Durchsuchung und Beschlagnahme von Daten

Die Festplatte des Computers ist eine wahre Fundgrube. Sie ist heutzutage die Quelle schlechthin, um einen Menschen kennenzulernen – Beukelmann[1]

A. Einleitung

1 Der ständig wachsende EDV[2]- Einsatz in sämtlichen Bereichen des privaten und geschäftlichen Lebens macht durch das oben aufgeführte Zitat in zweierlei Hinsicht deutlich, welche Auswirkungen die Durchsuchungs- und Beschlagnahmemassnahmen haben können.

2 Einerseits stellt der Zugriff auf elektronische Daten und ihre Sicherstellung im Strafverfahren durch die Untersuchungsbehörde eine hohe Eingriffsintensität in die Grundrechte dar. Die Grundrechte werden damit unterwandert, da die Beweismittelfindung öfters einen höheren Stellenwert als die Wahrung der Grundrechte geniesst. So greifen Zwangsmassnahmen, wie die Durchsuchung und die Beschlagnahme einschneidend in verfassungsmässige Rechte des Einzelnen, namentlich die persönliche Freiheit, die Eigentumsgarantie und die Privat- und Geheimsphäre (vgl. Art. 10, 13, 26 BV[3]). Jedoch sind solche Eingriffe zulässig, wenn sie den in Art. 36 BV statuierten Voraussetzungen nicht zuwiderlaufen. Werden die Voraussetzungen nicht verletzt, so ist der Eingriff auf die Festplatte mit den gespeicherten Daten erlaubt. Dadurch können Informationen über den Menschen erkenntlich und somit gegenüber Drittpersonen zugänglich gemacht werden.[4]

3 Anderseits resultiert aus dem technischen Fortschritt ein positiver Aspekt, der zu einem Aufschwung der elektronischen Datenverarbeitung führt. Es können immer mehr Daten auf unterschiedlichen Medien gespeichert und verarbeitet werden, was wiederum zu einem immer grösseren Informationsvolumen führt. Die explosionsartige Verbreitung des Internets hat unsere Gesellschaft tiefgreifend verändert.

4 Die vielfältige Nutzung der *Festplatte des Computers* ist ein positiver Aspekt der Digitalisierung.[5] Demgegenüber wird durch die Möglichkeit eines Zugriffs auf die Daten des Einzelnen eine Gefahr geschaffen. Es kann zur ungewollten Preisgabe von Informationen führen, indem in die Grundrechte der Dateninhaber eingegriffen wird. *Der Mensch wird somit besser kennengelernt.*

---

[1] Näher dazu BEUKELMANN STEPHAN, Die Online- Durchsuchung, in: StraFo 2008, 1.
[2] EDV bezeichnet die elektronische Datenverarbeitung. Dieser ist ein Sammelbegriff für die Erfassung und Bearbeitung von Daten oder Dateien durch elektronische Medien wie z.B. Computer.
[3] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101).
[4] PARK TIDO, Durchsuchung und Beschlagnahme, 3. Aufl., München 2009, N 762. (zit. PARK, N ...).
[5] PARK, N 762.

B. Strafprozessuale Zwangsmassnahmen

5 Die Durchsuchung und die Beschlagnahme sind strafprozessuale Zwangsmassnahmen statuiert in Art. 196 StPO[6]. Meistens folgen sie nacheinander. Tatsache, dass sie grundsätzlich im Vorverfahren angewendet werden, in welchem Stadium die Tatschuld des Betroffenen noch wenig geklärt ist, lässt sie als problematisch erscheinen.

6 Erforderlich nach Art. 197 StPO i.V.m. Art. 36 BV sind eine gesetzliche Grundlage, nach Lehre[7] und Rechtsprechung[8] ein hinreichender Tatverdacht[9], die Beachtung des Subsidiaritätsgrundsatzes, die Beachtung der Verhältnismässigkeit und die Beachtung des öffentlichen Interesses.[10]

C. Durchsuchung von Daten

7 Das Ziel einer Durchsuchung ist die Auffindung von Beweisgegenständen, welche auf ihre Beweiseignung hin zu prüfen sind.[11] Gemäss Art. 246 StPO dürfen Aufzeichnungen, Datenträger sowie Anlagen zur Verbreitung von Speicherung durchsucht werden, wenn die Vermutung besteht, dass darin Informationen vorgefunden werden können, die der Beschlagnahme unterliegen. Es werden damit Urkunden i.w.S. erfasst, namentlich gespeicherte Daten, Laptops, USB- Sticks und Mobiltelefone.[12]

I. Grundsatz

8 Der in Art. 246 StPO beschriebene Grundsatz setzt neben dem hinreichenden Tatverdacht,[13] die Vermutung für das Vorhandensein relevanter Informationen in den Aufzeichnungen voraus. Es genügt zwar der Nachweis eines konkreten Verdachtsmomentes, wonach das strafbare Verhalten die erforderliche Wahrscheinlichkeit die Tatbestandsmerkmale erfüllen könnte.[14] Die Vermutung stellt aber dann wiederum eine Abschwächung der Wahrscheinlichkeit dar, weshalb die Hürde zur Durchsuchung sehr tief liegt. Damit dann der Datenträger nach benötigten Informationen durchsucht werden

---

[6] Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0).

[7] Mit weiteren Verweisen SCHMID NIKLAUS, Strafprozessrecht, Eine Einführung auf der Grundlage des Strafprozessrechtes des Kantons Zürich und des Bundes, 4. Aufl., Zürich/Basel/Genf 2004, N 686. (zit. SCHMID, Strafprozessrecht, N ...); BRUN THEOBALD, Die Beschlagnahme von Bankdokumenten in der internationalen Rechtshilfe, Schweizer Schriften zum Bankenrecht, Bd. 39, Zürich 1996, 19 f. (zit. BRUN); HAUSER ROBERT/SCHWERI ERHARD/HARTMANN KARL, Schweizerisches Strafprozessrecht, 5. Aufl., Basel 2005, § 69 N 28. (zit. HAUSER/SCHWERI/HARTMANN, § ... N ...); OBERHOLZER NIKLAUS, Grundzüge des Strafprozessrechts, Dargestellt am Beispiel des Kantons St. Gallen, Bern 1994, 258 f. (zit. OBERHOLZER).

[8] Prägnant BGE 103 IV 115 und 120; BGE 106 IV 413 und 418; 119 IV 328; 120 IV 299.

[9] Vgl. zum hinreichenden Tatverdacht BRUN, 19 f.

[10] AEPLI MICHAEL, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Zürich 2004, 62. (zit. AEPLI).

[11] MATZKY RALPH, Zugriff auf EDV im Strafprozess, Rechtliche und Technische Probleme der Beschlagnahme und Durchsuchung beim Zugriff auf das Beweismittel „EDV“, Diss., Berlin 1999, 216. (zit. MATZKY).

[12] BGer vom 10.01.2013, 1B_588/512; BGE 139 IV 128 E. 1.3-1.5.

[13] BGer vom 10.10.2012, 1B_397/2012, E 5.1.

[14] Vgl. BGE 139 IV 246; BGer vom 8.5.2013, 1B_637/2012.

kann, braucht es die potenzielle Erheblichkeit[15] zur Auffindung. Es liegt Nahe, dass beim Durchstöbern der Datenträger auch unnütze Dateien gefunden werden, weshalb der Gegenstand genügend genau umschrieben werden sollte, damit die Konnexität mit dem Tatverdacht überprüft werden kann.

II. Durchführung

9 Elektronische Daten sind immaterielle Objekte und untrennbar mit dem Datenträger verknüpft.[16] Nachfolgen soll auf den Verfahrensablauf der Durchführung der Datensuche eingegangen werden, wobei der Schwerpunkt auf AEPLI gesetzt werden soll, der die Sicherstellung von gespeicherten Daten am Beispiel des Kantons Zürich erläutert.

1. Durchsuchung der Datenträger

10 Spezielle Suchprogramme verhelfen Daten aufzuspüren.[17] Dabei ist der Einsatz von Volltext-Suchprogramme oder Detailscanner unzulässig, weil die Untersuchungsbehörde nicht vom Dateiinhalt Kenntnis nehmen darf.[18] Das führt dazu, dass nur nach dem Dateinamen und nicht deren Inhalt durchsucht werden kann. Es besteht die Gefahr, dass damit Beweismittel nicht gefunden werden können, da die Suche zu restriktiv ausgestattet ist. Deshalb soll die Durchsuchung (mit Hilfsmitteln wie den Suchprogrammen) im Lichte der Verhältnismässigkeit ausgelegt werden.[19]

2. Inbetriebnahme der Datenverarbeitungsanlage des Betroffenen

11 Aufgrund des Umstandes, dass Daten schnell manipuliert werden können, muss der Zugriff auf die Datenverarbeitungsanlage rasch erfolgen. Bevor die Untersuchungsbehörde auf den Datenträger mit den gespeicherten Daten zugreifen kann, muss die Datenverarbeitungsanlage in Betrieb genommen werden. Dieser Vorgang ist deshalb zulässig, weil ansonsten auf keine Daten zugegriffen werden könnten. Dabei lehnt ein Teil der Lehre dien Vorgang aufgrund des starken Eingriffs in die Eigentümerverhältnisse ab und dadurch diese in die materielle Enteignung. Ein weiterer streitiger Punkt besteht in der Mitwirkungspflicht. Ein Teil der Lehre stellt die behördliche Anordnung der Pflicht gleich, währen das Schrifttum dies aufgrund mangelhafter gesetzlicher Grundalge ablehnt. Die passive Duldung des Betroffenen ist jedoch erlaubt.[20] Die Durchsuchung dient dazu die Beschlagnahme zu beschränken.[21] Die Zulässigkeit der Durchsuchung endet dort, wo die beweisrelevanten Daten aufgefunden wurden.[22]

---

[15] BGE 108 IV 75 f; BGE 122 II 367 E 2c; BGer vom 2.3. 2010, 1B_354/2009, E 3.2, BGer vom 14.3.2012, 1B_300/2012, E 3.2.
[16] MATZKY, 220.
[17] RYSER DOMINIC, "Computer Forensics", eine neue Herausforderung für das Strafprozessrecht, in: Internet-Recht und Strafrecht, Schwarzenegger/Arter/Jörg (Hrsg.), 2005, 574 f. (zit. RYSER).
[18] Suchprogramme dürfen nur die Existenz von Dateien kennzeichnen, d.h. die Orientierung an Dateien sollen nur anhand von Dateinahmen gestattet sein.
[19] AEPLI, 125; RYSER, 574 f.
[20] Umfassend und übersichtlich AEPLI, 108 f.; MUSKATELZ STEFAN, Der Datenzugriff im Strafverfahren, Juristische Schriftenreiche, Bd. 186, Wien 2000, 84; RYSER, 565 f.
[21] Vgl. BGE 106 IV 423 f.
[22] AEPLI, 126.

3. Zugriff auf Daten über Netzwerke

12 Aufgrund der raschen wachsenden Vernetzung von Datenverarbeitungsanlagen über die lokalen Netzwerke, besteht zunehmend die Möglichkeit, dass auf Daten, welche ausserhalb der aufgefundenen Datenverarbeitungsanlage gespeichert sind, zugegriffen werden kann. Inwiefern das zulässig ist, soll nachstehend beantwortet werden.[23]

13 In der Lehre haben sich zwei Prinzipien herauskristallisiert. Der eine Teil der Lehre befürwortet das Territorialitätsprinzip[24], bei welchem sich die Prozesshandlungen der Untersuchungsbehörde auf das Territorium ihrer Gerichtsbarkeit beschränken müssen. Durch die Durchsuchung von Datenträger, welche im Ausland gespeichert sind, greift die Untersuchungsbehörde in die Souveränität des anderen Staates ein. Diese Daten unterliegen dem Verwertungsverbot.[25] Die Daten können nur noch mit einem Rechtshilfeersuchen (Convention on Cybercrime) an den betreffenden Staat erfolgen.[26]

14 Der andere Teil der Lehre befürwortet das Zugriffsprinzip. Dieser beschreibt, wer von wo aus Zugriff auf die Daten hat. Mittels eines Hausdurchsuchungsbefehls kann die Untersuchungsbehörde die beantragten Räumlichkeiten durchsuchen. Gäbe es diesen Befehl nicht, hätte sie unlimitierten Zugang zu Daten, weshalb dies einem Onlinezugriff[27] gleichkommen würde.

15 Die nationale Gesetzgebung toleriert die direkten Zugriffsmöglichkeiten im Ausland, weshalb diese jederzeit in anderen Ländern abgerufen werden können. Da sich die Daten verstreut auf mehreren Servern befinden, können die Daten einer Durchsuchung leicht entzogen werden. Der Speicherort (Territorium) sollte deshalb nicht das zentrale Kriterium darstellen. Vielmehr sollte das Territorialitätsprinzip auf das Territorium wonach der Datenzugriff erfolgt, abgestellt werden und somit der Eingriff in die Freiheitsrechte des Betroffenen.[28]

---

[23] AEPLI, 127.

[24] Befürwortung des Territorialitätsprinzips ist die traditionelle Lehre wie AEPLI, HEIMGARTNER, RYSER.

[25] BÄR WOLFGANG, Strafprozessuale Fragen der EDV- Beweissicherung, MMR 1, 1998, N 196. (zit. BÄR, Strafprozessuale Fragen, N ...); AEPLI, 130.

[26] Näher dazu HAUSER/SCHWERI/HARTMANN, § 96 N 30.

[27] Der Onlinezugriff erfolgt im Geheimen, weshalb der Betroffene seine Rechte nicht geltend machen kann. Sodann deckt der Onlinezugriff die Umgebung ausserhalb des Hausdurchsuchungsbefehls ab. Da nationale Reglungen keine Lösung bringen, sollten internationale Regelwerke dafür bestehen. Die CCC versucht ein solches Rechtshilfesystem zu etablieren.

[28] BANGERTER SIMON, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht unter vergleichender Berücksichtigung der StPO, Zürich 2014, 282.

D. Beschlagnahme von Daten

16 Unter Beschlagnahme nach Art. 263 ff. StPO ist die Sicherstellung von Gegenständen und Vermögenswerten durch die Wegnahme unter der behördlichen Verfügungsgewalt ohne Einwilligung der betroffenen Person zu verstehen.[29] Dabei betreffen beschlagnahmefähige Objekte nicht nur physische Gegenstände, sondern vielmehr auch elektronische Datenspeicherungen.[30] Doch werden einzelne Daten davon erfasst?

17 So klar die Definition von Daten bei der Durchsuchung ausgefallen ist, so unklar ist die Auslegungsproblematik bei der Beschlagnahme. Die daraus resultierende Frage ist, ob Daten unter die Kategorie der Gegenstände fallen. Dabei wird von der schweizerischen Lehre[31] und Rechtsprechung[32] ausgegangen, dass der Begriff des Gegenstandes nur physische Objekte umfasst und somit die unkörperlichen Daten nicht darunter subsumiert werden können. Demgegenüber plädiert ein Teil der deutschen Lehre – TSCHACKSCH und MATZKY –darauf, dass Beweisgegenstände auch elektrische gespeicherte Daten sein können.

18 Nach den verschiedenen Auslegungsmethoden[33] im Sinne eines Methodenpluralismus kann daraus geschlossen werden, dass Daten Gegenstände sind. Weil jedoch als Beweismittel im Verfahren nur körperliche Objekte (zivilrechtlicher Begriff der Sache i.V.m. Art. 641 ZGB) vorgelegt werden können, werden elektronische gespeicherte Daten nicht unter der Kategorie der Gegenstände nach Art. 263 StPO erfasst. Sie können lediglich mit dem jeweiligen Speichermedium beschlagnahmen werden.[34]

I. Grundsatz

19 Die Voraussetzungen einer Beschlagnahme sind die gleichen wie dieser der Zwangsmassnahme nach Art. 196 f. StPO. Gemäss der StPO wird die Beschlagnahme nach funktionalen Gesichtspunkten in vier Beschlagnahmearten statuiert. Namentlich resultieren daraus die Beweismittel- (lit. a), die Deckungs- (lit. b), die Restitutions- (lit. c), und die Einziehungsbeschlagnahme (lit. d).

20 Nachstehend wird der Schwerpunkt auf die Beweismittelbeschlagnahme gesetzt, da die Untersuchungsbehörde mit der Verfolgung von Wirtschaftskriminalität vermehrt mit Fragen der Beweissicherung konfrontiert wird. Der Zweck der Beweismittelbeschlagnahme liegt in der Beschaffung und der Erhaltung von unverfälschten Beweisgegenständen.[35]

---

[29] SCHMID, StPO Praxiskomm., Art. 263 ff. N 1.

[30] MÜLLER HERMANN/SAX WALTER (Hrsg.), Kommentar zur Strafprozessordnung und zum Gerichtsverfassungs- und Ordnungswidrigkeitengesetz, Bd. 2, 6. Aufl., Darmstadt 1966, KMR-MÜLLER, § 94 N 2; PARK, 215.

[31] HAUSER/SCHWERI/HARTMANN, § 69 N 2; SCHMID NIKLAUS, Strafprozessrecht, Eine Einführung auf der Grundlage des Strafprozessrechtes des Kantons Zürich und des Bundes, 4. Aufl., Zürich/Basel/Genf 2004, N 755. (zit. SCHMID, Strafprozessrecht, N ...).

[32] BGE 126 I 58 f.

[33] Nach der grammatikalischen Auslegung ist der Begriff des Gegenstandes nicht zwingend auf körperliche Objekte beschränkt. Nach der historischen Auslegung gilt der Begriff Gegenstand nur für körperliche Objekte, jedoch hat der historische Gesetzgeber die heutigen technischen Möglichkeiten nicht erahnen können.

[34] AEPLI, 59.

[35] HAUSER/SCHWERI/HARTMANN, § 67 N 2.

II. Durchführung der Beweismittelbeschlagnahme

21 Daten sind keine Gegenstände, sondern nur unkörperliche Objekte. Mittels Datenträger können sie beschlagnahmt werden. Damit eine Beschlagnahme des Gegenstandes jedoch geschehen kann, muss ein entsprechender Deliktsbezug bzw. potenzielle Beweisbedeutung nachgewiesen werden.[36] Diese beschreibt, dass die beschlagnahmten Gegenstände zumindest für die Aufklärung einer vermeintlichen Straftat dienen müssen bzw. Aufschluss über eine strafbare Handlung oder eines Beteiligten geben müssen. Darunter fällt alles mittelbare, wie auch unmittelbare was für die Begehungstat bzw. Person des Täters als Beweis zu erbringen.[37] Die Gewissheit, dass der beschlagnahmte Gegenstand tatsächlich als Beweismittel herangezogen werden kann, ist hierbei nicht erforderlich. Die potenzielle Beweisbedeutung reicht aus.[38]

22 Wie verhält sich die potenzielle Beweisdeutung zur Hardware? Beweisrelevante Daten sind mittels dem jeweiligen Gegenstand inklusive den elektronischen Daten bei der Beschlagnahme erforderlich. Da die körperliche Abspaltung dieser beweisrelevanten Daten nicht möglich ist, kommt dem Datenträger potenzielle Beweisbedeutung zu.

23 Die Datenverarbeitungsanlage wie z.B. eine Festplatte als Workstation[39], die nicht der internen Speicherung von Daten dient, kommt keine potentiellen Beweisbedeutung zu. Folglich darf sie nicht beschlagnahmt werden. Hingegen kommen Datenverarbeitungsanlagen, die auf integriertem Speichermedien beweisrelevanten Daten erhalten, grundsätzliche Beweisbedeutung zu.

24 Weil die Datenverarbeitungsanlage mehrere Speicherchips[40] mit beweisrelevante Daten enthält und diese mit der Hauptplatine fest verlötet ist, ist eine Isolierung der einzelnen Speicherchips mit gewissen Schwierigkeiten verbunden.[41] Eine Datenverarbeitungsanlage kann als Gegenstand deshalb beschlagnahmt werden, wodurch dann Daten ohne Beweisrelevanz mitkonfisziert werden müssen.

Im Rahmen der Durchführung der Beschlagnahme können damit Daten nach dem Grundsatz *a maiore ad minus* mittels Reproduktion sichergestellt werden. Diese können nur benützt werden, wenn ihr potenzielle Beweisbedeutung zukommt. Falls sie diese nicht aufweist, darf die Herstellung einer Reproduktion nicht angewendet werden. Der Betroffene kann aber freilich die Einwilligung geben, da eine Reproduktion ein weniger einschneidendes Ergebnis darstellt, als die Beschlagnahme selbst. Wird jedoch in diese nicht eingewilligt, kann die Untersuchungsbehörde zur Erhebung der Daten eigene Hardware benützen.[42] Besteht der Verdacht, dass Daten gelöscht, versteckt oder verschlüsselt sind, können aufgrund neuer Techniken vermeintlich gelöschte Daten wiederhergestellt werden. Dafür muss sich der Quellendatenträger (meist die Festplatte)

[36] AEPLI, 64.
[37] Prägnant und mit weiteren Verweisen AEPLI, 65; HAUSER/SCHWERI/ HARTMANN, § 69 N 2.
[38] Vgl. Bge 103 IV 119; BGE 199 IV 328; vgl. auch 122 II 371; OBERHOLZER, 359.
[39] Zusammenfassung zur Definition einer Workstation i.V.m. einer Datenverarbeitungsanlage AEPLI, 66.
[40] Einen Überblick über die verschiedenen Speicherchips befindet sich bei MATZKY, 294 ff.
[41] Schwierigkeiten im Sinne von Gefahren, dass im Prozess des Ausbaus von Speicherchips Daten verloren gehen bzw. nicht mehr funktionstüchtig sein können und somit der Auswertung nicht unterliegen können.
[42] AEPLI, 76.

einer Spiegelung[43] unterstellen.[44] Sind die Daten verschlüsselt oder durch ein Passwort geschützt, kann durch Zeugenbefragung des Betroffenen vor Ort ermittelt werden. Werden sie preisgegeben, kann von einer Beschlagnahme grundsätzlich abgesehen werden.[45]

III. Herausgabepflicht – Sicherstellung von elektronischen gespeicherten Daten

25 Die Herausgabepflicht stellt eine öffentlich- rechtliche Pflicht dar, die sich aus dem Aussage- und Zeugnisverweigerungsrecht ableitet. Dadurch erwächst die Pflicht jedes Bürgers, der als Zeuge aussagt, die Beweismittel herauszugeben, die für die Durchführung von Relevanz sein könnten.[46] Gewisse Personen sind jedoch von dieser Pflicht befreit (Art. 264 und Art. 265 Abs. 2 StPO).

26 Die erste Voraussetzung liegt darin, dass der herauszugebende Gegenstand in tatsächlicher Sachherrschaft der betroffenen Person sein muss. Als zweite Voraussetzung muss die Personengruppe der Herausgabepflicht gemäss Art. 265 StPO unterstellt sein. Dabei ist das Aussage- und Zeugnisverweigerungsrecht von grosser Bedeutung.

27 Die Problematik, welche sich im Rahmen der Herausgabepflicht stellt, bildet die Auslegung des Begriffs des Gegenstandes.[47] Das Objekt der Herausgabepflicht beinhaltet nur körperliche bereits existierende Gegenstände. Die tatsächliche Sachherrschaft liegt demnach vor, wer den Gegenstand unter Gewahrsam hat. Ausnahme bildet die Gewahrsams Konstellation im Zusammenhang mit dem Zeugnisverweigerungsrecht. Weil zeugen eine beschränkte Mitwirkungspflicht haben, haben sie auch keine Pflicht zur Herausgabe von Reproduktionen. Eine Vielzahl wird nur bereit sein, weil eine drohende Beschlagnahme bevorsteht. Dieses Ergebnis fällt jedoch unbefriedigend aus. Ist die Herausgabe unverhältnismässig, besteht für die Untersuchungsbehörde nur die Möglichkeit einer Kopie oder einen Ausdruck der Daten im Rahmen der Beschlagnahme sicherzustellen.

E. Fazit

28 Die Untersuchungsbehörde ist bezüglich der Durchsuchung und der Beschlagnahme von Daten mit einigen Problemen konfrontiert, wie die Sicherstellung von elektronischen gespeicherten Daten als Beweismittel bildet die Diskussion über den Begriff des Gegenstandes in Art. 264 StPO. Die rasche Entwicklung zwingt die Untersuchungsbehörde

[43] Die Spiegelung stellt einen speziellen Kopiervorgang dar. Damit gelöschte Daten von EDV-Spezialisten wiederhergestellt werden können, braucht es einen Quelldatenträger oder einen Klon, welcher dann durch eine Spiegelung erstellt wird.

[44] AEPLI, 79.

[45] BÄR WOLFGANG, Der Zugriff auf Computer Daten im Strafverfahren, Europäische Schriftenreiche zum Informationsrecht, Bd. 4, Köln 1992, N 272. (BÄR, Zugriff, N ...); DERSELBE, Strafprozessuale Fragen, N 272.

[46] AEPLI, 8 ff.

[47] Siehe dazu LEICHT ARMIN, Pflicht zur Herausgabe von Datenträgern und Mitwirkungspflichten bei der Aufbereitung von Dateien im Strafverfahren, IuR 1986, 346 ff.; BÄR, Zugriff, N 467.

ihre Vorgehensweise entsprechend anzupassen. Der mangelnde Eintrag in der StPO ist einerseits aufgrund des rasanten technischen Fortschritts richtig, auf der andern Seite gibt es keine wirklichen Anhaltspunkte für den Umgang mit Daten, weshalb viel Raum für Interpretation geduldigt werden muss.