstand können sich substanzielle Angriffspunkte für Verteidigung ergeben.
- Auch analoge Daten können einen erheblichen Umfang erreichen, das Datenvolumen elektronischer Daten übertrifft diese Umfänge jedoch bei Weitem; computergestützten Verfahren des Datamining und der repräsentativen Datenselektion kommt eine zunehmende Bedeutung zu (siehe LegalTech und Künstliche Intelligenz).
- Umgang mit digitalen Beweismitteln ist unter Ermittlungspersonen aber auch bei Staatsanwaltschaften und Gerichten immer noch ›Neuland‹, der Kenntnis- und Ausbildungsstand ist selbst bei Ermittlungspersonen oft nur ansatzweise gegeben, was zu spekulativen Erklärungen und Fehleinschätzungen führen kann.
- Die rasante technologische Entwicklung erhöht tendenziell die Unsicherheiten im Umgang mit digitalen Beweismitteln und zwingt zudem zu ständiger Fortbildung, die häufig nicht zeitnah absolviert werden kann.

Mythen zu digitalen Beweismitteln, besonders zu deren Objektivität und Zuverlässigkeit

Die ›Scientific Working Group on Digital Evidence‹ (SWGDE) hat eine Liste von »Mythen« im Zusammenhang mit der Herstellung digitaler Beweise zusammengestellt.[54]

Vermutlich befördert durch die relative Neuheit digitaler Beweismittel, wird der Vortrag von digitalen Forensikern oder Datenanalysten der Polizei oder forensischen Labors insbesondere, wenn umfangreiche Visualisierungen präsentiert werden, mit einem festen Glauben an deren Objektivität wahrgenommen (durch Studien belegt). Richtiger wäre es, der Vorstellung digitaler Beweise mit äußerst kritischer Aufmerksamkeit zu folgen und die verschiedenen Verarbeitungsschritte in Bezug auf die angewandten Techniken und Methoden akribisch zu hinterfragen und z.B. Protokolle zu den Auswertungsaktivitäten zu prüfen oder Ergebnisse und Schlussfolgerungen zur Standortbestimmung aus Funkzellenabfragen im Detail zu hinterfragen.[55]

Übersichten, Checklisten und Arbeitsorganisation im Umgang mit Massen-eBM auf Seiten der Strafverteidigung

Im Verfahren mit Massen-eBM macht es Sinn – richtiger: ist es zwingend erforderlich – in entsprechenden Strafverfahren von Anfang an eine Art Logbuch zu den eBM und deren Verarbeitung auf den verschiedenen Verfahrensstufen durch diverse Beteiligte zu führen, das verschiedene Elemente enthalten sollte. Ein solcher Ansatz ist eigentlich in der Sache nichts völlig Neues; normalerweise folgen in Umfangsverfahren erstellte Listen zur Vernehmung von Zeugen

54 Siehe: https://www.swgde.org/faq/view, zuletzt besucht: 26. Juni 2018

55 *Coutts*, R. P., & *Selby*, H., Problems with cell phone evidence tendered to 'prove' the location of a person at a point in time. Digital Evidence and Electronic Signature Law Review, 13(0), 2016 doi:10.14296/deeslr.v13i0.2298, 2016

und Beschuldigten, verbunden mit Zusammenfassungen zu den wesentlichen Aussagen und gegebenenfalls enthaltenen Widersprüchen nebst einer Einschätzung von Glaubwürdigkeit und Glaubhaftigkeit dem gleichen Grundgedanken. Für digitale Massendaten stellt sich eine solche Übersicht, wie sie aus der Natur dieser Daten sowie der Komplexität des Verarbeitungsprozesses folgt, etwas vielschichtiger dar. Im Folgenden sollen einige wesentliche Ebenen dargestellt werden.[56]

10-Punkte Checkliste zur Datenerfassung und zum Prozess der Datenverarbeitung

Eine von Anfang an geführte Protokollierung bzw. Übersicht zur Datenerfassung und dem Prozess der Datenverarbeitung ist besonders wichtig, weil nur dann relativ zeitig erkannt werden kann, auf welchen Umfang und auf welche Einzelfragen und -probleme sich die Verteidigung im Verfahren einstellen muss und – als eine wesentliche Schlussfolgerung aus einer solchen Einschätzung – welche Ressourcen benötigt werden, um einen adäquaten und effektiven Umgang mit den elektronischen Beweismitteln auf Verteidigerseite zu planen und umzusetzen. Mit anderen Worten: Die Verarbeitung von eBM sollte als komplexer, langfristiger und systematischer Vorgang betrieben werden, der nicht irgendwann zu einem späteren Zeitpunkt ad hoc und eklektisch nachgeholt werden kann.

Eine *grundlegende Orientierung sowie den Rahmen für eine Checkliste* können folgende zehn Fragen bieten (inhaltliche Überschneidungen sind gewollt):

(1) Welche Arten von elektronisch verfügbaren Daten (digitalisierte und digitale Daten) liegen im Ergebnis der polizeilichen Ermittlungen vor? (fließender Prozess bis zum Abschluss der Beweisaufnahme)

a. Orientierung am Modell der elektronischen Beweismitteln – siehe acht Themen (S. 296f.);

b. Grundlegende Übersicht zum Inhalt der Daten - Umfang der jeweiligen Datenarten, Abdeckung von Zeiträumen (TKÜ, Handydaten...), Relevanz der jeweiligen Daten mit Blick auf Personen und Ereignisse, die in der Anklageschrift genannt sind, welche Datenarten gibt es, Verzeichnisse - Telefon, E-Mail-Accounts, Kalender, Daten aus sozialen Netzwerken, GIS-Daten...).

(2) Gibt es potentiell relevante elektronische Daten, die im Rahmen der polizeilichen Ermittlungen *noch nicht* erfasst wurden, aus der Sicht der Verteidigung jedoch von Bedeutung sein könnten (eigener Recherche, Befragung Mandanten bzw. Zeugen)?

c. Offene Quellen;

d. Mandanten befragen;

e. Zeugen und dritte Personen befragen.

(3) Woher kommen die Daten (ursprüngliche Quellen)?

f. Originäre Erzeugung der elektronischen Daten (Ausgangsdaten);

g. Ersterfassung/Speicherung der originären elektronischen Daten (es kann zum Beispiel bei der Quellen-TKÜ oder bei der heimlichen online-Durchsuchung wichtig sein, die im Rahmen der heimlichen polizeilichen Überwachung erfassten Daten mit den ursprünglich aufgezeichneten originären Daten zu vergleichen).

(4) Wie stellt sich die Verwahrkette (Chain of Custody) dar (wer hat wann welche Daten in Besitz gehabt/verarbeitet, wer hatte Zugriffsrechte)?

h. Wer (Institution, Person) hatte Zugriff auf die Daten, wer hat tatsächlich mit den Daten gearbeitet, insbesondere auch Einbeziehung von Dritten? (Protokolle)

i. Waren die mit der Datenverarbeitung betrauten Sachbearbeiter und Ermittlungspersonen hinreichend qualifiziert, die Standards für eine gerichtsfeste Verwahrkette anzuwenden? (Beweiswert)

56 *Nelson*, S.D., *Olson*, B.A. & *Simek*, J.W., The electronic evidence and discovery handbook: Forms, checklists, and guidelines. Chicago: American Bar Association, 2006; Sedona Conference, The Sedona Principles. Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3rd Edition, Working Group Series, Sedona 2017

(5) Auf welchen Computersystemen (Hardware) sind die Daten entlang der Verwahrkette verarbeitet worden?

j. Art und Bezeichnung der Hardware (Server, Mainframe, Network file systems, Laptops, PCs, Voice mail, Mobiltelefone, GPS-Systeme, Back-up-Systeme und Speichermedien, Cloud-Service...; gegebenenfalls technische Details und Registrierungsnummern (IP, IMEI, IMSI...).

k. Sind allgemeine Probleme bzw. Begrenzungen, die aus der verwendeten Hardware herrühren, bekannt (Zertifizierung, Beweiswert)?

l. Sind Zuverlässigkeitsprobleme aus der Erfahrung der digitalen Forensik grundsätzlicher Art zum Beispiel im Zusammenhang mit anderen Strafverfahren bekannt? (Beweiswert).

(6) Welche Software wurde auf der jeweiligen Stufe der Verwahrkette benutzt?

m. Liste der Software-Tools (Anlage eines eigenen Software-Wiki, Übersicht über das grundsätzliche Funktionieren verschaffen).

n. Sind aus der Anwendung der Software Reliabilitäts- oder Validitätsprobleme bekannt? (Siehe Beispiel Celebrite/UFED Fehler beim Eintrag zu Datumsangaben. - Beweiswert)

o. Waren die Analysten hinreichend qualifiziert, die verwendete Software anzuwenden bzw. die Ergebnisse der Datenverarbeitung hinsichtlich ihrer Zuverlässigkeit und Validität kritisch einzuschätzen?

(7) Wie erfolgte die Datenanalyse?

p. Welches analytische Konzept und welche analytischen Einzelfragen wurden zur Auswertung der Massendaten entwickelt?

q. Wer gehörte zum Team der analytischen Auswertung - durch wen erfolgte die Anleitung, Abstimmung und Rückkopplung der Teilergebnisse?

r. Welche Qualifikation und Erfahrung besitzen die an der analytischen Aufbereitung Beteiligten?

s. Welche Auswertungssoftware/Analyse Software wurde für die Auswertung benutzt – war/ist sie State-of-the-Art?

(8) Welche Protokollierung, Reports/Auswertungen (auch Reports von Untersuchungen im Rahmen der digitalen Forensik), analytischen Aufgabenstellungen oder Aktenvermerke befinden sich in den Verfahrensakten?

t. Liste dieser Quellen mit kurzer Angabe zu Autoren und Inhalt erstellen.

u. Welche analytisch-methodischen Probleme (Validität, Reliabilität, Objektivität, Plausibilität) werden in diesen Berichten bereits benannt bzw. gibt es überhaupt eine methoden-kritische Betrachtung (zumindest in den komplexeren Auswertungsreports)? (Beweiswert)

(9) Wurden State-of-the-Art-Standards der Verarbeitung (einschließlich der Analyse) von elektronischen Massendaten eingehalten und protokolliert (siehe weitere Ausführungen weiter unten)?

v. Gibt es solche ›State of the Art Standards‹ überhaupt?

w. Sedona-Regeln und SWGED, EU Electronic Evidence Project, BSI-Standards.

(10) Gibt es Auffälligkeiten in Bezug auf Datensicherheit und Datenschutz? (Beweiswert, Verwertungsverbot)

x. Eine Einschätzung der Datensicherheit ergibt sich aus dem Ergebnis der Betrachtung von 1 - 9 und zielt auf die Fragen der Integrität und Authentizität von elektronischen Daten/Informationen, die als Beweismittel Verwendung finden

y. Die Frage des Datenschutzes (berührt mögliche Verwertungsverbote) ist fallbezogene anhand des EU-Datenschutzrechts (Datenschutz-Grundverordnung, Datenschutz-Richtlinie), Bundes- und Landesrecht zu entscheiden.

Natürlich kann jede dieser Fragen bzw. Schwerpunkte noch erheblich vertieft werden.

III. Digitale Herausforderung für die Strafverteidigung

1. Beherrschung der Auswertung digitaler Beweismittel – Möglichkeiten und Grenzen

1.1. Eigene Kompetenzen

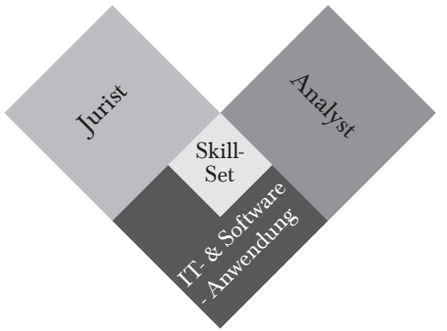
Stephen Mason beschreibt in seinem Artikel ›Towards a Global Law of Electronic Evidence? An Exploratory Essay‹[57] die überwiegend problematische Einstellung von Juristen zu neuer Informationstechnologie und ihre Neigung zu rückwärtsgewandter Betrachtung, die erkennen lässt, dass die große Mehrheit die Tiefe des Wandels noch nicht realisiert und nicht erkannt hat, dass digitale Beweismittel zur bestimmende Form von Beweismitteln werden. Vielmehr gebe es drei Gruppen von Juristen, zum einen die große Mehrheit, die nicht einmal weiß, dass sie nichts über elektronische Beweismittel weiß, zum zweiten eine kleinere Gruppe, die weiß, dass sie nichts weiß und schließlich eine dritte noch kleinere Gruppe einer ›Elite‹, die etwas über digitale Beweismittel weiß, aber realistisch genug ist ebenso zu wissen, dass dieses Wissen noch unzureichend ist. Zwei Jahre später stellt *Mason* in einem weiteren Artikel in unveränderter Perspektive fest: »Artificial Intelligence: Oh Really? And Why Judges and Lawyers are Central to the Way we Live Now—But they Don't Know it«.[58]

Die allgemeine Beobachtung scheint diese Einschätzung *Mason*s auch für Strafverteidiger und Strafverteidigerinnen zu bestätigen. Natürlich werden für die Verteidigung der Mandanten ständig analoge oder digitalisierte Beweismittel ausgewertet. Im Sinne der Methoden empirischer Sozialwissenschaften handelt es sich dabei überwiegend um qualitative Textanalysen, die entweder anhand von Kopien (Papier) oder in elektronischen Textformaten (Word, PDF...) händisch ausgeführt wird. Die Tiefe der Auswertung hängt dabei wesentlich von der Merkfähigkeit der Anwälte ab; größere Datenmengen sind auf diese Weise analytisch nicht zuverlässig zu beherrschen.

57 *Mason*, St., Towards a Global Law of Electronic Evidence? An Exploratory Essay, in: Information Law Journal, Volume 8, Issue 3, 2015, S. 2-19

58 *Mason*, St., Artificial intelligence: Oh really? And why judges and lawyers are central to the way we live now – but they don't know it, in: Computer and Telecommunications Law Review, Volume 23, Issue 8, 2017, S. 213-225

Grafik 6: Notwendiges Skill-Set für die Auswertung elektronischer Beweismittel



Computergestützte Auswertung und Analyse elektronischer Beweismittel erfordert, soll sie effektiv sein, neben der vorausgesetzten juristischen Qualifikation und der notwendigen Computer- und Softwarekenntnis auch ein grundlegendes analytisches Verständnis für die Auswertung digitaler und digitalisierter Daten, mit dem es möglich wird, die Annahmen der Anklagetheorie (bzw. eine Gegentheorie) strukturiert anhand der vorhandenen analogen und elektronischen Beweismittel weitgehend unabhängig von deren Umfang und Format systematisch auszuwerten.

1.2. Analysedesign

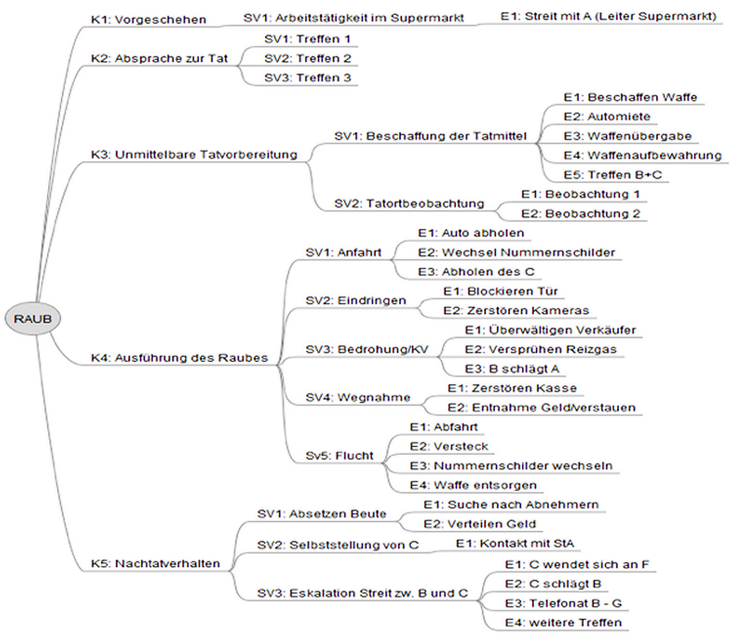
Die Ableitung eines analytischen Designs (Operating Model) aus der Anklagetheorie ist für das Datenmanagement und die Auswertung elektronischer Beweismittel von ganz entscheidender Bedeutung. Mitunter lässt sich – selbst bei der polizeilichen Verarbeitung und Analyse digitaler Beweismittel – beobachten, dass ohne weitere konzeptionelle Vorbereitung vorhandene digitale Daten mit entsprechender Software erfasst werden und dann ad hoc Recherchen (z.B. nach Telefonnummern oder einzelnen Namen) durchgeführt werden. Dieses Herangehen ist als Hauptmethode der Recherche äußerst fragwürdig und muss nahezu zwangsläufig eine zuverlässige Auswertung von Massendaten verhindern, mit anderen Worten, es kann kaum mit Sicherheit festgestellt werden, dass alle beweiserheblichen Informationen aus dem Datenbestand erfasst und ausgewertet wurden. Leider

ist aber diese Methode, in ein Strafverfahren als Beweismittel eingeführte digitale Massendaten wie einen Steinbruch zu behandeln, weit verbreitet.

Zielführender ist hier, zunächst aus der Anklageschrift die analytischen Fragestellungen strukturiert abzuleiten und bis auf die Ebene konkreter Sachverhalte/Ereignisse, die in der Anklagetheorie als Tatvorgang beschrieben werden, zu operationalisieren. Dieser Vorgang kann bereits mittels Analysesoftware durchgeführt werden. Ist Eile geboten, ist auch eine handschriftliche Skizze möglich. In jedem Fall sollte diese Vorüberlegung angestellt werden, da ansonsten auch durch die Anwendung entsprechender Software-Tools keine über simple Suchfunktionen hinausgehenden Effekte erzielt werden können.

Beispiel einer schematischen Erfassung einer Anklagetheorie zu einem Raubvorwurf:

Grafik 7: Prinzip eines Operationalen Modells einer Sachverhaltsbeschreibung



Erklärung der beschreibenden Ebenen: ›Raub‹ <Tatkomplex-gesamt>; ›K‹-Ebene <zusammenhängende Komplexe – oftmals in größeren zeitlichen Zusammenhängen>; ›SV‹-Ebene <Sachverhalte, aus denen sich die Komplexe zusammensetzen>; ›E‹-Ebene <Ereignis- oder Event-Ebene, welche die Sachverhalte konkretisieren>.

Sachverhalt: B und C verabreden, den Supermarkt von A (den C aus früheren Zeiten kennt) zu überfallen und auszurauben...<Details der Tat>. Der beschriebene Sachverhalt wird nun in ›Komplexe‹ (K), ›Sachverhalte‹ (SV) und singuläre Ereignisse (E) aufgegliedert (operationalisiert).

Entscheidend ist zu verstehen, dass die konkreteste Ebene bei der Dekonstruktion des Sachverhalts sich als ›Ereignis‹ oder ›Handlung‹ nicht weiter sinnvoll aufspalten lässt. Nur dann wird das so erzeugte Operationale Modell als Muster für die Kodierung der Daten stabil und zuverlässig sein – und auch bleiben. Damit ist zugleich eine relativ zuverlässige (gleichwohl sich verändernde) Matrix für das Formulieren konkreter analytischer Fragen sowie für die gezielte Recherche nach bestimmten Daten und Informationen bzw. der Analyse von Mustern und Netzwerken oder Geo-Mappings im Gesamtbestand der digitalen Massendaten möglich. Bei Anklageschriften mit komplexeren Sachverhaltsdarstellungen (Anklagetheorie) bietet es sich an, bereits die Dekonstruktion der einzelnen Teile und Elemente des Sachverhalts (üblicherweise entlang einer Zeitleiste spezifische Ereignisse und Aktionen von Angeklagten mit örtlicher Zuordnung) mit einer Analysesoftware durch Kodieren des Textes durchzuführen. Die so entstehende Code-Struktur formt ein Mehrebenen-Modell vergleichbar mit Grafik 6.

1.3. Datenorganisation und Aufbereitung

Die computergestützte Verarbeitung massenhafter digitaler Beweismittel kann sich als ein zeitraubendes Trial-and-Error-Verfahren erweisen, dessen Resultate nicht immer sicher abgeschätzt werden können. Darüber hinaus entstehen zum Teil erhebliche Kosten für Hard- und Software sowie für die notwendige Weiterbildung. Und: Infolge der kurzen Entwicklungszyklen im Bereich der Digitalisierung handelt es sich hierbei nicht um einmalige oder in größeren zeitlichen

Perioden zu investierenden Ressourcen, sondern um einen begleitenden und andauernden Prozess für die Zukunft – dem allerdings auch die Strafverteidigung nicht ausweichen kann.

Big Data eEvidence und Datenmanagement

Ein (wenn nicht das) wesentliche Ziel des Datenmanagements und der Aufbereitung der elektronischen Ausgangsdaten besteht darin, heterogene und weitgehend unstrukturierte Massendaten mit irrelevanter Information in homogene, strukturierte Daten mit überwiegend relevanter Information zu transformieren. Digitale und digitalisierte Daten bilden die Gesamtheit der eEvidence. Für eine effektive Analyse insbesondere in komplexen und längeren Strafverfahren ist es erforderlich, eine strukturierte Übersicht der Projektdaten anzulegen, welche im Zusammenhang mit dem Code- und Variablenplan (siehe unten) zu sehen ist.

Grafik 8: Beispiel für Datenstruktur eines Analyseprojektes

Sind die verschiedenen Arten von Beweismitteldaten einmal erfasst, lässt sich daraus die Ablagestruktur der elektronischen Daten in entsprechend bezeichneten Ordnern ableiten (Basis für spätere Metadaten-Bildung). Die Anlage dieser Struktur ist essentiell für die Analyse selbst, aber auch mit Blick auf die Zitierfähigkeit in der Verhandlung. Wenn PDF-Beweismittelordner entsprechend der Bezeichnung der analogen BM-Ordner angelegt werden, ist die Zitierfähigkeit in der Verhandlung bzw. schnelles Auffinden gewährleistet, wenn in Beweismittel mit Quellenverweis aufgerufen werden.

Außerordentlich hilfreich ist ebenso ein grundlegendes Verständnis des Systems der Datenquellen.

Mit »System der Datenquellen« sind

- zum einen die Art des Datenspeichers (lokale Datenspeicher, cloud- und server-basierte Datenspeicher),
- die zu diesen Datenspeichern gehörenden Kategorien von Daten
  * lokale Datenspeicher: Office-Dateien/Ordner, E-Mail-Container, Smartphone-Data-Exporte, Loadfiles, provider-spezifische Daten, Disk-Images, MS Exchange, EDB Archive,
  * cloud-/server-basierte Datenspeicher: E-Mail-Accounts, Cloudspeicher, Share Point,
- die Dateiformate, die zu den Datenkategorien gehören (Word, Excel..., PST, IBM Notes, UFED- oder XRY-Exporte ... Relativity, CSV, TSV...

gemeint.

Die computergestützte Aufbereitung und Auswertung der digitalen Daten aus diversen Quellen in diversen Formaten – strukturiert und unstrukturiert – kann nur mit der geeigneten Software erfolgen. Über verschiedene Stufen der Datenerfassung, Speicherung, Aufbereitung, Analyse, Präsentation und Archivierung werden unterschiedliche Softwaretools angewendet, um aus großen heterogenen Datenmengen die relevante Information zunächst herauszufiltern, zu strukturieren, dann inhaltlich zu analysieren und zu präsentieren. Dazu ist zu überprüfen, ob die Software mit der geeigneten Funktionalität (zur Auswertung der Daten im Sinne der analytischen Fragestellung) auch in der Lage ist, die vorliegenden Datenformate in dem jeweils gegebenen Umfang zu verarbeiten.

3.1.4 Software-Anwendungen für die Auswertung von eEvidence

Dieser Abschnitt gibt eine erste Übersicht zu verschiedenen, für die Auswertung elektronischer Beweismittel eingesetzten Software-Tools. Dabei erfolgt eine Konzentration auf einige der marktführenden bzw. gebräuchlichsten Software-Pakete im Bereich der Extraktion (steht für Strafverteidigung sicher nicht im Zentrum der Anwendungen), Aufbereitung und Analyse von eEvidence.

(a) Software aus dem forensischen Bereich (Auswahl)

Spezielle Software-Tools, die im engeren Sinne dem forensischen Bereich (eDiscovery, eEvidence) zuzurechnen sind bzw. (wie dtSearch) mit besonderen Funktionen für die forensische Analyse ausgestattet sind, wurden in den letzten Jahren zunehmend zu Standard-Anwendungen der polizeilichen Erfassung und Auswertung elektronischer Daten im Rahmen von Ermittlungsverfahren und werden darüber hinaus von Beratungsfirmen, Anwaltskanzleien und forensischen Laboren, Kompetenzzentren bzw. eEvidence-Experten eingesetzt. Nicht alle dieser Tools sind wegen ihrer Komplexität und des Aufwandes für Installation und Pflege für kleinere Kanzleien oder Einzelanwälte geeignet (z.B. Relativity, Zylab oder Brainspace) – andere hingegen bieten sehr wohl die Möglichkeit der Anwendung auch in IT-kleineren Umgebungen (z.B. dtSearch, Nuix, Intella).

Brainspace stellt sich als ›augmented intelligence platform‹ dar, mit deren Hilfe ein ›erweitertes‹ Verständnis basierend auf maschinellem Lernen und einer interaktiven Visualisierung von Big Data möglich wird. Die Ergebnisse sind in der Tat überzeugend, gleichwohl bezieht sich Brainspace auf Anwendungsfälle mit erheblichem Datenumfang und wird bei einem Einstiegspreis von 98.000 US-Dollar pro Jahr kaum zu einer unter Anwaltskanzleien verbreiteten Standardsoftware werden. Brainspace-Technologie zeigt jedoch in gewisser Weise eine Richtung zukünftiger Massendatenauswertung auch im Bereich der forensischen Analyse digitaler Beweismittel an, die zunehmend durch erweiterte Möglichkeiten künstlicher Intelligenz geprägt sein wird.

Cellebrite ist ein globaler Marktführer im Bereich der mobilen Forensik. Die Software kann Daten der meisten mobilen Geräte auslesen, wiederherstellen und analysieren. Cellebrite bietet weitere Tools für die Auswertung digitaler Daten an. *UFED Analytics* ermöglicht eine differenzierte Datenauswertung. *UFED Reader* erlaubt einfache Analysen und den Export von Smartphonedaten und wird der Verteidigung häufig in Strafverfahren für die Auswertung von Smartphone-Daten zur Verfügung gestellt.

dtSearch erlaubt die gleichzeitige Suche in Terrabytes unterschiedlichster Datenformate und (über die Report-Funktion) deren

Integration in einer Datenbank. Damit ist – zudem preiswert – eine erste Möglichkeit gegeben, als Beweismittel übergebene elektronische Daten (soweit sie nicht verschlüsselt sind) zu recherchieren. dtSearch bietet darüber hinaus spezielle Funktionen z.B. zur Recherche in E-Mails, verschlüsselten PDFs, Kreditkarten-Nummern oder sozialen Netzwerken und Websites. In Kombination mit QDA-Software (siehe B) Software aus dem Bereich der empirischen Sozialforschung) eröffnet dtSearch die Möglichkeit, große Datenmengen für die Zwecke der Verteidigung für die Auswertung verfügbar zu machen.

Intella von Vound verbindet eDiscovery und Computer Forensics und bietet mit einer sehr intuitiven Benutzeroberfläche auch für Juristen einen einfachen Zugang zur Aufbereitung und Analyse von eEvidence. Intella ist designed, die gängigen eEvidence-Dateiformate zu verarbeiten, und bietet eine robuste Funktionalität zur Klassifizierung von unstrukturierten Daten. Z.B. ist die Recherche und Analyse von großen E-Mail-Beständen und das Verfolgen von Informationspfaden mit Intella effektiv.

Magnet Forensics ist eine vergleichsweise neue Software, die insbesondere auf die Auswertung von Android-Smartphonedaten ausgerichtet ist. Sie steht damit in Konkurrenz zu Cellebrite ist jedoch wesentlich preisgünstiger.

Maltego ist ein relativ einfach zu erlernendes Tool für OSINT (Open Source Intelligence) Recherche im Internet. Da auch Polizei und Sicherheitsbehörden einen Großteil ihrer Informationen aus offenen Quellen des Internets (z.B. soziale Netzwerke) beziehen, kann eine Überprüfung oder eigene Background-checks aus Verteidigerperspektive mit Maltego sinnvoll sein.

Nuix wird weltweit – überwiegend von Polizei und Sicherheitsbehörden – im Bereich der forensischen Aufbereitung elektronischer Beweismittel verwendet und gilt als einer der Marktführer. Wegen seiner überschaubaren Lernkurve (eine seriöse praktische Anwendung sollte nach einem Drei-Tage-Kurs möglich sein) und zugleich komplexer Funktionalität bietet es die für die Fallanalyse von digitalen Massendaten notwendige Unterstützung. Nuix kann z.B. Daten von UFED oder XRY importieren, so dass die Recherche in Smartphonedaten problemlos möglich wird.

OpenText bietet verschiedene Software-Tools für die Auswertung von Big Data in Unternehmen oder umfangreichen Strafverfahren an. *EnCase* (Teil von OpenText) unterstützt die forensische Ermittlung von der Datenerfassung über die Aufbereitung bis zur Herstellung von Reports und Präsentationen der Befunde.

Oxygen Forensics Detective kann u.a. Daten von mobilen Geräten und Dronen extrahieren und verarbeiten.

Passware ist eine spezielle Software, die es ermöglicht, versteckte und gelöschte Daten aufzufinden und ggf. zu dekodieren bzw. einen Passwortschutz zu überwinden.

Die vorstehend stichwortartig vorgestellten forensischen Software-Tools[59] stellen lediglich eine Auswahl dar.[60] Zur Anwendung für kleinere und mittlere Anwaltskanzleien könnten dtSearch, Nuix, Intella, Magnet Forensics[61] möglicherweise bei Bedarf auch Maltego und Passware in Betracht gezogen und getestet werden.

(b) Software aus dem Bereich der empirischen Sozialforschung (Auswahl):

Während die unter (a) genannten Software-Pakete speziell auf die Aufarbeitung digitaler Massendaten im Zusammenhang mit Ermittlungsverfahren ausgerichtet sind, handelt es sich bei der unter (b) aufgeführten Software um Anwendungen, die historisch im Bereich der qualitativen empirischen Sozialwissenschaft entwickelt wurden. Computer Aided Qualitative Data Analysis (CAQDAS) wurde im Laufe der letzten 20 Jahre zu einem Standard bei der Auswertung unstrukturierter (meist textlicher) Daten, wobei eine Verbindung von qualitativen und quantitativen Methoden der Auswertung (mixed methods) erreicht wurde. Insbesondere für Netzwerk- und Musteranalysen ist diese Verbindung bedeutsam.

Digitalisierte Inhalte von Beweismittelordnern liegen überwiegend als Textdaten vor. Auch digitale Beweismittel in Form z.B. von

59 Es wird hier darauf verzichtet, zu jeder erwähnten Software entsprechende Links anzugeben. Diese können durch einfache Internet-Recherche gefunden werden.

60 Für weitere Übersichten siehe https://www.capterra.com/electronic-discovery-software/ zuletzt besucht: 24. Juni 2018

61 Aus Sicht des Autors decken Nuix, Intella und Magnet Forensics bei aller Unterschiedlichkeit ähnliche funktionale Bereiche der eEvidence-Analyse ab.

Smartphonedaten können in Textformaten (z.B. durch Export über den UFED- oder XRY-Reader) lesbar gemacht werden. Datamining zu weiteren Datenformaten kann mit dtSearch erfolgen und als Word-Dokument gespeichert werden. Diese Daten sind dann für nachstehende Software auswertbar. Der praktische Vorteil dieser Software besteht neben ihrer starken analytischen Funktionalität auch darin, dass sie in der Regel preiswerter sind. Üblicherweise werden Trial-Versionen angeboten, so dass zunächst die Brauchbarkeit für die eigenen Zwecke getestet werden kann.

Atlas.ti ist eine der am meisten verbreiteten Anwendungen, mit denen Muster Zusammenhänge (z.B. zwischen Angeklagten) erkannt werden können. Atlas.ti ist dabei sehr nutzerfreundlich und intuitiv.

MAXQDA besitzt Stärken in der Datenorganisation und Visualisierung sowie der Mixed-Method-Analyse.

NVivo unterstützt ebenfalls den Mixed-Method-Ansatz und eignet sich auch für größere Datenmengen.

Provalisresearch bietet mit QDA Miner und WordStat zwei Software-Pakete an, welche die Auswertung von Big Data ermöglichen (ebenfalls Mixed-Method-Ansatz).

Die hier kurz dargestellten Software-Tools unterstützen u.a. folgende analytische Funktionen:

- Auswertung von im Rahmen von TKÜ-Maßnahmen erfassten Daten (auch Standortdaten, Geo-Mapping);

- Datamining und Herstellen integrierter, ganzheitlicher Datenbanken aus Handy-Spiegelungen (die Heterogenität der auf Smartphones üblicherweise gespeicherten Daten stellt eine besondere Herausforderung für eine komplexe Datenanalyse dar - gleiches gilt für mittels Online-Durchsuchung oder IP-Überwachung gesammelte Massendaten);

- Möglichkeiten von (zugegebenermaßen qualifizierteren) Auswertungsmöglichkeiten zu Kontextdaten (hier bezieht sich die Analyse nicht nur auf einzelne Begriffe oder Taxonomien, sondern es werden Funktionen von Software benutzt, die auf statistischen Funktionen oder so genanntem ›maschinellem Lernen‹ basieren);

- Aufdeckung von Netzwerken anhand von Verbindungsdaten,

semi-automatisches Herstellen von Timelines (chronologische Erfassung von Ereignissen über (möglichst) die Gesamtheit der vorhandenen elektronischen Daten).

Die Auswahl von Software-Tools richtet sich im Wesentlichen nach den ersichtlichen analytischen Fragestellungen sowie der Art der elektronischen Daten, die als Beweismittel zur Verfügung stehen. Aus den analytischen Fragestellungen ergibt sich zunächst, welche Ergebnisse der Analyse angestrebt werden. Während es in manchen (eher einfachen) Fällen ausreichend sein kann, eine mehr oder weniger komplexe Recherche durchzuführen, ist in anderen (eher komplexeren) Fällen eine Analyse netzwerkartiger Zusammenhänge oder Geo-Mapping gefragt.

Wie im vorangegangenen Abschnitt gezeigt, können digitale Beweismittel aus sehr heterogenen Quellen stammen und in den unterschiedlichsten Formaten vorliegen.

Um eine effektive Analyse durchführen zu können, muss die Auswahl der Software so erfolgen, dass die vorliegenden Datenformate verarbeitet werden können und entsprechende Funktionen vorhanden sind, um die analytischen Fragestellungen zu bearbeiten und darzustellen (visualisieren).

Unabhängig davon, ob eine eigenständige Anwendung der unter (a) und (b) genannten Software erfolgt, eine gewisse Kenntnis der Grundfunktionen dieser Software-Tools und der methodischen Prinzipien ihrer Anwendung ist auch deshalb von Nutzen, da an die Strafverteidigung im Rahmen der Akteneinsicht übergebene Bestände an elektronischen Daten mit diesen (oder ähnlichen) Applikationen erzeugt und ausgewertet werden, mithin das Verständnis der übergebenen Datenstrukturen und Datenformate sowie mögliche Schwachstellen und Fehlerquellen für die eigene Analyse hilfreich ist.

Allgemeine IT-Fitness in der zumindest grundlegenden Beherrschung von Applikationen wie Office-Software, insbesondere Word, Excel, Notepad aber auch von Adobe, OCR-Software wie z.B. ABBYY FineReader, aber auch von einfacher Verschlüsselungssoftware und der Nutzung verschlüsselter Cloud-Dienste sowie von VPN- oder Proxyzugängen zum Internet erleichtert darüber hinaus das Verständnis und die Verarbeitung elektronischer Beweismittel und die

häufig notwendige Teamarbeit und damit den gesicherten Austausch forensischer Daten.

2. Outsourcing

In mancher Hauptverhandlung ist der Mythos der Objektivität von beweisrelevanten Befunden, die auf die Auswertung digitaler Daten gestützt wird, zu beobachten. Z.B. wenn bei der Darstellung der Ortung von Handys durch Berechnung der Abstrahlwinkel von Sendemasten oder beim Jonglieren mit allen möglichen technischen Fachbegriffen aus dem IT-Bereich bzw. der digitalen Forensik am Ende eine wie in Stein gemeißelte Behauptung der Staatsanwaltschaft zum Beweis dieses oder jenen Fakts steht: »eine Kommunikation zwischen A und B hat *nicht* stattgefunden, da sie in den Daten nicht nachzuweisen ist« und diese Behauptung gutgläubig aufgenommen wird und unwidersprochen bleibt. Es besteht die Tendenz zu glauben, was man sieht, und viele der Ergebnisse der Auswertung elektronische Beweismittel (z.B. Netzwerkanalyse) werden notwendigerweise visuell dargestellt. Dieser ›Gläubigkeit‹ kann nur durch Entwicklung eigener ITK-Fitness und methodenkritischer Befragung begegnet werden. Gleichwohl wird es in manchen Fällen unumgänglich sein, externe Sachverständige hinzuzuziehen. Während sich zum Beispiel in den USA in diesem Bereich (Digital Forensic Laboratories) bereits ein ganzer Markt entwickelt hat,[62] sind solche Experten in Deutschland (und in den meisten anderen EU Mitgliedstaaten) noch nicht so häufig zu finden.

Bei Vereinbarungen mit Experten in der digitalen Forensik bzw. computergestützten Kriminalitätsanalyse sollten ein paar Punkte besondere Beachtung finden (im Wesentlichen dem ABA-Handbuch entlehnt):[63]

Grundsätzliches:

- Die Aufbereitung und Analyse elektronischer Massendaten ist ein äußerst komplexer und normalerweise langfristiger und umfangreicher Vorgang, es sei denn, man kann eine Aufgabe

62 *Valli*, A. J., Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility. Butterworth-Heinemann 2009

63 *Nelson*, *Olson* & *Simek*, 2006 (Fn. 56), S. 32

punktuell herauslösen und sehr genau hinsichtlich des Auftragsvolumens abgrenzen.

- Es ist grundsätzlich nur schwer mitunter gar nicht möglich, eine halbwegs zuverlässige Ergebnisschätzung (was wird die Analyse konkret erbringen) vorzunehmen und dabei den zeitlichen Aufwand konkret abzuschätzen; es gibt zu viele Unbekannte und durch die rasante technische Entwicklung verursachte nicht vorherzusehende Überraschungen bei der Datenaufbereitung und Datenanalyse, die eine solche Vorhersage nahezu unmöglich machen.
- Jenseits und vorab des technisch-analytischen Projektes ist eine intensive inhaltliche Beschäftigung mit den möglichen Beweisthemen und der daraus abgeleiteten Fragen zwingend erforderlich um einzuschätzen, ob die digitalen Daten in einem Verfahren mit einer gewissen Wahrscheinlichkeit potentielle Informationen enthalten, die in der Perspektive der Verteidigung einzubringen wären; mit gewisser Regelmäßigkeit könnte das der Fall sein, wenn ein Alibi nachzuweisen ist oder wenn behauptete Kommunikationsverbindungen nach Darstellung der Mandanten nicht zutreffen.

(1) Notwendige Vorüberlegungen zur Art der Expertise

Es sollten vor der ersten Absprache *Vorüberlegungen zu einem Auswertungsdesign* angestellt werden, die einerseits von den wesentlichen Annahmen der Anklagetheorie ausgehen und andererseits das *Potenzial der elektronischen Daten* hinsichtlich einer Überprüfung oder Widerlegung dieser Annahmen vorläufig einschätzen. Nur wenn hier die Wahrscheinlichkeit möglicher Befunde (im Sinne der Verteidigung) anzunehmen ist, macht die Beauftragung von Experten einen Sinn. »Wahrscheinlichkeit« ist dabei eine relative Größe und kann unter Umständen auch bedeuten, dass es nur ›nicht auszuschließen‹ ist, in den elektronischen Daten der Anklagetheorie widersprechende Informationen zu finden. Dies dürfte abstrakt in der Mehrzahl der Fälle zu bejahen sein; die Frage ist, ob gefundene Widersprüche oder Lücken in der polizeilichen Auswertung im Sinne effektiver Verteidigung durchgreifen.

(2) Prüfung der Qualifikation und Expertise (Referenzen)

Vorsicht vor Experten die behaupten, den gesamten Zyklus der Datenverarbeitung abzudecken – besonderes Augenmerk auf Objektivität im methodischen Herangehen legen.

- Analyse ohne ›finale Subsumtion‹ - die Entscheidung über die Verwendung von Analyseergebnissen liegt ohnehin in der Hand der Verteidigung, jedenfalls zunächst, solange der Experte nicht als Sachverständiger vor Gericht geladen wird.
- Die tatsächliche Datenlage (auch wenn sie die eigene Verteidigungsstrategie nicht unterstützen sollte) zu kennen, ist in jedem Fall besser, als ein methodisch voreingenommenes Ergebnis vor Gericht zu präsentieren und im Zweifel damit im Ergebnis einer Gegenanalyse widerlegt zu werden.

(3) Gerichtserfahrungen (Referenzen!)

»You don't need a Greenhorn cutting his teeth on your case.«

(4) Absicherung des Datenschutzes und der Vertraulichkeit

Hierzu sind konkrete Absprachen und ggf. vertraglich Vereinbarungen erforderlich. Einzelheiten ergeben sich aus den Regeln des Datenschutzes.

(5) Inanspruchnahme von Diensten außerhalb Deutschlands bzw. außerhalb der EU

Achtung: Von ganz spezifischen Einzelfragen abgesehen sollte der Experte der deutschen Sprache mächtig sein.

(6) Innovative und explorative Einstellung

Nur in einer offenen Kommunikation zwischen Strafverteidigung und Forensik-Experte bzw. Datenanalyst lässt sich die Auswertung der Daten innovativ und effektiv gestalten. Beide Seiten müssen sich hier in aller Regel sehr kreativ verhalten, selten gibt es bereits feststehende methodische oder analytische Wege für den konkreten Fall, sondern es wird ein methodisches Grundwissen auf einen Fall angewendet. D.h. auch, dass in einem nicht unerheblichem Maße auf dem Wege von Versuch und Irrtum die Lösung eines Problems gesucht werden muss. Wer dieses Risiko vermeiden will, sollte von einer solchen Analyse und auch von der Kooperation mit Experten Abstand nehmen.

(7) Die Geldfrage

Forensik-Experten und Analysten bzw. Data Scientists arbeiten für Stundensätze von beginnend etwa 60 bis 80 Euro. Je nach Komplexität und Umfang sowie Schwierigkeitsgrad der Analyse können aber auch bis zu 220 Euro in Rechnung gestellt werden. Wegen der oben festgestellten Schwierigkeit, den Zeitumfang für die Lösung eines analytischen Problems exakt zu bestimmen, sollte bei der vertraglichen Vereinbarung zwischen Anwalt und Forensiker/Analyst eine Balance zwischen einer auf gewissen Erfahrungswerten bestehenden Schätzung hinsichtlich des zeitlichen Gesamtumfanges und den abrechenbaren Ergebnissen hergestellt werden. Pauschalvergütungen sind zwar nicht unüblich, aber in der Regel auf Seiten des Analysten riskant. Praktisch ratsam sind Prioritätenlisten und ›Sollbruchstellen‹ – gleitende Projektierung, d.h. es werden Schrittfolgen und deren sukzessive Erfüllung/Bezahlung vereinbart. Entlang dieses Weges erkennt man dann auch schnell, ob einerseits die Zusammenarbeit zwischen Anwalt und Forensiker/Analyst funktioniert und das vereinbarte Vorgehen andererseits in dem konkreten Fall zu brauchbaren Ergebnissen (die den finanziellen Aufwand rechtfertigen) führt.

IV. Resümee und Ausblick

Strafverteidigung muss sich auf die aus der Digitalisierung folgenden Herausforderungen insbesondere im Bereich neuer IT-gestützter Überwachungs- und Ermittlungsmethoden mit Blick auf die nächsten zehn bis 15 Jahre einstellen und eigene Kompetenzen im Umgang mit elektronischen Beweismitteln ausbilden.

Die signifikanten Veränderungen im Informationsmanagement der Beweiserhebung im Übergang vom Analogen zum Digitalen führen zu einer Kompetenzverschiebung bezüglich der Unabhängigkeit und Eigenständigkeit in der Entscheidungsfindung der Gerichte, aber auch auf Seiten der Staatsanwaltschaft und der Strafverteidigung mit dem Risiko der Gefährdung von Verfahrensgrundsätzen des rechtsstaatlichen Strafverfahrens. Das Entstehen einer Substruktur der eGovernance/eJustiz (z.B. in Gestalt der Gemeinsamen Kompetenz- und Dienstleistungszentren) monopolisiert Fähigkeiten der Informationsverarbeitung und entscheidet (durchaus gemeinsam mit der IT-Industrie) über Grundsätze der Entwicklung der Digitalisierung der Justiz und des Strafverfahrens.

In einem Strafverfahren sind das Gericht, die Staatsanwaltschaft und die Strafverteidigung an einem diskursiven Prozess der Entscheidung über die Anklagevorwürfe (Anklagetheorie) als die maßgeblichen Akteure beteiligt, als juristische Akteure, die in einem historisch seit der Aufklärung gewachsenen System rechtsstaatlicher Strafrechtsprechung in einem differenzierten gesetzlichen Rahmen Daten und Informationen zu den mit den Anklagevorwürfen verbundenen rechtserheblichen Tatsachen (Tatbestandsmerkmale) verarbeiten und – letztlich in der gerichtlichen Entscheidung – zu einer ›prozessualen Wahrheit‹ gelangen. Diese Entscheidung ist – soweit rechtlich zulässig zustande gekommen – legal und legitim zugleich, da sie aus diesem demokratisch-rechtsstaatlichen Verfahren von dazu autorisieren und dafür qualifizierten Akteuren bei Wahrung deren Unabhängigkeit und Eigenständigkeit hervorgeht.

Im analogen Zeitalter sind Daten als Grundlage der unabhängig-eigenständigen Entscheidungen im Rahmen des Beweisverfahrens für Richter, Staatsanwälte und Strafverteidiger als Personen grundsätzlich gleichermaßen als sinnlich wahrnehmbare Informationen zugänglich und zu verarbeiten – überwiegend durch Aktenstudium, also qualitative Datenanalyse. Soweit Sachverständige im Rahmen der Beweiserhebung eine Rolle spielen, bezieht sich ihr Beitrag gewöhnlich auf einen Teilbereich, und von Experten vertretene Positionen können ggf. durch Gegengutachten kontrastiert werden. Mit dem Übergang zum digitalen Zeitalter verändert sich der Prozess der Informationsverarbeitung dramatisch. Infolge der Digitalisierung nahezu aller lebensweltlichen Zusammenhänge auf der einen und einer digitalen Sicherheitsarchitektur auf der anderen Seite, werden beweiserhebliche Daten zum Nachweis (oder der Widerlegung) von Anklagevorwürfen zunehmend und in massenhafter Form als digitale Beweismittel eingebracht. Nicht nur, dass allein der Umfang dieser Daten im Vergleich zu analogen Zeiten die menschliche Verarbeitungskapazität von Richtern, Staatsanwälten und Strafverteidigern bei weitem übersteigt, digitale oder digitalisierte Daten sind sinnlich nicht unmittelbar zugänglich, sondern bedürfen der Nutzung von Hard- und Software.

Die Tatsache, dass die Fähigkeit der eigenständigen Hard- und Software-Nutzung (oder mindestens das Verständnis derselben) zum Erhalt der unabhängigen und eigenständigen Datenverarbeitung im Beweisverfahren zwingend erforderlich ist, hat weitreichende Folgen. Wird diese Fähigkeit bei den beteiligten Juristen nicht entwickelt, bildet sich im Zuge der Anwendung von Hard- und Software zur Verarbeitung elektronischer Beweismittel eine neue Struktur der eGovernance und der eJustiz heraus, zu denen von Seiten der Richter, Staatsanwälte und Strafverteidiger ein substanzielles Abhängigkeitsverhältnis entsteht, da für die Entscheidungsfindungen im Beweisverfahren erhebliche Informationen nicht mehr sinnlich-unmittelbar (also unabhängig und eigenständig) persönlich erfasst werden, sondern von IT-Experten aufbereitet und zur Verfügung gestellt werden, ohne dass die Methoden des Zustandekommens der Daten und damit ihre Zuverlässigkeit hinreichend nachvollzogen werden kann.

Neben der Ausbildung eigener Kompetenzen bei der Auswertung von eEvidence stellt sich der Auf- und Ausbau von Forensischen Laboren oder Kompetenzzentren, die analytische Fragestellungen der Strafverteidiger und Strafverteidigerinnen unter Beachtung von Datenschutz und Datensicherheit sachgerecht bearbeiten, als eine weitere und möglicherweise zentrale Perspektive für die Schaffung einer tragfähigen Informationsverarbeitung im digitalen Beweisverfahren dar.

Prof. Dr. Ralf Kölbel

Zu den jugendstrafrechtlichen Verwerfungen durch den Ausbau von Verfahrens- und Entschädigungsrechten des Verletzten

I. Einführung

Die Berücksichtigung von »Opferinteressen« ist ein zentraler rechtspolitischer Topos der letzten Jahrzehnte – im (Jugend-)Strafverfahren (unten 2.) ebenso wie im materiellen Recht (unten 3.). Damit folgt der Verlauf in Deutschland einem international zu beobachtenden Kurs.[1] Kriminalsoziologisch wird dies demgemäß auch als übergreifende spätmoderne Entwicklung analysiert. Zu deren Kennzeichen zähle es, die Aufmerksamkeit von den Ursachen der Delinquenz auf deren Folgen (Kosten, Unsicherheitsgefühle usw.) zu verlagern und deshalb auch die Interessen der Tatopfer in den Vordergrund zu rücken.[2] In dieser dezidierten »Opferzuwendung« macht man einen integralen Baustein einer neuen Kontrollkultur aus, die sich vom wohlfahrtsstaatlichen, d.h. resozialisatorisch orientierten Strafrecht entfernt.[3] Möglich ist dies auch deshalb, weil »das Opfer« mit seinen Bedrohungen und Bedürfnissen für die Legitimation der unterschiedlichsten strafrechtlichen Umstellungen fungibilisiert werden kann – denn die diskursive Berufung auf das Opfer stellt durch dessen Identifikationsfähigkeit letztlich eine Berufung auf die individuellen Ängste, Befürchtungen

1 Dazu rechtsvergleichend für das Strafprozessrecht *Weigend*, in: Barton/Kölbel (Hrsg.), Ambivalenzen der Opferzuwendung des Strafrechts, 2012, S. 29*ff.*; speziell für das Jugendstrafverfahren vgl. den internationalen Überblick bei *Kölbel*, in: BMJV (Hrsg.), Berliner Symposium zum Jugendkriminalrecht und seiner Praxis, 2017, 9, S. 22*ff.*

2 *Garland*, Culture of Control, 2001, S. 121*ff.*

3 Es ist nachgerade »a central theme« dieser Debatte, dass »the shift from a welfarist to a retributivist perspective on crime has brought with it a shift in focus away from the defendant/offender's rights and interests to those of the victims of crime« (*Marshall*, Critical Review of International Social and Political Philosophy 7, 2004, S. 104).