Prof. Dr. Carsten Momsen
& Ass. iur. Nils Hercher

Digitale Beweismittel im Strafprozess
Eignung, Gewinnung, Verwertung, Revisibilität

Digitale Daten besitzen ein erhebliches Potential, verschiedene Kommunikationsformen zu verändern.|[1] Da der Strafprozess natürlich nichts anderes als eine spezifische Kommunikationsplattform darstellt,|[2] wirken sich diese Veränderungen auch hier aus. Als handgreiflichstes Beispiel sei vorab nur daran erinnert, in welchem Umfang in den letzten Jahren – zumindest in komplexeren Strafverfahren - die Auswertung von E-Mails und Kommunikationsdaten, sog. »Social Networks«, zum Gegenstand der Beweisaufnahme geworden ist.|[3]

Und: In welchem Umfang durch die Auswertung dieser Daten die Beweisgrundlage für eine spätere Verurteilung gelegt wird. Dies mag uns in einem ersten Zugriff aus der Verteidigerperspektive wünschen lassen, die Mandanten würden weniger freizügig entsprechende Beweisspuren legen, so wie es im Bereich tradierter Kommunikationsformen seit jeher – der Ausdruck sei gestattet – »lege artis« ist.

Zum anderen aber wird Verteidigern wie auch Beschuldigten zumindest retrospektiv vor Augen geführt, wie wenig gesichert die meisten digitalen Kommunikationswege sind – Diskretion und Vertraulichkeit sind mit den üblicherweise zur Verfügung stehenden Mitteln kaum zu gewährleisten.
Dieser Aspekt ist meines Erachtens von primärer Bedeutung, wenn man sich über Konsequenzen digitaler Beweismittel im Strafprozess Gedanken macht, wie auch dann, wenn notwendige Veränderungen konturiert werden sollen.
Von ebenso zentraler Bedeutung ist der mit der Datensicherheit eng zusammenhängende Aspekt der Manipulierbarkeit digitaler Beweismittel, mit den daran hängenden Fragen der Beweissicherung und des Beweiswerts.
Der Weg von hier zur Verwertbarkeitsproblematik ist nicht weit und führt schließlich unmittelbar in das Revisionsrecht.

1 Dazu mit diversen Beispielen: *Rudolph*, Akzeptanz des Rechtsstaats in der Justiz, 2013, Materialband zum 36. Strafverteidigertag in Freiburg i.Br. vom 8.-10.März 2013, im Erscheinen.

2 AK-*Wassermann*, Einl. II, Rn. 10 ff.

3 Die Polizei Hannover hat bspw. ein Pilotprojekt »Facebook-Fahndung« gestartet, http://www.handelsblatt.com/politik/deutschland/pilotprojekt-wie-die-polizei-in-hannover-nach-zeugen-sucht/7382618.html.

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

I. Allgemeines

Gestatten Sie mir zunächst, den Gegenstand der Betrachtung in etwas vereinfachender Form zu umreißen – ich darf zur Vertiefung auf die Ausführungen von Carsten Rudolph |[4] verweisen.

1. Arbeitsdefinition

In den vergangenen Jahren ist die Digitalisierung des Alltags stetig vorangeschritten. Der Konsum digitaler Medien jedweder Art ist mittlerweile genauso selbstverständlich wie die für jedermann und jederzeit mögliche Erstellung digitaler Medien.

Inhalte und Informationen werden zusätzlich, zunehmend aber auch ausschließlich, digital erstellt und verbreitet. Geschäfte werden online getätigt; EDV-Systeme finden sich in nahezu allen größeren Firmen oder auch Banken. Diese Entwicklung wirkt sich auch auf die Strafrechtspflege aus: Der Inbegriff des Strafverfahrens ist die Wahrheitsfindung mittels der Rekonstruktion des tatsächlichen Geschehens, die nur gelingen kann, wenn sämtliche vorhandenen Beweismittel erkannt und sachgerecht ausgewertet werden. |[5] Gleichzeitig entstehen gänzlich neue Möglichkeiten der Begehung von Straftaten im digitalen Raum, die unter dem prägnanten Begriff der »Cybercrimes« |[6] zusammengefasst werden können. Die Anpassung der bestehenden Normen des Straf- und Strafverfahrensrechts kann dieser Entwicklung weder vollumfänglich, noch zeitnah folgen. |[7] Sie sollte es – ultima ratio – auch nicht. Ähnlich wie es beispielsweise für die Entwicklung neuer Dopingmethoden oder Designerdrogen gilt, läuft das Recht auch im Bereich digitaler Kommunikation der tatsächlichen Entwicklung in jeweils unterschiedlichem Abstand hinterher.

Es gilt daher eine Möglichkeit zu finden, digitale Medien und deren Besonderheiten im Rahmen der bestehenden Gesetzeslage in die Strafrechtspflege einzugliedern und dabei Standards zu schaffen, die den Anforderungen eines Strafverfahrens gerecht werden.

4 Fn.1

5 Vgl. BVerfGE 57, 250 (275); 63, 45 (61); *Meyer-Goßner*, EinlRn. 10; § 244 Rn. 11.

6 Zur Definition vgl. unter »3. Deliktsstruktur und digitale Beweismittel«.

7 Vgl. *Gercke,* Der unterbliebene Schritt vom Computer- zum Internetstrafrecht, AnwBl 2012, 709 (710ff.).

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

2. Steigende Bedeutung digitaler Informationen steigende Bedeutung digitaler Beweismittel

Die Zunahme digitaler Informationen geht zwangsläufig einher mit der steigenden Bedeutung digitaler Beweismittel. Textdokumente sowie Foto-, Video- und Audioaufnahmen werden mittlerweile überwiegend digital erstellt und gespeichert. Aufbewahrt werden alle Arten von Daten auf Speichermedien in Computern und Handys oder aber auf Servern und in der Cloud. Kommunikation findet über das Internet statt, sei es über Dienste wie Facebook oder Twitter, sei es über Foren – und natürlich via E-Mail. Handys lassen sich orten; über die Einwahl in Funkzellen können Bewegungen oder Aufenthalte nachvollzogen werden. Alle diese Informationen können für ein Strafverfahren relevant sein und daher als Beweismittel in Betracht kommen. Alibis können verifiziert oder falsifiziert werden, Beweggründe lassen sich möglicherweise nachvollziehen und Verbindungen zwischen Personen können ebenfalls nachvollzogen werden. Aufgrund dessen ist eine Berücksichtigung digitaler Daten als Beweismittel nicht nur geboten, sondern praktisch unausweichlich.

Häufig ist zudem der Aufwand der Überwachung erheblich geringer, da die Daten entweder von den Betroffenen selbst oder von den Diensteanbietern erhoben und konserviert werden.

3. Besonderheiten digitaler Beweismittel

Dabei ist indes zu beachten, dass digitale Beweismittel Besonderheiten aufweisen, die es im Umgang mit diesen zu berücksichtigen gilt. Bedingt durch die digitale Form der gespeicherten Informationen besteht die Möglichkeit, diese relativ einfach und in vielerlei Hinsicht zu verändern.[8] Es ist jedermann ohne größere Schwierigkeiten möglich, mit einem Computer erstellte Texte zu verändern oder Bilder und Videos zu bearbeiten. Die entsprechenden Programme sind zum Teil kostenlos erhältlich und bieten Möglichkeiten der nachträglichen Veränderung, die bei einem handschriftlich erstellten Dokument oder einem von einem Negativ entwickelten Foto jedenfalls nicht so einfach möglich wären.

Mit dieser leichten Veränderbarkeit einher geht eine hohe Unsicherheit in Bezug auf die Richtigkeit einer Tatsache, die mit der jeweiligen Datei nachgewiesen werden soll. Probleme kann auch die Zuordnung digitaler Informationen zu einer Person bereiten. Wird beispielweise ein zur Begehung eines Cybercrimes benutzter Computer in einem Familienhaushalt, einer WG oder

8 *Gercke* a.a.O. (Fn. 7), 713.

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

in einem Unternehmen von mehreren Menschen benutzt, wird die Beantwortung der Frage nach der Täterschaft unter Umständen erhebliche Schwierigkeiten bereiten. | [9]

Auch die Rechtsprechung verneint (wenn auch zumeist in Akteneinsichtsgesuche betreffenden Fällen) bei Delikten mit Internetbezug einen hinreichenden Tatverdacht gegen den Anschlussinhaber nur anhand der Zuordnung zu seiner IP-Adresse, da die konkrete Täterschaft damit gerade nicht festgestellt/angenommen werden kann. | [10]

4. Unterschiede zu »herkömmlichen« Beweismitteln

Diese Unsicherheiten können noch verstärkt werden, wenn man die Unterschiede digitaler Beweismittel zu ihren herkömmlichen analogen Pendants betrachtet.

Digitale Daten müssen zwingend einen oder mehrere Zwischenschritte durchlaufen, um überhaupt nutzbar zu sein. Natürlich muss beispielsweise auch ein analog aufgenommenes Foto entwickelt werden. Die Entwicklung eines solchen ist indes ein rein chemischer Prozess, mit dessen Hilfe das fotografierte Motiv in unveränderter Form sichtbar gemacht wird. | [11] Für digitale Dateien dagegen benötigt man entsprechende Programme, um die in einer Text-, Bild- oder Audiodatei vorhandenen Informationen sinnvoll gebrauchen zu können; zur Verkörperung ist das Erstellen eines Ausdrucks erforderlich. Hierbei kann nicht ausgeschlossen werden, dass die Anzeige je nach dem verwendeten Programm variieren könnte; es ist nicht gewährleistet, dass eine Datei in der Form und Vollständigkeit wiedergegeben wird, die der ursprünglich Erstellten entspricht. | [12] Entsprechendes lässt sich in Bezug auf die Daten von »Voice over IP«-Telefongesprächen feststellen.

5. Vorteile digitaler Beweismittel

Neben den genannten Unsicherheiten darf aber nicht vergessen werden, dass die Digitalisierung auch Vorteile mit sich bringt. So einfach nachträgliche

9 Vgl. *Casey,* Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, Summer 2002, Volume 1, Issue 2, S. 2; *Chaski,* Who's at the Keyboard? – Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Spring 2005, Volume 4, Issue 1, S. 1ff.

10 Vgl. LG Karlsruhe MMR 2010, 68; LG Köln, Beschluss vom 20. Oktober 2008 – 106-5/08, juris; MMR 2009, 291; LG Saarbrücken K&R 2008, 320.

11 Vgl. den entsprechenden Wikipedia-Eintrag unter http://de.wikipedia.org/wiki/Entwicklung_(Film).

12 Als Beispiel seien nur Textdateien genannt, für die aufgrund der unterschiedlichsten Konfigurationen bei der Erstellung das PDF-Format zur möglichst einheitlichen Wiedergabe geschaffen worden ist, vgl. http://de.wikipedia.org/wiki/Portable_Document_Format.

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

Veränderungen von Dateien auch vorgenommen werden können, geschieht dies in der Regel doch nicht spurlos. Denn wie die Ursprungsinformationen können auch die Modifikationen, häufig sogar die einzelnen Datenaufrufe, nachvollzogen und nachgewiesen werden. Dass hier in Bezug auf Modifikationen der Metadaten der Weg gleichwohl in einen im übertragenen Sinne »infinitiven Regress« eröffnet ist, bedarf keiner näheren Erläuterung.

Eine Rekonstruktion der Datei in ihrer ursprünglichen Form ist von sachkundiger Hand zu bewerkstelligen. Gleiches gilt für eine Wiederherstellung vernichteter Daten. Das einfache Formatieren einer Festplatte ist weniger endgültig als das Verbrennen eines Briefes oder eines Fotofilms.[13] Das Internet ist weniger anonym, als es viele Menschen glauben; die Bewegungen eines durchschnittlichen Nutzers lassen sich nachverfolgen.[14] Allerdings gilt auch hier das »Hase-und-Igel«-Prinzip. Man kann nur mutmaßen, ob im konkreten Fall gerade die Strafverfolgungsbehörden oder die Manipulatoren »die Nase vorn« haben werden.

Zu beachten ist dabei auch, dass die unter dem Aspekt der IT-Sicherheit vielfach und dringend angeratene Benutzung von Anonymisierungssoftware geradezu eine systematische Entwertung des digitalen Beweismittels zur Folge hat.[15]

Ebenfalls nicht aus dem Fokus der Aufmerksamkeit sollte geraten, dass - wie jedes Beweismittel auch - das digitale zur Entlastung von einem Vorwurf dienen kann.

II. Gewinnung und Erhebung digitaler Beweismittel

1. Umgang mit digitalen Beweismitteln/Beweissicherung

Bedingt durch die dargestellten Besonderheiten digitaler Beweismittel bedarf der Umgang mit ihnen spezifischen Methoden und einer besonderen Sorgfalt.

Nur wenn möglichst einheitliche Standards bestehen und beachtet werden, lassen sich etwaige Unsicherheiten hinsichtlich der Integrität einer zum Beweis geeigneten und gedachten Datei von Anfang an vermeiden.

Um die jeweilige Datei in ihrem ursprünglichen Zustand zu erhalten, sollte als erster Schritt die Erstellung einer Kopie erfolgen. Mittels des Hashwertes[16] - der jedenfalls nur mit erheblichem Aufwand zu manipulieren ist[17]

13 *Casey,* Foundations of Digital Forensics, in: *Casey*, Digital Evidence and Computer Crime, S. 26.

14 *Casey* a.a.O. (Fn. 13), S. 29.

15 *Meier*, MSchrKrim 2012, S. 198.

16 Wikipedia Stichwort »Hashfunktion«: Eine *kryptologische Hashfunktion* oder *kryptographische Has-*

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

- kann zu jeder Zeit nachgewiesen werden, dass im Laufe der weiteren Ermittlungen keinerlei Veränderung der Ausgangsdatei erfolgt ist:

Etwaige Zweifel dahingehend können so ohne Weiteres ausgeräumt werden.[18] Mögliche Fehlerquellen sind zu erkennen und zu beachten – je nach Datentyp und Endgerät.

Bei E-Mails sind nicht nur die bereits abgerufenen und heruntergeladenen Nachrichten zu beachten, sondern auch diejenigen, die sich noch auf dem Server des Mail-Anbieters befinden.

Mit einem Handy aufgenommene Dateien oder verschickte und empfangene Kurznachrichten können sich nicht nur auf dem internen Speicher befinden, sondern auch auf Speicherkarten.[19] Genau wie auch bei »herkömmlichen« Beweismitteln sollten möglichst wenige Personen eine Datei be- oder verarbeiten und sämtliche Schritte lückenlos dokumentieren.

2. Beweissicherung – Datensicherung – Datensicherheit

Die soeben dargestellten Besonderheiten im Umgang mit digitalen Beweismitteln setzen voraus, dass »digitale Tatorte« möglichst von Beginn der Ermittlungen an auch als solche wahrgenommen und entsprechend behandelt werden. Unerlässlich ist eine vollständige Beweissicherung.

Es reicht gerade nicht aus, die Ermittlungen auf ein Endgerät wie einen Computer oder ein Handy zu beschränken, wenn Peripherie existiert, auf der sich ebenfalls Daten befinden können. Externe Festplatten und Speicherkarten müssen gefunden und beachtet werden.[20]

Die gefundenen Daten sind sachgerecht zu sichern, wobei sich die Anfertigung einer vollständigen Kopie des betroffenen Datenträgers anbietet.[21] Auf

hfunktion ist eine spezielle Form der Hashfunktion, welche kollisionsresistent oder eine Einwegfunktion (oder beides) ist. Eine Hashfunktion ist eine Funktion, die eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge mit fester Länge abbildet. Mathematisch ist diese Funktion nicht injektiv (linkseindeutig) und nicht notwendigerweise surjektiv (rechtstotal). Anwendungen von kryptologischen Hashfunktionen sind vor allem die Datenverarbeitung, zur Integritätsprüfung von Dateien oder Nachrichten. Darüber hinaus werden sie eingesetzt zur Verschleierung von Passwortdateien, als Datenbasis digitaler Signaturen, als Pseudo-Zufallszahlengeneratoren oder zur Konstruktion von Blockchiffren.

17 Vgl. LG Köln, Beschluss vom 20. Oktober 2008 – 106-5/08, juris.

18 Vgl. *Meyers/Rogers,* Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Fall 2004, Volume 3, Issue 2, S. 6f.

19 Vgl. *Casey/Schatz,* Conducting Digital Investigations, in: *Casey,* Digital Evidence and Computer Crime, S. 211f.

20 Vgl. dazuausführlichauch*Casey,* Handling a Digital Crime Scene, in: *Casey,* Digital Evidence and Computer Crime, S. 227ff. (241).

21 Vgl. aber auch *Bäcker/Freiling/Schmitt,* Selektion vor Sicherung - Methoden zur effizienten forensischen Sicherung von digitalen Speichermedien, DuD 2010, 80.

diese Weise können die weiteren Ermittlungen anhand des gesamten Datenbestands geführt werden, ohne dass der Betroffene auf die Benutzung des Endgeräts verzichten muss: Ein Umstand, der gerade bei Selbstständigen, die auf ihren Computer angewiesen sind, von entscheidender Bedeutung ist. Dies setzt indes voraus, dass die sichergestellten Daten ihrerseits bei den Ermittlungsbehörden mit dem geringstmöglichen Risiko eines Verlustes aufbewahrt werden müssen.

Der Zugang dazu muss so abgesichert sein, dass ein Zugriff durch Unbefugte – sowohl externe, als auch interne – nahezu ausgeschlossen werden kann. Dies ist zwingend erforderlich, wenn man berücksichtigt, dass nicht ausgeschlossen werden kann, dass unter den Daten auch vertrauliche Informationen, angefangen von Zugangskennwörtern zu Online-Diensten bis hin zu Geschäftsgeheimnissen, vorhanden sein können. | [22]

Wird eine Festplatte vollständig kopiert, erschließt sich deren gesamter Inhalt, anders als bei einem Aktenordner, nicht ohne Weiteres und insbesondere auch nicht zwangsläufig nach einem erstmaligen Überblick.

Der Vorauswahl, welche Daten und in welcher Reihenfolge diese zu sichten sind, kommt daher eine noch wesentlich höhere Bedeutung zu, als bei herkömmlichen Beweismitteln. Ebenso stellt sich für die spätere Verhandlungsführung die Frage, welche Daten durch Ausdruck für die Verfahrensakte - von einer »Handakte« zu sprechen, erscheint nicht wirklich sachgerecht - perpetuiert werden sollen und in welcher Form dem Mündlichkeits- und Unmittelbarkeitsprinzip Rechnung zu tragen ist.

Dies gilt nicht zuletzt mit Blick auf die gegebenenfalls am Verfahren beteiligten Laienrichter und ist – wie noch zu zeigen sein wird – auch für mögliche Revisionen von entscheidender Bedeutung: Stichwort »Rekonstruktionsverbot«!

3. Deliktsstruktur und digitale Beweismittel

Welche Bedeutung digitalen Beweismitteln in einem konkreten Einzelfall zukommt, ist nicht zuletzt abhängig von der jeweils gegenständlichen Deliktsstruktur.

Handelt es sich um ein »klassisches« Delikt, bei dem sich die Tathandlung nicht im digitalen Raum abspielt, werden in der Regel herkömmliche Beweismittel vorhanden und auch ausreichend sein, um die Tat rekonstruieren zu können.

22 Vgl. den Leitfaden IT-Forensik des BSI, S. 42ff., 89. Der Leitfaden kann unter der Adresse https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/ThemenCS/IT-Forensik/it-forensik.html heruntergeladen werden.

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

Ein Diebstahl kann beispielsweise durch Zeugenaussagen und das Auffinden des Diebesguts aufgeklärt werden. Digitale Beweismittel sind in einem solchen Fall nur als weitere Indizien geeignet und erforderlich. Hat der Täter sich per Email über die Tat ausgetauscht oder das Diebesgut online zum Verkauf angeboten, werden diese Aspekte bei der Verfolgung der Tat und von Anschlussdelikten wie einer Hehlerei zwar von Bedeutung, aber nicht zwingend erforderlich sein. Selbstverständlich kann es auch vorkommen, dass ein Diebstahl einzig mit Hilfe digitaler Beweismittel aufgeklärt werden muss.
Sind keine Zeugen vorhanden oder ist das Diebesgut nicht auffindbar, besteht dennoch die Möglichkeit, dass die Anwesenheit des Täters am Tatort durch die Einwahl seines Handys in die örtliche Funkzelle bestätigt wird, und dass eventuell damit aufgenommene Bilder von der Beute existieren. Derartige Daten dürften für sich alleine betrachtet im Einzelfall sogar für eine Überführung ausreichend sein.

Offenkundige Relevanz besitzen digitale Beweismittel dagegen im Bereich von »Cybercrimes«. Nach der Cybercrime Convention des Europarats versteht man darunter

(1) Angriffe auf die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen,

(2) Angriffe auf netzunabhängige Rechtsgüter, bei denen I(nformations-) u(nd) K(ommunikations) – Technologie zum Einsatz kommt,

(5) über das Internet verbreitete inhaltsbezogene Straftaten und

(4) entsprechende Schutzgüterverletzungen.[23]

Interessant daran ist, dass sich ein Großteil dieser Delikte natürlich auch gegen das digitale Beweismittel selbst richten kann!

Liegt ein solches Cybercrime vor, also eine Tat, die sich ausschließlich im digitalen Raum abspielt, bleibt den Ermittlungsbehörden in Ermangelung herkömmlicher Beweismittel nichts anderes übrig, als sich einzig und alleine auf digitale Daten zu verlassen und sich dieser zu bedienen. Wer beispielsweise unbefugt in ein Firmennetzwerk eindringt und sich dort vertrauliche Daten beschafft, hinterlässt keine greifbaren Spuren.

Nochmals sei darauf hingewiesen, dass die Rechtsprechung bislang bei Delikten mit Internetbezug einen hinreichenden Tatverdacht gegen den Anschlussinhaber nur anhand der Zuordnung zu seiner IP-Adresse verneint, da die konkrete Täterschaft damit gerade nicht festgestellt/angenommen werden

23 Näher *Meier*, MSchrKrim 2012, S. 184.

kann.|[24] Die Rekonstruktion einer solchen Tat kann nur unter Auswertung von Log-Dateien, der IP-Adresse des Täters und den bei diesem gespeicherten Daten erfolgen. Eine derartige Ermittlungsarbeit erfordert zwingend die notwendige Sachkunde und vor allem auch Ausstattung.

Die Rückverfolgung eines Zugriffs wird in den meisten Fällen durch Anonymisierungsmaßnahmen erschwert werden, die erkannt und umgangen werden müssen.|[25] So gilt es nachzuweisen, wer den angreifenden Computer zum Tatzeitpunkt benutzt hat, beispielsweise durch die Auswertung der erfolgten Log-ins mittels eines nur dem Täter bekannten Kennworts. Dass insoweit, etwa bei einer großangelegten Ermittlung, die trotz erheblichem Aufwand im Sande zu verlaufen droht, auch einmal die Versuchung bestehen könnte, durch Selektion oder andere Manipulationsformen Daten »passend« zu machen, ist auch ins Kalkül zu ziehen.

Sodann gibt es natürlich Mischformen, wie die sogenannten eBay-Betrügereien, welche in aller Regel mit kombinierten Ermittlungsansätzen verfolgt werden. Der Anfangsverdacht wird sich in den meisten Fällen aus einer Zeugenaussage ergeben, die weitere Ermittlung ist dagegen in hohem Maße auf die Auswertung digitaler Daten angewiesen.

Eine steigende Bedeutung weisen auch allgemeine Delikte wie Beleidigungen, Nötigungen oder auch der Diebstahl immateriellen Eigentums im sogenannten »second life« auf.|[26]

Empirisch gesehen hat der Betrug die größte Bedeutung bei den knapp 250.000 erfassten Straftaten, die mit dem »Tatmittel Internet« begangen wurden (80 %). Dabei hat in einigen Deliktsbereichen die Internetkriminalität eine »nahezu konstitutive Bedeutung« erlangt. Für den Warenbetrug geht man von ca. 75 % aus, ebenso beim Computerbetrug. Verbreitung pornographischer Schriften erfolgt zu gut 60 % und strafbare Urheberrechtsverstöße erfolgen zu ungefähr 50 % via Internet.|[27]

Der Missbrauch von Kreditkarten wiederum kann auch durch die Anzeige von Geschädigten zur Kenntnis der Ermittlungsbehörden gelangen. Sehr häufig jedoch werden verdächtige Umsätze dadurch auffällig, dass die algorithmen-basierten automatischen Überwachungsprogramme der Kreditkar-

24 Vgl. Fn. 10.

25 Vgl. dazu insbesondere in technischer Hinsicht auch ausführlich *Casey,* PracticalApproachestoRecoveringEncrypted Digital Evidence, International Journal of Digital Evidence, Fall 2002, Volume 1, Issue 3, S. 1ff.

26 *Meier*, MSchrKrim 2012, S. 188.

27 Ausf. *Meier*, MSchrKrim 2012, S. 187.

tenunternehmen anschlagen, in aller Regel lange, bevor ein Kunde Verdacht schöpft.

Abseits der Massenkriminalität haben digitale Beweismittel in Umfangsverfahren der Wirtschafts- und Steuerkriminalität eine kaum zu überschätzende Bedeutung. Dies gilt beispielsweise im Bereich der Kapitalmarktkriminalität, wo häufig schon sämtliche inkriminierten Aktionen und Vorgänge ausschließlich digital abgewickelt werden, man denke nur an den sogenannten »Hochfrequenzhandel«.

Geht es beispielsweise um den Vorwurf der Marktmanipulation, so werden verdächtige Transaktionen häufig allein im Wege automatisierter empirischer Echtzeit-Auswertung der Kursentwicklung bestimmter Papiere bekannt. Diese Daten lassen gegebenenfalls wiederum einen Rückschluss auf die Urheber der Transaktionen zu. Gleiches gilt für Kontodatenauswertungen und ähnliches.

Wenn nun beispielsweise für § 20a WpHG die prozentuale Höhe der Kursschwankung eine entscheidende Rolle spielt, so müssen die Preisbildungsfaktoren unter Ausblendung von Reserveursachen und Berücksichtigung des Marktverhaltens anderer Marktteilnehmer ermittelt werden, um überhaupt einen zurechenbaren Taterfolg vorwerfen zu können. Hierzu wird es regelmäßig sachverständigen Beistands bedürfen. | [28]

Abgesehen von den Deliktsformen, bei deren Begehung digitale Daten bereits eine zentrale Bedeutung haben, steigt die Bedeutung digitaler Beweise im Grundsatz umso stärker, je mehr Kommunikation zwischen den Tatbeteiligten erfolgt.

Dementsprechend verkompliziert sich die Problematik, wenn die digitalen Beweismittel ursprünglich im Rahmen einer unternehmensinternen Ermittlung erhoben werden. Denn diese folgt als private Ermittlung nur sehr begrenzt strafprozessualen Grundsätzen. Dies führt zu noch ungeklärten Fragen für die Verwertbarkeit so gewonnener Beweismittel, seien diese nun mit oder ohne Einverständnis des Unternehmens oder des Unternehmensanwalts in den Strafprozess eingeführt worden.

4. IT-Forensik – Bedeutung unternehmensinterner Ermittlungen

Für die Bearbeitung der vorgenannten Fallkonstellationen ist die sog. »IT-Forensik« unerlässlich. Üblicherweise wird darunter ein Fachgebiet verstanden, das sich mit dem Nachweis und der Aufklärung von Straftaten unter

28 Ausf. *Schröder*, Handbuch Kapitalmarktstrafrecht, Rn. 563 ff., 585d.

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

Verwendung von IT-Komponenten beschäftigt. Diese Sichtweise auf die IT-Forensik umfasst insbesondere die Tätigkeiten speziell geschulter Strafverfolgungsbehörden, aber auch rein private, unternehmensinterne Ermittlungen, die sich ausschließlich mit dem Erkennen und Protokollieren von Eingriffen in Daten- und Netzwerksystemen befassen. Definiert wird die IT-Forensik als die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung, insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.

Unterschieden wird zwischen der Post-mortem-Analyse, die einen Vorfall nachträglich aufklärt, und der Live- oder Online-Forensik, bei der die Untersuchung bereits während des Vorfalls beginnt. Beiden Methoden gleich ist das Ziel, eine zum Eindringen in das System genutzte Lücke nicht nur zu finden, sondern auch zu schließen. Das Vorgehen ist vergleichbar mit dem bei der Rekonstruktion eines herkömmlichen Tathergangs: Zu beantworten ist die Frage, was wo wann wie passiert ist; für eine etwaige Strafverfolgung ist zusätzlich nach dem »durch wen« zu fragen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in einem Leitfaden die Anforderungen an einen forensischen Ermittlungsprozess im IT-Bereich zusammengefasst, die im Wesentlichen den bereits dargestellten Besonderheiten digitaler Beweismittel Rechnung tragen.[29] Verlangt wird eine Akzeptanz der angewandten Methoden und Schritte; diese müssen in der Fachwelt beschrieben und allgemein anerkannt sein. Bei der Anwendung neuer Methoden ist deren Korrektheit nachzuweisen. Um eine Glaubwürdigkeit zu gewährleisten, muss die Robustheit und Funktionalität von Methoden nachweisbar gegeben sein.

Eine Wiederholbarkeit muss möglich sein; bedienen sich Dritte der eingesetzten Hilfsmittel und Methoden, so müssen bei dem gleichen Ausgangsmaterial dieselben Ergebnisse erzielt werden. Sichergestellte digitale Beweise dürfen nicht unbemerkt durch die Untersuchung selbst verändert werden.

Die Sicherung dieser Integrität muss belegbar sein. Durch die Auswahl der Methoden muss es möglich sein, logisch nachvollziehbare Verbindungen zwischen Ereignissen und Beweisspuren und auch zu Personen herzustellen; nur so können Ursache und Auswirkung miteinander verknüpft werden.

Schließlich muss für jeden einzelnen Schritt des Ermittlungsprozesses eine lückenlose Dokumentation erstellt werden. Zusätzlich bedarf es eines lücken-

29 Siehe Fn. 22; dazu, dass diese Vorgaben technisch gesehen relativ sind, näher *Rudolph*aaO. (Fn. 1).

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

losen Nachweises über den Verbleib von digitalen Spuren und der Ergebnisse der daran vorgenommenen Untersuchungen, also der Nachverfolgbarkeit der im englischsprachigen Raum bekannten »Chain of Custody«. | [30]

Der typische Ablauf einer Untersuchung im Bereich der IT-Forensik lässt sich - ausgehend von oben genanntem Leitfaden | [31] - im Groben wie folgt darstellen:

Ausgangspunkt einer jeden forensischen Untersuchung – insbesondere einer solchen, die durch den Betroffenen selbst durchgeführt wird – ist ein Symptom in Form eines anormalen Verhaltens innerhalb des Systems. Bereits dieser Ausgangspunkt der Untersuchung ist zu dokumentieren, was beispielsweise durch einen Eintrag in der Logdatei einer Firewall erfolgen kann.

Wird ein Symptom festgestellt, erfolgt die Vorbereitung von dessen Untersuchung. In dieser Phase geht es darum, geeignete forensische Werkzeuge auszuwählen sowie bereitzustellen, und auch dieses zu dokumentieren. Sodann werden die erforderlichen und relevanten Daten gesammelt, also erfasst und gespeichert, und anschließend untersucht.

Da in der Regel bei einem einzelnen Vorfall mehrere Komponenten eines Systems betroffen sind, sind auch mehrere Untersuchungen erforderlich, die im Rahmen einer Datenanalyse zu einem einheitlichen Zeitverlauf zusammengeführt und in einen logischen Zusammenhang gebracht werden. Zum Abschluss wird der gesamte Untersuchungsverlauf dokumentiert, die bereits protokollierten Schritte also in Berichtsform zusammengefasst.

Das so gefundene Ergebnis kann präventiv genutzt werden, um Verbesserungen am System oder auch der IT-Forensik vorzunehmen – ebenfalls denkbar ist natürlich, dass es zur Grundlage einer Strafanzeige gegen den Verursacher des Symptoms gemacht und den Strafverfolgungsbehörden als eine Zusammenstellung digitaler Beweismittel vorgelegt wird.

Ich will auf die allgemeine Problematik der strafprozessualen Verwertung von Informationen, die im Rahmen unternehmensinterner Ermittlungen gewonnen wurden, hier nicht näher eingehen. Zusammengefasst geht es um die hinlänglich bekannten Kollisionen arbeitsvertraglicher Mitwirkungspflichten mit den Beschuldigtenrechten, Fragen der Beschlagnahmefreiheit und last not least des Eingreifens spezifischer Verwertungsverbote aus dem Grundsatz der Fairness, in Fortentwicklung der Hörfallenrechtsprechung. | [32]

30 Leitfaden IT-Forensik (Fn. 22), S. 24; vgl. auch *Casey,* a.a.O. (Fn. 11), S. 21f.

31 Ausführlich Leitfaden IT-Forensik (Fn. 22), S. 87ff.

32 *Momsen* ZIS 2011, 508 ff..

Für digitale Beweismittel ergibt sich insoweit eine besondere Situation, als die internen Ermittler diese zunächst erhoben und ausgewertet haben. Sämtliche der oben genannten Kriterien ordnungsgemäßer Beweiserhebung müssten also bei der erstmaligen Erhebung von den internen Ermittlern beachtet worden sein. Fehler, die bereits hier gemacht werden, können im Strafverfahren in der Regel nicht mehr kompensiert werden, denn die Ermittlungsbehörden finden nicht nur einfach die sprichwörtliche »gemähte Wiese« vor. Häufig werden die Beweismittel in der Weise ausgewertet, zusammengestellt und den staatlichen Strafverfolgungsorganen überlassen, wie es dem Unternehmensinteresse entspricht. Vollständigkeit ist nicht unbedingt die oberste Priorität. So wird der verständliche und strafrechtlich eingehegte Schutz von Geschäftsgeheimnissen beispielsweise häufig dazu führen, dass bestimmte Daten nicht weitergegeben werden. Der Wunsch, bei bestimmten Taten auf die baldige Verjährung oder die geringe Aufdeckungswahrscheinlichkeit zu setzen, ist ebenfalls nicht zu unterschätzen.

Für die Ermittlungsbehörden wird vielfach nicht mehr nachzuvollziehen sein, wie sich das präsentierte Beweismaterial im Verhältnis zu einer Gesamtdatenmenge verhält. Dies macht die Interpretation an sich schon schwierig. Bei digitalen Beweismitteln dürfte der im Rahmen der internen Ermittlung nicht benötigte Rest der digitalen Informationen häufig nach Durchsicht unwiederbringlich gelöscht sein. Teilweise nötigen hierzu auch Datenschutzrichtlinien – denn wie erwähnt handelt es sich im Ursprung um eine private Datenerhebung. Diese Umstände müssen sich meines Erachtens je nach Lage der Dinge massiv auf den Beweiswert dieser, den Strafverfolgungsbehörden zugänglich gemachten, Daten auswirken.

III. Verwertung digitaler Beweismittel

1. Rechtliche Einordnung digitaler Beweismittel im Beweisrecht der StPO

Hat man sich nun vergegenwärtigt, dass die Beachtung digitaler Beweismittel in der heutigen Zeit unumgänglich ist und wie diese zu erheben sind, muss man sich im nächsten Schritt nach dem Ermittlungsverfahren dem Hauptverfahren zu wenden.

Um die gewonnenen Erkenntnisse auch verwerten zu können, stellt sich zwangsweise die Frage nach der sachgerechten Einordnung digitaler Beweismittel in das bestehende Beweisrecht der Strafprozessordnung. Eine solche Verortung ist aufgrund des im Hauptverfahren geltenden Strengbeweisver-

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

fahrens unumgänglich. Die Schwierigkeit liegt hier darin, dass digitale Daten in der Gesetzgebung bislang nicht in dem Umfang berücksichtigt worden sind, der ihrer praktischen Bedeutung gerecht wird. Es fehlt gerade an der Erfahrung und dem Entwicklungsprozess, den analoge Beweismittel und mit ihnen auch die Strafprozessordnung in jahrzehntelanger Anwendung durchlaufen haben. | [33]

Insoweit ist gerade die Strafprozessordnung in diesem Bereich gegenüber den anderen Prozessordnungen im Nachteil, weil es an konkreten Regelungen fehlt, die anderweitig bereits Einzug gefunden haben.

Die Zivilprozessordnung greift elektronische Dokumente an mehreren Stellen auf. In den §§ 130a, 130b ZPO ist explizit geregelt, wie Schriftsätze von den beteiligten Parteien und auch dem Gericht wirksam in elektronischer Form eingebracht werden können. Wie der Ausdruck eines elektronischen Dokuments für die Akte zu erfolgen hat, ergibt sich aus § 298 ZPO; die Möglichkeit zur elektronischen Aktenführung ermöglicht § 298a ZPO. Beweisrechtlich von entscheidender Bedeutung ist § 371 Abs. 1 ZPO, der elektronische Dokumente dem Beweis durch Augenschein zuordnet; zudem begründet § 371a ZPO für diese einen Anscheinsbeweis. Auch im verwaltungsgerichtlichen Verfahren sind elektronische Dokumente kraft Gesetzes als Augenscheinobjekte zu behandeln; dies folgt aus dem Verweis des § 98 VwGO auf die Vorschriften der Zivilprozessordnung inklusive dem genannten § 371 Abs. 1 ZPO.

Der Strafprozessordnung sind derartige Regelungen dagegen gänzlich fremd. Einzige dahingehende Vorschrift ist § 41a StPO, der schriftliche Erklärungen auch in elektronischer Form zulässt, wenn diese mit einer digitalen Signatur versehen sind.

Betrachtet man die anderen Prozessordnungen, liegt es nahe, digitale Beweismittel auch im Strafprozess dem Beweis durch Augenschein zuzuordnen. Dies führt nicht nur zu einer einheitlichen Bewertung innerhalb der gesamten Rechtsordnung, sondern ist auch sachgerecht. Dann allerdings stellt sich die oben bereits angesprochene Frage der Perpetuierung beziehungsweise Visualisierung im Zusammenhang mit Mündlichkeit und Unmittelbarkeit.

Als einzige Alternativen in Betracht kommt meines Erachtens, eine denkbare Einordnung als Urkunde oder allenfalls der »Umweg« über den Sachverständigenbeweis.

33 Vgl. *Knopp,* Rechtliche Perspektiven zur digitalen Beweisführung, 39. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 28.9.2009, Lübeck, S. 2; abrufbar unter http://subs.emis.de/LNI/Proceedings/Proceedings154/gi-proc-154-116.pdf.

Die Heranziehung des § 249 StPO erscheint naheliegend, wird es doch in der Regel auf den Inhalt der jeweiligen Datei ankommen. Allerdings setzt § 249 I StPO Urkunden mit Schriftstücken gleich,[34] also einer bereits verkörperten Gedankenerklärung, die ohne Weiteres verlesen werden kann. Gerade an dieser Eigenschaft fehlt es den digitalen Beweismitteln aber.

Daran ändert auch der Umstand nichts, dass beispielweise Abschriften oder mechanische Vervielfältigungen dem Begriff der Urkunde unterfallen[35] – diese haben gemeinsam, dass sie ihrerseits auf einer bereits vorhandenen Verkörperung basieren, diese aber eben nicht erstmalig schaffen. Anders als bei einem Schriftstück kann nach der Erstellung ohne Weiteres gerade kein direkter Zugriff auf den Inhalt einer Datei erfolgen.

Der Sachverständigenbeweis gewinnt demgegenüber eher im Rahmen der Interpretation von Inhalt und vor allem Authentizität der Information seine entscheidende Bedeutung.[36]

Naheliegender und den Besonderheiten digitaler Medien eher gerecht werdend ist eine Einordnung als Augenscheinobjekt. Der insoweit einschlägige § 86 StPO erfüllt de facto eine Auffangfunktion für sämtliche potentiellen Beweismittel, die nicht den speziell geregelten Fällen des Zeugen-, Sachverständigen- oder Urkundenbeweis unterfallen.[37] Es folgt aus der Natur der Sache, dass sich auch insoweit das Problem ergibt, dass die für einen Augenschein erforderliche sinnliche Wahrnehmung nicht ohne Weiteres, sondern eben erst nach einer Sicht- oder Hörbarmachung möglich ist.

Dem Augenscheinbeweis ist diese Problematik aber nicht fremd, sondern – je nach Augenscheinobjekt – geradezu inhärent:

Als Augenscheingegenstände anerkannt sind auch Lichtbilder, Filme sowie Audio- und Videoaufnahmen,[38] allesamt Medien, bei denen es in aller Regel entscheidend auf den Inhalt ankommt, wodurch eine vorherige Entwicklung beziehungsweise Wiedergabe durch ein entsprechendes Abspielgerät unausweichlich ist.

Anders als bei analogen Medien genügt ein bloßes Abspielen auf einem Gerät allerdings nicht; vielmehr muss neben der Hardware auch die erforderliche Software vorhanden sein und ordnungsgemäß bedient werden. Dennoch

34 LR-*Gollwitzer,* § 249, Rn. 6.

35 *Meyer-Goßner,* § 249, Rn. 6 m.w.N.

36 *Knopp*a.a.O. (Fn. 33) S. 8f.

37 LR-*Krause,* § 86, Rn. 1.

38 *Meyer-Goßner,* § 86, Rn. 10.

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

erscheint die Bejahung eines Augenscheinobjekts angebracht, da es sich bei digitalen Medien letztendlich um die Fortentwicklung der oben genannten analogen Medien handelt. Darüber hinaus ist diese Lösung – soweit es auf den Inhalt ankommt – aber auch diejenige mit der höchsten Praktikabilität.

Der Augenscheinbeweis dürfte in der Regel erst dort an seine Grenzen stoßen, wo nicht der Inhalt einer Datei erheblich oder strittig ist, sondern deren Echtheit, Urheberschaft oder Manipulationsfreiheit. In einem solchen Fall dürfte es dem erkennenden Gericht nahezu unmöglich sein, eine dahingehende qualifizierte Aussage aufgrund eigener Sachkunde zu treffen. Es bleibt nur der Weg über die Hinzuziehung eines Sachverständigen.[39]

Der Sachverständige wiederum ist seinerseits auch auf die entsprechende Ausrüstung - zunächst zur Anzeige und sodann zur Überprüfung von Echtheit, Integrität oder Urheberschaft der betroffenen Datei - angewiesen, deren Einsatz natürlich ebenfalls entsprechend dokumentiert werden muss.

Um jedwede Zweifel von vornherein auszuschließen, müsste ein Gericht vor der Verwertung eines jeden erheblichen digitalen Beweismittels einen Sachverständigen konsultieren, um sich dessen Echtheit oder das Nichtvorhandensein von Manipulationen bestätigen zu lassen. Dies dürfte in der Praxis indes an dem damit einhergehenden Aufwand und den entstehenden Kosten scheitern, weswegen es im Einzelfall dem Betroffenen oder dessen Verteidiger obliegen wird, eine entsprechende Maßnahme herbeizuführen.

2. Besonderer Beweiswert digitaler Beweismittel

Sowohl der Augenscheins-, als auch der Sachverständigenbeweis unterliegen der freien Beweiswürdigung. Soll eine Verurteilung aufgrund der Verwertung digitaler Beweismittel erfolgen, muss das Gericht zu einem - nach der Lebenserfahrung ausreichenden - Maß an Sicherheit gelangen, demgegenüber vernünftige Zweifel nicht mehr aufkommen.[40] Rekapituliert man nun die Besonderheiten einer digitalen Datei, gelangt man unweigerlich zu der Frage, welchen Beweiswert eine solche eigentlich per se besitzt.

Selbst wenn alle Schritte der Beweisgewinnung nachvollzogen und eine Veränderung innerhalb des Ermittlungsverfahrens gänzlich ausgeschlossen werden kann, so sagt dies noch nichts darüber aus, ob nicht schon vor der ersten Sicherstellung eine Manipulation vorgenommen worden ist.[41] Ich verweise nochmals auf den Bereich interner oder privater Ermittlungen!

39 Vgl. *Casey* (Fn. 9), S. 4.

40 BGH NStZ 1988, 237 (238); *Meyer-Goßner,* § 261, Rn. 2 m.w.N.

41 Vgl. dazu anhand des Beispiels eines Digitalfotos ausführlich *Knopp,* Digitalfotos als Beweismittel, ZRP 2008, 156 (158).

Eine gewisse Grundskepsis erscheint wohl angebracht, wenn man bedenkt, dass der Gesetzgeber seinerseits ja selbst für gerichtswirksame elektronische Dokumente eine qualifizierte Signatur nach dem Signaturgesetz verlangt. Handelt es sich bei dem zu berücksichtigen Beweismittel um eine E-Mail, dürfte eine solche Signatur dafür sorgen, dass beispielsweise keine vernünftigen Zweifel an deren Urheberschaft mehr bestehen. Mit dem Vorhandensein einer qualifizierten digitalen Signatur dürfte indes nur in den wenigsten Fällen zu rechnen sein, ist dieses doch eher die Ausnahme als die Regel.

In der Praxis wird diese nur von den wenigsten Benutzern eingesetzt.[42] Diese Problematik lässt sich auf einen Großteil der digitalen Beweismittel übertragen[43]: Technisch realisierbar sind derartige Signaturen oder ähnliche Maßnahmen; zu nennen sind in diesem Zusammenhang auch digitale Wasserzeichen oder Metadaten. Erstere sind indes in der Praxis wenig verbreitet, letzteren wird von der Rechtsprechung aufgrund der wiederum gegebenen Manipulierbarkeit kein erhöhter Beweiswert zugemessen. Wesentlich weiter verbreitet ist demgegenüber die Nutzung der bereits angesprochenen Anonymisierungssoftware.[44] Diese führt im Erfolgsfall zu einer massiven Minderung des Beweiswerts.

Alle diese Umstände könnten den Schluss zulassen, dass der Beweiswert digitaler Beweismittel grundsätzlich als ausgesprochen gering anzusehen ist. Dies lässt aber außer Acht, dass jedwedem Beweismittel eine gewisse Unsicherheit anhaftet. Als Beispiel sei ein Foto genannt: Auch ein analoges Bild kann selbstverständlich manipuliert werden. Wird das aufgenommene Foto verändert und sodann abfotografiert, entsteht ein neues Negativ und mithin ein neues vermeintliches Original. Dieses Vorgehen ist zwar aufwändiger als die Nachbearbeitung oder Veränderung eines digitalen Fotos, es ist aber dennoch möglich.[45]

Werden also keine plausiblen Anhaltspunkte vorgebracht, die gegen die Authentizität einer Datei sprechen, muss einer solchen nicht ohne Weiteres und nur aufgrund ihrer Art ein geringerer Beweiswert beigemessen werden als dem jeweiligen analogen Pendant. Sobald aber Zweifel bestehen, sind diese bei der Entscheidung zu berücksichtigen und müssen – so keine weiteren Beweismittel bestehen – für den Fall der nicht möglichen Ausräumung auch zu einer konsequenten Anwendung des Grundsatzes in dubio pro reo führen.

42 So auch *Knopp* a.a.O. (Fn. 33), S. 9.

43 Vgl. für Digitalfotos *Knopp*a.a.O. (Fn. 41), S. 158f. m.w.N. sowie *Alvarez,* Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis, International Journal of Digital Evidence, Winter 2004, Volume 2, Issue 3, S. 1ff.

44 *Meier*, MSchrKrim 2012, S. 199.

45 Vgl. *Knopp* a.a.O. (Fn. 41), 157 m.w.N.

Problematisch allerdings wird die Situation dort, wo wir sicher wissen, dass ein bestimmter, wenn auch geringer Teil der digitalen Information bei der Speicherung verloren geht. So geht man - meines Wissens etwa - bei Voice-over-IP-Telefongesprächen von einem Verlust von jeweils wenigen Sekunden aus. Dies wird in der Regel die Information nicht entscheidend verfälschen – kann es aber im Einzelfall. | [46]

Zur Erläuterung:

> »Das Telefonieren mit der IP-Telefonie kann sich für den Teilnehmer genauso darstellen wie in der klassischen Telefonie. Wie bei der herkömmlichen Telefonie teilt sich das Telefongespräch dabei in drei grundsätzliche Vorgänge auf, den *Verbindungsaufbau,* die *Gesprächsübertragung* und den *Verbindungsabbau*. Im Unterschied zur klassischen Telefonie werden bei VoIP aber keine dedizierten »Leitungen« durchgeschaltet, sondern die Sprache wird digitalisiert und in kleinen Daten-Paketen über das Internetprotokoll transportiert [...] Da das Internet in seiner heutigen Form (Stand 2008) keine gesicherte Übertragungsqualität zwischen Teilnehmern garantiert, kann es durchaus zu Übertragungsstörungen, Echos, Aussetzern oder Verbindungsabbrüchen kommen. [...] Der Transport von Daten benötigt Zeit. Sie wird als Laufzeit beziehungsweise Latenz (engl. *delay* oder *latency*) bezeichnet und ist bei herkömmlicher Telefonie im Wesentlichen die Summe der Signallaufzeiten auf den Übertragungskanälen. Bei Telefonie über IP-Netze kommen weitere Verzögerungen durch die Paketierung und Zwischenspeicherung sowie gegebenenfalls Datenreduktion, Kompression und Dekompression der Daten hinzu. [...] Daraus resultierende Schwankungen werden als »Jitter« Bezeichnet. Um diese zu kompensieren, werden so genannte »Puf-

46 Wikipedia Stichwort IP-Telefonie: *IP-Telefonie* (kurz für Internet-Protokoll-Telefonie) auch *Internet-Telefonie* oder Voice over IP (kurz VoIP) genannt, ist das Telefonieren über Computernetzwerke, welche nach Internet-Standards aufgebaut sind. Dabei werden für Telefonie typische Informationen, d. h. Sprache und Steuerinformationen beispielsweise für den Verbindungsaufbau, über ein auch für Datenübertragung nutzbares Netz übertragen. Bei den Gesprächsteilnehmern können sowohl Computer, auf IP-Telefonie spezialisierte Telefonendgeräte, als auch über spezielle Adapter angeschlossene klassische Telefone die Verbindung herstellen.

IP-Telefonie ist eine Technologie, die es ermöglicht, den Telefondienst auf IP-Infrastruktur zu realisieren, so dass diese die herkömmliche Telefontechnologie samt ISDN, Netz und allen Komponenten ersetzen kann. Zielsetzung dabei ist eine Reduzierung der Kosten durch ein einheitlich aufgebautes und zu betreibendes Netz. Aufgrund der hohen Einsatzdauer klassischer Telefoniesysteme und der notwendigen Neuinvestitionen für IP-Telefonie wird der Wechsel bei bestehenden Anbietern oft als lang andauernder, gleitender Übergang realisiert. Währenddessen existieren beide Technologien parallel (sanfte Migration). Daraus ergibt sich ein deutlicher Bedarf an Lösungen zur Verbindung beider Telefoniesysteme (etwa über VoIP-Gateways) und die Notwendigkeit zur gezielten Planung des Systemwechsels unter Berücksichtigung der jeweiligen Möglichkeiten für Kosten- und Leistungsoptimierung. Neue Anbieter drängen zunehmend ausschließlich mit neuer Technologie (also IP-Telefonie statt herkömmlichem Telefon) auf den Markt. Ende 2010 nutzten in Deutschland rund 7,7 Millionen Menschen ausschließlich die Voice over IP-Technologie. ...

ferspeicher« (Jitterbuffer) eingesetzt, die eine zusätzliche absichtliche Verzögerung der empfangenen Daten bewirken, um anschließend die Daten isochron auszugeben. Pakete, die noch später ankommen, können nicht mehr in den Ausgabedatenstrom eingearbeitet werden. Die Größe des Pufferspeichers (in Millisekunden) addiert sich zur Laufzeit. Sie erlaubt also die Wahl zwischen mehr Verzögerung oder mehr Paketverlustrate. [...] Von Paketverlust spricht man, wenn gesendete Datenpakete den Empfänger nicht erreichen und deshalb verworfen werden. Bei Echtzeitanwendungen spricht man auch von Paketverlusten, wenn das Paket zwar den Empfänger erreicht, aber zu spät eintrifft, um noch in den Ausgabestrom eingefügt werden zu können. Für Telefonie wird nach ITU-TG.114 eine Paketverlustrate *(packet loss rate)* bis maximal 5 % noch als akzeptabel eingestuft«.

Das bedeutet, dass man auf dieser Basis regelmäßig bei entsprechenden Datenverwertungen in der Beweisaufnahme - jedenfalls in dubio pro reo - unterstellen müsste, dass es noch 5 % nicht dokumentierte Gesprächsinhalte geben kann. Wie soll das Gericht hier jenseits begründeter Zweifel zu der Überzeugung gelangen können, dass nicht an entscheidender Stelle eine kurze Passage verloren gegangen ist. Um es bewusst zu simplifizieren: Ist der letzte dokumentierte Satz »so machen wir es!«, könnte der 5 %-Verlust das allerletzte Wort, nämlich das alles entscheidende »nicht« betroffen haben.

»Durch die Integration der Sprachdatenübertragung in das IP-Netz ergeben sich (weitere) neue Herausforderungen an die IT-Sicherheit.

Die VoIP-Pakete werden über ein so genanntes »Shared Medium« übertragen, also über ein Netz, welches sich mehrere Teilnehmer und unterschiedliche Dienste teilen.

Unter gewissen Voraussetzungen kann es Angreifern möglich sein, die Daten auf dem Übertragungsweg abzugreifen und das Gespräch aufzuzeichnen. Es existieren beispielsweise Programme, mit deren Hilfe der Datenstrom auch aus geswitchten Umgebungen mittels »ARP-Spoofing« abgegriffen und daraus wieder eine Audiodatei erzeugt werden kann«. | [47]

Bereits die wenigen Ausführungen, die im Wesentlichen aus »Wikipedia« entnommen sind, verdeutlichen eines ganz sicher: Sicherheit ist im Bereich nicht gespeicherter Daten de facto nicht zu erlangen. Es sei denn, man kann flankierend auf andere Beweismittel, typischerweise eine Zeugenaussage, zurückgreifen. Die Erkenntnis muss sich auf die Verwertbarkeit der Beweise

47 Wikipedia Stichwort IP-Telefonie

und den ihnen zuzubilligenden Beweiswert im Hauptverfahren genauso wie auf die Überprüfung beider Aspekte im Revisionsverfahren auswirken.

In einem spontanen Zugriff könnte man versucht sein, die Lösung in einer Beweislastumkehr für solche digitalen Beweismittel zu suchen, bei denen von einer entsprechenden Verlustrate auszugehen ist. Das Problem daran ist die mangelnde Praktikabilität. Der Gegenbeweis wird in vielen Fällen nicht gelingen können. Beweislastumkehr würde Nichtbeweisbarkeit bedeuten und zu erheblichen Strafverfolgungsdefiziten gerade im Bereich Cybercrime, Missbrauchskriminalität, rechtsextremistischer Verbreitungsdelikte und organisierter Kriminalität führen. Das wird weder politisch durchsetzbar sein, noch erscheint mir eine so rigide verfassungsrichterliche Einschränkung der Beweiswürdigungstätigkeiten der ordentlichen Gerichtsbarkeit wahrscheinlich zu sein. Hierzu werden eventuell im weiteren Verlauf des Tages nähere Informationen erhalten.

Also kommt alles auf das Gesamtbild der Beweislage an. Hier aber meine ich, werden sich die Gerichte einer zunehmenden Zahl von Beweisanträgen, namentlich auf Hinzuziehung von Sachverständigen, anständigerweise nicht entziehen können. Deren vorhersehbare Ablehnung in vielen Fällen führt in den letzten Bereich meiner Überlegungen, das Revisionsrecht.

IV. Revisionsrechtliche Besonderheiten

Nachstehend seien nur einige Aspekte pars pro toto herausgegriffen. Entsprechende Fehler können im Wege der Sachrüge in Bezug auf die richterliche Überzeugungsbildung, wie sie aus den Urteilsgründen ersichtlich wird, angegriffen werden – Verletzung von § 261 und ggf. auch § 267 StPO in sachlichrechtlicher Hinsicht. In anderen Fällen wird man mit einer Verfahrensrüge wegen der Ablehnung von Beweisanträgen, also als Verletzung von § 244 StPO, ggf. § 261 StPO eher Erfolg haben. Gegebenenfalls kommt auch eine sogenannte »Aufklärungsrüge« nach § 244 in Frage.

1. Rekonstruktionsverbot

Zunächst ist das sogenannte Rekonstruktionsverbot für das Revisionsgericht zu beachten. Das heißt, auch wenn das Revisionsgericht an sich ohne Weiteres die digitalen Beweise gleichsam aus der Akte und im Freibeweis überprüfen könnte, so ist eine dergestaltige eigenständige Beweiswürdigung als tatsachenwertender Akt nach ständiger Rechtsprechung nicht zulässig.[48] Eine darauf zielende Rüge wäre von vornherein ohne jede Erfolgsaussicht.

48 BGH StV 2012, 272; dazu ausf. *Gercke/Wollschläger* StV 2013, 106.

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

Wesentlich weniger klar ist aber – wie *Gercke* und *Wollschläger* jüngst herausgearbeitet haben | [49] –, was das für die Darstellung in den Urteilgründen bedeutet. Einerseits können die digitalen Beweismittel selbst nicht in die Urteilsbegründung eingefügt werden, andererseits sind Verweisungen in die Hauptverhandlungsakte nur in sehr eingeschränktem Umfang zulässig. Das Rekonstruktionsverbot kann sich hier zugunsten des Revisionsführers auswirken. | [50]

Im Ergebnis müssen jedenfalls alle wertenden Aspekte aus den Urteilsgründen unmittelbar nachvollziehbar sein – der BGH hat dies meines Erachtens obita dicta am Beispiel einer digitalen Videoaufzeichnung der Körpermerkmale einer tatverdächtigen Person näher ausgeführt. | [51]

Der Senat kann zwar ein Augenscheinsobjekt oder eine Urkunde im Wege des Freibeweises betrachten, beispielsweise um festzustellen, ob das in den Urteilsgründen in Bezug genommene Beweismittel überhaupt existiert oder überhaupt Daten zu dem angegebenen Thema enthalten kann. Wurde das in Bezug genommene digitale Beweismittel überhaupt zum Gegenstand der Hauptverhandlung gemacht? Gerade dort, wo das Gericht sich aus einem unüberschaubaren Konvolut von digitalen Informationen auf nur einige beschränken muss, unterlaufen derartige Fehler von Zeit zu Zeit. Eine darüber hinausgehende eigentliche Würdigung darf das Revisionsgericht jedoch nicht vornehmen. Das Grundprinzip dürfte sich auf die meisten Erscheinungsformen digitaler Daten als Beweismittel übertragen lassen.

Als Revisionsführer wird man das Urteil genau daraufhin zu untersuchen haben, ob eine erfolgreiche Rüge angebracht werden kann, weil die Gründe entweder die überprüfbaren nahezu offensichtlichen Fehler enthalten oder aber in Bezug auf die Darstellungen im Zusammenhang mit dem digitalen Beweismittel und seinen Beweiswert lückenhaft oder widersprüchlich sind.

2. Besondere Anforderungen an die Beruhensprüfung

In den meisten Fällen wird es um einen relativen Revisionsgrund im Sinne von § 337 StPO gehen. Im Hinblick auf das dann bei ausgeführten Rügen notwendig darzulegende Beruhen ergeben sich die ersten Schwierigkeiten:

Die überaus angenehme Folge einer Beweislastumkehr in der Hauptverhandlung wäre für Revisionsverfahren, dass der Revisionsführer im Hinblick auf

49 *Gercke/Wollschläger*StV 2013, 107; vgl. BGH StV 2013 und StV 2012, 272 sowie.Bspr.v. *Deutscher*NStZ 2012, 229; *Sandherr* NZV 2012, 143; *Krumm* NZV 2012, 267; vgl. zum Ganzen auch *Meyer-Goßner* § 249 Rn. 23

50 BGH StV 2013, 73.

51 Näher die genannten Entscheidungen, dazu ausf. *Gercke/Wollschläger*StV 2013, 107 f.

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

den Beruhensnachweis ein erhebliches Stück weit entlastet würde. Der Umstand, dass nicht sichergestellt wurde, dass keine relevanten Datenverluste stattgefunden haben, kann als Negativtatsache nicht in die Beruhensfrage einfließen. Vielmehr müsste nur dargetan werden, dass das Tatgericht derartige Untersuchungen unterlassen hat, was sich gegebenenfalls aus dem Sitzungsprotokoll ergeben wird, je nachdem, wie weit dessen negative Beweiskraft angesichts der großen Senatsentscheidung zur Rügeverkümmerung überhaupt noch fortbestehen soll. Gehen wir einstweilen davon aus, dass § 274 Absatz 1 StPO bis auf weiteren Widerruf im Übrigen noch gelten soll.[52] Zur Beweislastumkehr aber wird es wie erwähnt nicht kommen.

Daher muss das Beruhen des Urteils auf dem Fehler dargetan werden. Dies wird am ehesten im Wege der Rüge des § 244 StPO wegen fehlerhafter Ablehnung eines Sachverständigenbeweisantrags gelingen können. Dies setzt voraus, dass bereits der Antrag in der Hauptverhandlung entsprechend begründet wurde und dort beispielsweise dargelegt wurde, dass ein entsprechendes Datenverlustrisiko im Angesicht darzulegender aktueller wissenschaftlicher Erkenntnisse besteht, und dass der benannte Sachverständige für das konkrete Beweismittel Anhaltspunkte für einen Datenverlust darlegen wird, zumindest aber es als sicher anzusehen ist, dass das statistische Risiko sich im konkreten Fall verwirklicht hat. Diesem Antrag wird sich das Gericht nicht durch die Behauptung eigener Sachkunde und - meines Erachtens nach – in der Regel auch nicht im Wege der Wahrunterstellung entziehen können.

Ich möchte es bei diesem Beispiel belassen, verbunden mit dem Hinweis, dass sich die Anforderungen an die Sicherstellung des Beweiswertes in der Hauptverhandlung eben auch auf die Ausgestaltung der Revisionsrüge und des Beruhensnachweises auswirken. Dass im Angesicht der Rechtsprechung zu den Rügepräklusionen durch Obliegenheitsverletzungen damit auch die Anforderungen an die Instanzverteidigung nicht geringer werden, liegt auf der Hand.

Mit Blick auf das oben dargestellte Rekonstruktionsverbot hat der Revisionsführer darauf zu achten, dass dargelegt wird, dass und warum die Beweiskette nicht mit alternativen Beweismitteln ebenso durchgängig besteht. An einem Beruhen fehlt es etwa dann, wenn sich aus den in den Urteilsgründen nur unzureichend dargelegten digitalen Beweisen ergibt, wie die Beute beschaffen ist und wie die Täter damit verfahren wollten, aber die Beute später bei einem Hehler sichergestellt wurde, der als Belastungszeuge aussagt.[53]

52 *Docke/v.Döllen/Momsen*StV 1999, 582 ff.; *Momsen* FS-Roxin, 2011, 1403 ff.; KMR-*Momsen* § 337 Rn. 241 ff.
53 Vgl. *Gercke/Wollschläger*StV 2013, 111.

Mit Blick auf die hohen formalen Anforderungen des § 344 StPO trifft den Revisionsführer insoweit eine Pflicht, auch sehr genau darzulegen, dass der Senat den behaupteten Verfahrensfehler ohne Verstoß gegen das Rekonstruktionsverbot nachvollziehen kann. Anderenfalls ist der Weg über die Rüge der Verletzung des § 261 StPO in materieller Hinsicht zu gehen.[54]

3. Verquickung privater und staatlicher Ermittlungen

Auf die Problematik nicht staatlicher beziehungsweise unternehmensinterner Ermittlungen im Zusammenhang mit unüberprüfbaren Beweisverlusten oder anderen Defiziten vor der Weitergabe an die staatlichen Verfolgungsorgane wurde bereits hingewiesen. Diese Aspekte müssen in den Urteilsgründen widergespiegelt werden, anderenfalls sind diese lückenhaft.

Daneben spielen aber auch datenschutzrechtliche Aspekte eine Rolle. Wie also ist zu verfahren, wenn im Unternehmen die Informationen unter offensichtlichem oder auch nur möglichen Verstoß gegen geltendes Datenschutzrecht gewonnen wurden. Ein Beweiserhebungsverbot wird insoweit nicht in Betracht kommen, weil eben nicht die Ermittlungsbehörden erheben. Es mag hier weiterführend sein, sich die Rechtsprechung zur Erhebung und Verwertung der Steuerdateien in der Schweiz und anderen Staaten vor Augen zu halten.

4. Bestehen etwaiger Beweiserhebungs-/-verwertungsverbote

Damit wird sich vieles auf die Verwertbarkeitsfrage konzentrieren.[55] Im Grundsatz gilt meines Erachtens nichts anderes als bei »nicht-digitalen« Beweismitteln. Es gibt spezifische Varianten von denkbaren unselbständigen Verwertungsverboten infolge verbotener Beweiserhebung. Hier ist an das eben schon genannte Datenschutzrecht zu denken, aber auch Beschlagnahmeverbote können von Bedeutung sein und vor allem auch an geschützte Kommunikationsbeziehungen im Sinne von § 53 StPO. Im Hinblick auf die private Beweisgewinnung wird es eher um selbständige Verwertungsverbote gehen, gegebenenfalls wegen fairnesswidriger Datensammlung oder aber wegen rechtswidriger Speicherung der Daten durch Provider oder Anbieter sonstiger Telekommunikationsleistungen. Ebenso kann es beim Einsatz von Trojanern, gleichsam einer verdeckten und proaktiven Schaffung und Gewinnung von digitalen Beweismitteln auf gegebenenfalls staatliche Initiative, zu Problemen kommen. Denn diese Ermittlungsmaßnahme, sei sie privat oder staatlich veranlasst, stellt eine Manipulation des Beweismittels bereits im Ursprung des Gewinnungsprozesses dar.[56] Hier wird unter anderem das

54 Näher KMR/*Momsen* § 337Rn. 74 ff.; 131 ff.

55 Näher *Starostik* LINK und hier im Band.

56 *Singelnstein*, Begleitheft zum 36. Strafverteidigertag, 2012, S. 73

Prof. Dr. Carsten Momsen & Ass. iur. Nils Hercher: Digitale Beweismittel im Strafprozess Eignung, Gewinnung, Verwertung, Revisibilität, in: Die Akzeptanzdes Rechtsstaats in der Justiz, Texte und Ergebnisse des 37. Strafverteidigertag, Freiburg, 8. - 10. März 2013; Hrsg. Strafverteidigervereinigungen, Organisationsbüro, Schriftenreihe der Strafverteidigervereinigungen, Bd.37, Berlin 2014, 173 - 196

Grundrecht auf informationelle Selbstbestimmung in erheblicher Weise betroffen, was in Bezug auf die Rechtmäßigkeit der Verwertung ebenfalls zu berücksichtigen ist – wie auch die Einhaltung der prozessualen Voraussetzungen verdeckter Ermittlungsmaßnahmen.

V. Fazit

Als sehr knappes Fazit: Für das Strafverfahren ergeben sich im Ergebnis vielschichtige Sonderprobleme. Diese liegen zunächst im Bereich der Datenerhebung. Weiterhin ist angesichts der teilweise fragwürdigen Datensicherheit und der häufig nur schwer nachvollziehbaren Manipulierbarkeit ein besonderes Augenmerk auf den Beweiswert digitaler Beweise zulegen – mit Auswirkungen bei der Beweiswürdigung in Hauptverhandlung und Urteil, wie auch für deren Überprüfung in der Revisionsinstanz. Last, not least wird eine Verurteilung, welche maßgeblich auf digitalen Beweismitteln aufbaut, häufig die Heranziehung von Sachverständigen notwendig machen.