Die strafprozessuale Datenbeschlagnahme im Zeitalter der Digitalisierung[1]

Dr. Eren Basar

A. Die Digitalisierung des Beweisrechts

Das Thema „Digitalisierung im Strafverfahrensrecht" erzeugt nicht selten futuristische Vorstellungen wie z.B. die Frage, ob Richter in Zukunft durch einen Roboter ersetzt werden könnten.[2] In der Wirklichkeit des Strafverfahrensrechts spielen solche Ideen (noch) keine Rolle. Gleichwohl kann bereits eingangs festgehalten werden, dass vor allem die Ermittlungsbehörden von der Digitalisierung profitiert haben. Diese hat nämlich dazu geführt, dass die Beweisgewinnung für die Strafverfolgungsorgane in den meisten Konstellationen deutlich ertragreicher geworden ist. Dies folgt in erster Linie daraus, dass durch die zunehmende Digitalisierung des Lebensalltags mehr Datenspuren erzeugt werden. Es gibt jedenfalls nur noch wenige Bereiche, in denen nicht digitaler Output erzeugt wird. Das weckt Begehrlichkeiten.

I. Metainformationen als beweisrechtlicher Mehrwert

Ein persönliches Beispiel mag dies vielleicht verdeutlichen: Vor einigen Tagen erhielt ich eine E-Mail von einem (bekannten) Streamingdienst, in der dieser anregt, dass ich mir „noch einmal" meine Lieblingsmomente aus den Serien und Filmen der vergangenen Zeit ansehe. Für die meisten mag dies wenig spektakulär erscheinen. Es zeigt aber, welche Fülle an Daten wir erzeugen. Dieser Streamingdienst hat analysiert, dass ich

---

1 Der Beitrag basiert auf einem Onlinevortrag des Verfassers auf den 26. Würzburger Europarechtstagen am 21.11.2020 und wurde für die Veröffentlichung mit Fußnoten versehen. Der Vortragsstil wurde dabei beibehalten.

2 So lautet der Titel des Beitrags von *Gless/Wohlers,* in: FS Kindhäuser (2019), S. 147 „Subsumtionsautomat 2.0 – Künstliche Intelligenz statt menschlicher Richter?" Die Verfasser sind sich bewusst, dass dies eine Vorstellung aus dem Bereich der Science-Fiction ist und halten als Ergebnis (S. 164) fest, dass es wenig wahrscheinlich sei, dass Richter durch Roboter ersetzt würden.

häufig, statt einen kompletten Film anzusehen, bestimmte „berühmte" oder „nachdenkliche" Szenen aus verschiedenen Filmen anschaue. Auf den ersten Blick wirkt diese Information vielleicht harmlos. Aber auch solche Daten können bei der Beweiswürdigung im Strafverfahrensrecht eine Rolle spielen.[3] Deshalb ist es auch keine Überraschung, dass Ermittler immer mehr – und vor allem bei Durchsuchungen – auf Daten zugreifen (wollen). Das hängt mit einer zweiten Verbesserung zusammen, die die Digitalisierung für Strafverfolger bedeutet. Der Zugriff auf Daten betrifft nicht nur die Inhalte, sondern die „Metainformationen",[4] die einen Rückschluss auf das ganze Benutzerverhalten zulassen.[5] Letzteres spielt in vielen Verfahren mittlerweile eine nicht zu unterschätzende Rolle. Stellen Sie sich vor, es geht bei der Beweisführung darum festzustellen, wer bei Vertragsverhandlungen für die (untreuerelevante) letzte eingefügte Passage verantwortlich gewesen ist. Im analogen Zeitalter hätte man dazu ausschließlich über den Zeugenbeweis Feststellungen treffen können. Aufgrund der Digitalisierung und der mit ihr verbundenen Erzeugung von Spuren in Dateien kann heute in vielen Fällen problemlos nachvollzogen werden, wer wann und wie auf das Dokument zugegriffen hat.[6]

II. E-Mails im Zentrum des Interesses

Eine weitere Erkenntnismöglichkeit der Ermittler ist der Zugriff auf E-Mails. Hierdurch können Ermittler in komplexen Verantwortungsgefügen schnell nachvollziehen, wer (vermeintlich) über welchen Vorgang informiert gewesen ist.[7] Damit verbunden ist zum Teil auch ein Einblick in die

---

3 Im Rahmen eines Verfahrens wegen des Verdachts des Totschlags kann es darauf ankommen, dass der Beschuldigte zu einer bestimmten Zeit an einem bestimmten Ort gewesen sein soll. Wenn dieser Beschuldigte zu seiner Entlastung vortragen würde, dass er an diesem Abend stattdessen zu Hause saß und sich „Fernsehschnipsel" aus verschiedenen Fernsehserien angesehen hat, könnte über eine Anfrage beim Streamingdienst diese Beweistatsache überprüft werden und die Glaubhaftigkeit der Einlassung überprüft werden.

4 Das sind nach *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik (2015), Glossar, Daten, die in den Daten enthalten sind. *Savic*, Die digitale Dimension des Strafprozessrechts (2019), S. 84 beschreibt die Metadaten als Kontext-Daten, also solche Daten, die das Dokument, dem sie beigefügt werden, beschreiben oder zusätzliche Informationen hierzu geben.

5 *Blechschmitt*, MMR 2018, 361, 362.

6 *Basar*, in: FS Wessing (2015), S. 635, 639.

7 *Lepper*, CCZ 2018, 178.

Gedankenführung der Verfasser von E-Mails, was die Beweisführung im subjektiven Tatbestand erleichtern kann. Bekanntlich ist der Nachweis des Vorsatzes nur selten direkt möglich, sondern wird aus begleitenden Umständen gewonnen. Insofern ist die Digitalisierung für Ermittler auch unter diesem Gesichtspunkt eine positive Entwicklung. Die Bedeutung dieses Zugriffs darf man nicht unterschätzen. Nicht ohne Grund hat zuletzt das Landgericht Görlitz für den Bereich der Digitalisierung hervorgehoben, dass auf Smartphones und ähnlichen Geräten intimste Inhalte zu finden sind. Hinsichtlich der Qualität dieser Kommunikation hat das Gericht eine Parallele zu Tagebucheinträgen gezogen.[8] Erstaunlich ist, dass die Strafprozessordnung zur Sicherstellung und Beschlagnahme von Daten unverändert § 94 StPO als Eingriffsnorm zur Verfügung stellt. Am Anfang der Digitalisierung stand rechtlich die Frage im Raum, ob Daten überhaupt eigenständig sichergestellt werden könnten. Grund für diese Diskussion war der Umstand, dass in § 94 Abs. 1 StPO ausschließlich von *Gegenständen* die Rede ist.[9] Die Zulässigkeit der Sicherstellung von Daten ist allerdings durch die Rechtsprechung[10] geklärt und steht in der Praxis auch nicht zur Diskussion.

B. Leitentscheidungen zum digitalen Beweisrecht

Angesichts der Funktion des § 94 StPO als Generalnorm zur Sicherstellung von Daten verwundert es nicht, dass die aus der Praxis resultierenden Fragen ebenfalls durch die Rechtsprechung geklärt werden mussten. Die Entscheidungen betrafen die generelle Zulässigkeit der Sicherstellung von Daten,[11] die Voraussetzungen für den Zugriff auf E-Mails,[12] die Separierung von Daten,[13] das digitale Akteneinsichtsrecht der Verteidigung,[14] den

---

8 LG Görlitz, Beschluss vom 18. Juni 2020 – 3 Qs 67/20 (Juris): „Der moderne Mensch hat den größten Teil seiner - teilweise intimsten – Kommunikation auf solchen Geräten gespeichert. Teilweise werden dort auch Selbstreflexionen niedergelegt. Die Parallele zum besonderen Schutz von Tagebucheinträgen drängt sich förmlich auf."

9 In anderen Vorschriften hat der Gesetzgeber bereits Anpassungen vorgenommen. So ist seit 2018 für den Urkundsbeweis in § 249 Abs. 1 S. 2 StPO definiert, dass elektronische Dokumente Urkunden sind.

10 BVerfG, Beschl. v. 12.04.2005 – 2 BvR 1027/02 = NJW 2005, 1917.

11 BVerfG, Beschl. v. 12.04.2005 – 2 BvR 1027/02 = NJW 2005, 1917.

12 BVerfG, Beschl. v. 16.06.2009 – 2 BvR 902/06 = MMR 2009, 673.

13 BVerfG, Beschl. v. 20.09.2018 – 2 BVR 708/18 = NJW 2018, 3571.

14 BGH, Beschl. v. 11.02.2014 – 1 StR 355/13 = StV 2015, 10.

Rechtsschutz gegen die Datenbeschlagnahme nach Erledigung der Maßnahme,[15] die Rückgabeverpflichtung von Datenträgern[16] und die Pflicht zur Löschung von Daten.[17] Zugespitzt lässt sich sagen, dass der Gesetzgeber keine dieser Fragen selbst geregelt hat. Die Digitalisierung des Strafverfahrensrechts wird vornehmlich durch die Rechtsprechung geformt. Das führt dazu, dass nicht alle Fragen geklärt sind.[18] Für die Datenbeschlagnahme halte ich immer noch den Beschluss des Bundesverfassungsgerichts aus dem Jahr 2005 für die wichtigste Entscheidung.[19] Das Bundesverfassungsgericht hat hier nicht nur allgemein über die Zulässigkeit der Sicherstellung von Daten befunden, sondern tatsächlich auch Eckpunkte zur Vorgehensweise der digitalen Sicherstellung beschrieben. Erstaunlicherweise sind die Ausführungen von damals auch heute noch für die Praxis relevant und haben sich durchaus als „best practice"-Lösung bewährt. Ausgangspunkt war, dass das Bundesverfassungsgericht für die Durchsuchung, Sicherstellung und Beschlagnahme von Datenträgern das Gebot aufgestellt hat, der Zugriff auf für das Verfahren bedeutungslose Informationen müsse im Rahmen des Vertretbaren vermieden werden. Damit hat das Bundesverfassungsgericht dem *umfassenden* Zugriff auf Datensätze strafprozessual[20] grundsätzlich[21] den Riegel vorgeschoben.[22] Dieser Grundsatz ist deswegen von besonderer Bedeutung, weil in der Praxis kaum noch Durchsu-

---

15 LG Nürnberg-Fürth, Beschl. v. 22.12.2017 – 18 Qs 49/17 = ZD 2018, 317.

16 OLG Schleswig, Urteil v. 21.12.2017 – 11 U 68/17 = NStZ-RR 2018, 38.

17 BayObLG München, Beschl. v. 27.01.2020 – 203 Vas 1846/19 (Juris).

18 Am drängendsten betrifft dies die Gratwanderung zwischen dem Grundsatz der Sicherstellung der Authentizität elektronischer Daten und dem rechtlichen Gebot der Datenminimierung, vgl. hierzu *Basar/Hieramente*, NStZ 2018, 681; *Rückert*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren (2020), S. 9, 11. Der Grundsatz der Datenminimierung gilt nach § 47 BDSG auch für Strafverfolgungsbehörden.

19 BVerfG, Beschluss vom 12.04.2005 – 2 BvR 1027/02 = NJW 2005, 1917.

20 Für die Verdachtsgewinnung spielen auch die polizeilichen Datenbanken eine wichtige Rolle, vgl. *Singelnstein*, in: FS Rogall (2018), S. 725, 729.

21 Anders soll es sein, wenn eine Begrenzung faktisch oder technisch nicht gewährleistet werden kann. Das Gericht hat aber darauf hingewiesen, dass die Möglichkeiten ausgeschöpft werden müssen. Aus forensischer Sicht ist dagegen eine Vollsicherung vorzugswürdig, vgl. *Jahn/Brodowski*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren (2020), S. 67, 75. Zur Auflösung dieses Spannungsverhältnisses vgl. *Basar/Hieramente*, NStZ 2018, 681, 685.

22 Wörtlich: „Der Zugriff auf den gesamten Datenbestand ist nicht erforderlich, wenn die Sicherung der beweiserheblichen Daten auf eine andere, die Betroffenen weniger belastende Weise ebenso gut erreicht werden kann", BVerfG NJW 2005, 1917, 1920.

chungen durchgeführt werden, bei denen die Ermittler nicht sofort (!) auf die IT zugreifen. Die Digitalisierung hat hier zu einer radikalen Trendwende geführt. Die Sicherstellung von digitalisierten Informationen war zu Beginn von großem Vorteil für die Betroffenen, weil ansonsten die Sicherstellung der entsprechenden Papierakten „drohte". Noch zu Beginn meiner Tätigkeit als Rechtsanwalt habe ich Verfahren erlebt, in denen aufgrund der Sicherstellung der Arbeitsunterlagen eine bereits bestehende Schieflage im Unternehmen zur Insolvenz des betroffenen Unternehmens oder Unternehmers geführt hat. Eine solche Situation wird durch die technisierte Beweiserhebung erfreulicherweise vermieden. Dagegen steht aber, dass bei der digitalisierten Beweissicherung die Grenze zwischen (zulässigen) Zufallsfunden und (unzulässigen) Strukturermittlungen leicht verwischen kann.[23]

C. Ungelöste strafprozessuale Probleme

Während die grundsätzliche Bedeutung der Digitalisierung für die Beweiserhebung damit nicht in Rede steht, stellen sich in der Praxis eine ganze Reihe von sich hieran anschließenden Fragestellungen. Dies betrifft die Fragen, (1.) ob bei einer Durchsuchung die Daten oder die Geräte sichergestellt werden bzw. wann welche Art der Sicherstellung vorzuziehen ist, (2.) welche Kriterien bei der Selektion der Daten herangezogen werden, (3.) wie Daten in der Cloud forensisch exakt sichergestellt werden (können), (4.) wie mit Passwörtern bei verschlüsselten Systemen umzugehen ist, (5.) ob und wann der gesamte Server sichergestellt werden kann, (6.) wie die Beeinträchtigung im System minimal bleiben kann und (7) unter welchen Bedingungen eine Vereinbarung zwischen der Staatsanwaltschaft und den Betroffenen in Betracht kommt. All diese Fragen können in jeder Durchsuchung akut werden und bedürfen dann einer entsprechenden Lösung. Ich will versuchen, einige der beschriebenen Probleme aus Sicht der Praxis „aufzulösen".

Bezüglich der Frage, ob bei einer Durchsuchung die Daten oder die Geräte sichergestellt werden, gilt, dass die Ermittler dazu neigen, die mobilen Geräte physisch sicherzustellen.[24] Hintergrund ist hier, dass diese einfach zu transportieren sind und eine Ortsbesichtigung oder Sicherung einen

---

23 *Basar*, in: FS Wessing (2015), S. 635, 635.

24 Zu den denkbaren Varianten *Bell*, Beschlagnahme und Akteneinsicht bei elektronischen Medien (2016), S. 11 f.

größeren Aufwand nach sich ziehen würde. Gleichwohl ist es für die Auswertung mittlerweile Standard, dass (auch) von diesen Geräten zunächst 1:1-Kopien gefertigt werden.[25] Bei größeren Geräten präferieren die Ermittler eine Sichtung und Sicherung vor Ort. Das kann insbesondere in Unternehmen dazu führen, dass Durchsuchungen mehrere Tage dauern, weil geklärt werden muss, welche Daten mitgenommen werden. Manchmal ist die Datenmenge dann so groß, dass die Sicherstellung über mehrere Nächte „laufen" muss. Vorsicht ist geboten, wenn es darum geht, die sogenannten Metadaten (mit-)zusichern. Ohne sogenannte „Schreibblocker" kann das einfache Kopieren von Information dazu führen, dass entsprechende Informationen beim Kopiervorgang überschrieben werden.[26] Beim Zugriff auf Server stellt sich hier allerdings das Problem, dass diese im laufenden Betrieb sind und so eine entsprechende Veränderung im System durch den Zugriff nicht vermieden werden kann. Hier wird man den Zugriff daher dokumentieren müssen, um die Integrität und den Beweiswert der betroffenen Daten zu gewährleisten.[27] In der Praxis ist es daher nicht unüblich, dass bei der Sicherstellung von Daten in Live-Systemen „Verhandlungen" über die Vorgehensweise geführt werden. Diese Gespräche leben davon, dass der Betroffene bereit ist, bestimmte Daten zur Verfügung zu stellen. Natürlich handelt es sich dabei nicht um eine „Basar-Feilscherei", weil für die Ermittler unverändert § 160 StPO gilt. Gegenstand solcher Gespräche können alle Aspekte einer digitalen Sicherstellung sein. In bestimmten Fällen kommt auch eine Datenlieferungsvereinbarung in Betracht.[28] Die Beteiligung des durch die Durchsuchung Betroffenen ist allerdings durch die DSGVO „verkompliziert". Hier besteht nämlich eine Sollbruchstelle zur StPO. Aufgrund der in Art. 2 Abs. 2 lit. d) DSGVO verankerten Regelung, müssen die Ermittlungsbehörden im Strafverfahrensrecht die Vorgaben der DSGVO nicht beachten. Dies gilt allerdings nicht für die Betroffenen einer Durchsuchungsmaßnahme mit der Folge, dass diese nicht völlig frei über diese Daten disponieren können. Aus Letzterem ergeben sich in der Praxis auch eine ganze Reihe von (bislang ungenutzten) Verteidigungsoptionen.[29] Bemerkenswert ist allerdings, dass ohne die Unterstützung der Betroffenen die Sicherstellung von Daten vor Ort die Ermittler vor große Herausforderungen stellen kann. Dies gilt nicht zu-

---

25 *Geschonneck*, Computer-Forensik, (6. Aufl. 2014), S. 91.
26 *Basar*, in: FS Wessing (2015), S. 635, 645.
27 *Heinson*, IT-Forensik (2018), S. 150; zum strafprozessualen Gebot der Authentizität von Beweismitteln *Basar*, in: FS Wessing (2015), S. 635, 641.
28 *Wenzl*, NStZ 2021, 395.
29 Zum Ganzen *Basar*, StraFo 2019, 222, 225.

letzt auch für die Sicherstellung von Daten in Clouds. Für eine Vielzahl von Cloud-Anbietern gilt, dass die Daten, die sich in der Cloud befinden, sich physisch nicht am Ort der Durchsuchung befinden. Nach unverändert herrschender Ansicht ist in diesem Punkt ohne die Hilfe der Betroffenen Schluss für die Ermittler. Diese haben bekanntlich – auch über § 110 Abs. 3 StPO – keine rechtliche Möglichkeit, von Deutschland aus auf Daten im Ausland zuzugreifen.[30] Ob dies so bleiben wird, wird man abwarten müssen.[31]

Ein zunehmendes Problem in der Praxis sind Passwörter bei verschlüsselten Systemen. Bei Durchsuchungen von Unternehmen ist dies allerdings seltener der Fall. Hintergrund ist, dass hier oftmals eine Sicherung an (laufenden) Servern erfolgt. Die Problematik des Zugriffs auf Datenträger spielt vor allem bei Smartphones eine erhebliche Rolle. Viele marktübliche Geräte bieten eine so gute Grundverschlüsselung an, dass Ermittler nicht oder nur mit großem Aufwand in der Lage sind, den Passwortschutz auszuhebeln und die auf dem Gerät befindlichen Daten zu entschlüsseln. In 80 % der Fälle fordern die Ermittler daher zunächst die Passwörter bei den Betroffenen an. Für mich etwas überraschend stimmen viele (unverteidigte) Beschuldigte dem zu und stellen ihr Passwort freiwillig zur Verfügung. Dies ist vor allem in Wirtschaftsstrafverfahren weit verbreitet. Ich bin mir sicher, dass wir in Deutschland eine andere Diskussion führen würden, wenn die Betroffenen bezüglich ihrer Passwörter gegenüber den Ermittlern zurückhaltender agieren würden. In Großbritannien besteht nach dem Regulation of Investigatory Powers Act aus dem Jahr 2000 für *Beschuldigte* die Pflicht, elektronische Schlüssel zur Verfügung zu stellen.[32] Und last but not least besteht das in der Praxis unzureichend gelöste Problem, wie mit der Auswertung von großen Datenmengen verfahren werden soll. Der Umfang der Daten ist für die meisten Ermittler und Landeskriminalämter in großen BTMG-, OK- und Wirtschaftsstrafverfahren kaum zu beherrschen. Teilweise sind die Landeskriminalämter so schwach besetzt, dass für einzelne Auswertungen von Handys ein Vorlauf von über einem Jahr eingerechnet werden muss. Daher hat sich mittlerweile ein Markt von EDV-Experten entwickelt, die den Ermittlungsbehörden ihre Unterstützung anbieten. Rechtlich ist die Art der Zusammenarbeit bislang nur rudi-

---

30 Zuletzt bestätigt im sog. "Jones Day" Verfahren vgl. BVerfG, Beschl. v. 27.06.2018 – 2 BvR 1405/17.

31 Zur geplanten E-Evidence-Verordnung vgl. den Beitrag von *Esser* in diesem Band. Eine erste Übersicht liefert *Basar*, Juris-PR Strafrecht 5/2019 Anm. 1; vgl. dann die Entscheidung des LA Koblenz, einführend *Hieramente/Basar*, Juris-PR Strafrecht.

32 Zur Rechtslage in Deutschland *Rottmeier/Eckel*, NStZ 2020, 193.

mentär geregelt. In der Praxis werden die entsprechenden (privaten) Unternehmen von der Staatsanwaltschaft als Sachverständige nach § 73 StPO benannt. Die Auswahl der Sachverständigen erfolgt nach den für Sachverständige üblichen Grundsätzen. Insofern ist bei der Bestellung wenig Kontrolle hinsichtlich der Qualifikation des Gutachters vorhanden. Ob es sich in der Sache noch um eine Tätigkeit als Sachverständiger oder schon um ausgelagerte Ermittlungstätigkeit handelt, ist Gegenstand einer aktuellen Diskussion.[33] Man wird angesichts der limitierten Ressourcen der Ermittlungsbehörden in Zukunft sicherlich nicht umhinkommen, private Unternehmen in die Ermittlungsarbeit einzubeziehen. Anders wird das Ressourcenproblem nicht lösbar sein. Gleichwohl wird es hierzu ein klares rechtliches Korsett geben müssen, das zwischen (interessengeleiteter) Ermittlungsarbeit und (unabhängiger) Tätigkeit als Sachverständiger klar unterscheidet und Qualitätsstandards für die digitale Zuarbeit definiert. All diese Problemkreise zeigen, dass die Digitalisierung das strafprozessuale Beweisrecht viel stärker verändert als der rechtliche Rahmen dies vermuten lässt. Teilweise werden Grundsätze des Strafverfahrensrechts tangiert. Vor dem Hintergrund der allgemeinen Entwicklung des Strafrechts und des Strafverfahrensrechts hin zu einem auf Sicherheit bedachten Steuerungsinstrument liegt es in der Natur der Sache, dass die Lösungen darauf zielen, der Beweiserhebung keine Steine in den Weg zu legen. Gedankengänge, die die Rechte des Beschuldigten stärken, finden sich dagegen nur selten.

D. Beweisstücke

Durch die Digitalisierung erleben wir einen Prozess der gleichzeitigen Technisierung des Strafverfahrens. Die Problematik der Auswertung der sichergestellten Daten zeigt, dass es vor allem auch um Ressourcen zur Aufklärung geht. In manchen Verfahren entwickelt sich nahezu eine Materialschlacht. Dabei geht es um die Frage, ob der Beschuldigte oder das neben ihm betroffene Unternehmen Zeit und Aufwand in die Hand nehmen, um die Daten schneller und besser auszuwerten als die Ermittlungsbehörden es tun können. Hier geht es nicht selten um die Verfahrens- und Deutungshoheit in der Beweiswürdigung. Aus Sicht der Verteidigung, die die Grundrechte der Beschuldigten zu wahren hat, existieren zwei Hauptprobleme. Zum einen besteht immer noch Streit um das Akteneinsichtsrecht in digitale Asservate. Desweiteren sind die Verteidiger regelmäßig

33 *Wackernagel/Graßie*, NStZ 2021, 12.

technisch gar nicht in der Lage, eine solche Auswertung vorzunehmen. Anders als die Staatsanwaltschaft verfügen die Verteidiger nicht über eigene Ermittlungsbeamte, die eine solche Auswertung vornehmen können.

I. Das (fehlende) Akteneinsichtsrecht

Hinsichtlich der Akteneinsicht in digitale Asservate – bzw. korrekt formuliert: in die Kopien von Asservaten – besteht derzeit eine rechtliche Diskussion. Um sich der Bedeutung dieser Frage gewahr zu werden, mag folgender Standardfall einen Einstieg bieten: Die Staatsanwaltschaft sichert in einem Strafverfahren gegen zwei Geschäftsführer eines Unternehmens 100.000 E-Mails aller mit einem bestimmten Projekt befassten Mitarbeiter. Gemäß den Vorgaben der Rechtsprechung hat die Staatsanwaltschaft eine Selektion vorgenommen, die mit Suchworten vorbereitet wurde. Zugleich erfolgte auch eine zeitliche Eingrenzung der gesichteten E-Mails. In der Praxis werden nicht alle E-Mails zur (digitalen) Akte genommen, sondern in der Regel nur diejenigen, die bei der Auswertung (durch die Kriminalpolizei oder den Sachverständigen) als für die Ermittlung relevant angesehen worden sind. Es versteht sich von selbst, dass die Selektion durch die im Raum stehende Verdachtshypothese geprägt wird und entlastende E-Mails nur selten gefunden werden. Ich kenne nicht wenige Verfahren, wo ich – meine Kanzlei verfügt über dasselbe Auswertungsprogramm wie die meisten Ermittlungsbehörden – nach eigener Auswertung zu einem völlig anderen Befund gelangt bin als die Ermittler in ihren forensischen Berichten. Dies hat mehrere Gründe: Zum einen suche ich als Verteidiger – anders als die ohnehin mit knapper Zeit ausgestatteten Beamten – natürlich *aktiv* nach Entlastungsmomenten. Außerdem habe ich mich unmittelbar mit dem Sachverhalt und der Akte auseinandergesetzt. Bei den Auswertungen der Ermittlungsbehörden werden diese von Sachbearbeitern durchgeführt, die den Fall selbst gar nicht bearbeiten. Das führt dann dazu, dass Inhalte meist isoliert und nicht kontextbezogen bewertet werden. Dabei ist für die Verteidigung von Vorteil, dass sie auf das Wissen des (beschuldigten) Mandanten zugreifen kann und so in bestimmten Konstellationen einen Wissensvorsprung hat.[34] Das alles verdeutlicht, warum es für die Verteidigung essenziell ist, denselben Zugang zu den unbearbeiteten Datensätzen zu erhalten wie die Ermittlungsbehörden. In der Praxis muss die-

34 *Schlothauer*, in: MAH Strafverteidigung (2. Aufl. 2014), Teil B. Verteidigung in den einzelnen Abschnitten des Strafverfahrens § 3 Ermittlungsverfahren Rn. 57.

ser Zugang allerdings immer wieder erstritten werden. Die strafprozessuale Qualität der digitalen Asservate hinsichtlich § 147 StPO, der das Akteneinsichtsrecht für die Verteidigung regelt, ist nicht geklärt. Bestritten wird, ob digitale Daten Bestandteil der Akte sind (oder sein müssen) oder als Beweisstücke im Sinne von § 147 Abs. 4 StPO zu werten sind. Hintergrund dieses Streits ist die Frage, ob die Verteidigung einen Anspruch auf Überlassung der Daten hat oder ob – wie für originale Beweisstücke grundsätzlich vorgesehen – ein Mitgabeverbot gilt und die Einsichtnahme in den Räumlichkeiten der Justiz vorzunehmen ist.[35] Hierzu hat sich mittlerweile auch eine ganze Reihe von Oberlandesgerichten positioniert. Einige Oberlandesgerichte haben das Mitgabeverbot bestätigt; andere haben der Verteidigung einen entsprechenden Anspruch zugesprochen.[36]

II. Auswertungsstrategien

Die Bedeutung dieser Frage wird erst dann deutlich, wenn man sich vergegenwärtigt, was die Konsequenz dieser Entscheidungen ist. Einige Staatsanwälte argumentieren damit, dass eine Einsicht auf der Geschäftsstelle die Rechte der Verteidigung und des Beschuldigten ausreichend sichert. Dies verkennt allerdings, dass die Auswertung von Datensätzen ein permanenter Prozess ist, der nicht mit einer einmaligen Durchsicht erledigt ist. Erinnert sei daran, dass die Auswertung ohne entsprechende Tools nicht möglich ist. Hinzu kommt, dass nur die wenigsten Strafjuristen die Fähigkeiten haben, entsprechende Programme ad hoc zu nutzen. Bei dem von Ermittlern immer noch am häufigsten genutzten Auswertungstool[37] handelt es sich um ein Tool zur forensischen Auswertung,[38] das ohne Einführung und wiederholte Anwendung von Nutzern kaum beherrscht werden dürfte. Insofern wird der Verteidiger – wie auch die Justiz – bei der Bearbeitung des Datensatzes Hilfe benötigen. Die Oberlandesgerichte haben entschieden, dass es im Ermessen des mit dem Verfahren betrauten Richters steht, ob er die Datensätze der Verteidigung zur eigenen Auswertung überlässt oder ob die Verteidigung diese digitalen Informationen auf der Geschäftsstelle zu den üblichen Zeiten der Justiz einsehen muss.

---

35 Zum Ganzen: *Thomas/Kämpfer*, in: MK (2014), § 147 Rn. 37 f.
36 Zum Ganzen: *Wettley/Nöding,* NStZ 2016, 633.
37 http://www.x-ways.net/forensics/index-d.html, Stand 11.08.2021.
38 Ein forensisches Programm ist nicht nur ein Analyseprogramm, sondern ermöglicht auch die Untersuchung digitaler Spuren, vgl. *Basar*, in: FS Wessing (2015), S. 635, 638.

Die Einsicht auf der Geschäftsstelle wird allerdings nur in den seltensten Fällen eine sachgerechte Verteidigung ermöglichen. Grund hierfür ist, dass eine Sichtung der Daten immer auch eine entsprechende Aufbereitung der Daten mit den Tools voraussetzt. Das kann deswegen notwendig sein, weil man auch gelöschte Dateien in die Suche miteinschließen will oder nach entsprechenden Dateistrukturen sucht oder bestimmte Filter anwenden will. Je größer die Datenmenge ist, umso mehr Zeit benötigt das Programm, um entsprechende Suchen durchzuführen. Nach meiner Erfahrung kann die Aufbereitung Tage und Wochen in Anspruch nehmen. Regelmäßig – und so arbeiten im Übrigen auch Ermittler – lässt man diese Vorgänge „zwischendurch" oder über Nacht laufen. Es ist erfahrungsgemäß auch immer wieder notwendig, den Stand des Aufbereitungsvorgangs zu überprüfen, weil es gerade bei großen Datenmengen vorkommt, dass das entsprechende Tool den Aufbereitungsvorgang nicht fehlerfrei durchgeführt hat und der Prozess von vorne gestartet werden muss. Insofern ist eine permanente und enge Kontrolle während des laufenden Aufbereitungsprozesses notwendig. Solche Prozesse lassen sich auf der Geschäftsstelle der Justiz zu den üblichen Geschäftszeiten kaum durchführen. Hierbei ist zu berücksichtigen, dass jedes Mal eine gesonderte An- und Abfahrt notwendig ist. Ungelöst bleibt darüber hinaus, auf welchen Datenträgern diese Suchläufe durchgeführt werden. Wenn die Ermittlungsbehörden den Datenträger zur Verfügung stellen und im Anschluss der Auswertung behalten, könnten Ermittler im temporären Verzeichnis der Festplatte nachvollziehen, welche Dateien die Verteidigung markiert und kopiert hat und mit welchen Suchbegriffen sie gearbeitet hat. Prinzipiell ist so ein Einblick in das Verteidigungskonzept möglich, da die Suchmethode des Verteidigers oftmals nur das Ergebnis der Sachverhaltsaufarbeitung mit dem Mandanten ist. Auch bei KI-gestützten Suchmethoden wird es immer erforderlich sein, Zwischenergebnisse mit dem Mandanten zu besprechen und entsprechende Analysen des Datenbestandes darauf anzupassen. Auch aus diesem Grund verbietet es sich, die Verteidigung auf die Einsicht bei der Geschäftsstelle zu verweisen.

E. Zusammenfassung und Thesen

Ich bin überzeugt, dass die Digitalisierung das Strafverfahren noch weiter verändern wird. Darauf müssen sich alle Verfahrensbeteiligte einstellen. Allerdings ist in Rechnung zu stellen, dass – trotz oder gerade wegen der ungelösten Probleme – die Ermittler im Strafverfahrensrecht heute so stark sind wie noch nie in der Geschichte der Strafprozessordnung. Die Digitali-

sierung hat dazu geführt, dass das Verhalten der Bürgerinnen und Bürgern überall (digitale) Spuren hinterlässt. Darauf können Ermittler zugreifen. Dagegen hat die Digitalisierung nicht dazu geführt, die Verteidigungsrechte des Beschuldigten zu stärken. Der verstärkte Einsatz von Software zur Auswertung von großen Datenmengen durch Spezialisten lässt besorgen, dass Sachbeweise selektiv in das Verfahren eingeführt werden.

Dem kann nur begegnet werden, wenn sich alle Strafjuristen in Zukunft auch mit der Technik solcher Programme beschäftigen.[39] Dies gilt vielleicht noch mehr für die Verteidiger als für die Gerichte und Staatsanwaltschaften. Ohne die Fähigkeit, selbstständig Daten auswerten zu können, wird es der Verteidigung jedenfalls zunehmend erschwert, Beweiswürdigung oder gar ganze Verdachtshypothesen einer kritischen Prüfung zu unterziehen und gegebenenfalls anzugreifen. Damit entfällt aber auch die Möglichkeit, alternative Hypothesen in den Raum zu stellen und somit aktiv Einfluss auf das Verfahren zu nehmen. So gestaltet würde die Digitalisierung einen wesentlichen Faktor des Strafverfahrens – die kontradiktorische Verhandlung – schwächen und die Qualität der Wahrheitssuche mindern. Der Gesetzgeber wäre gut beraten, die Digitalisierung zum Anlass zu nehmen, das Strafverfahrensrecht neu aufzusetzen und an das 21. Jahrhundert anzupassen. Dazu gehört es auch, die Verteidigung in der (digitalen) StPO aufzuwerten und somit die Grundrechte der Bürgerinnen und Bürger zu stärken.

---

39 So auch *Rückert*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren (2020), S. 9, 35.