B. Elektronisch gespeicherte Daten bei privaten Trägern von Berufsgeheimnissen

In diesem Kapitel werden die Grundbegriffe für die Beschlagnahme elektronisch gespeicherter Daten bei privaten Trägern von Berufsgeheimnissen beleuchtet, um die einzelnen für die Beschlagnahme potentiell bedeutsamen Beweisgegenstände ermitteln zu können. Daher wird im Abschnitt I. zunächst der Begriff der „elektronisch gespeicherten Daten" dargestellt, wie er in der Informatik und der Strafprozessordnung verstanden wird. Da elektronische Daten aber grundsätzlich auf Speichermedien fixiert werden und diese zumeist Bestandteil einer EDV-Anlage sind, kommen neben den elektronischen Daten für eine Beschlagnahme auch diese Objekte in Betracht. Der Abschnitt II. untersucht deshalb die unterschiedlichen Arten von Speichermedien und EDV-Anlagen und analysiert, welche davon für eine Beschlagnahme bei privaten Trägern von Berufsgeheimnissen potentiell Bedeutung erlangen können. Dabei wird auch auf die Zugriffsmöglichkeiten der Ermittlungsbehörden auf Datenbestände eingegangen, weil dies Auswirkungen auf die Art und Weise der Durchführung einer Beschlagnahme und damit letztlich auf die Rechtmäßigkeit der konkreten strafprozessualen Zwangsmaßnahme haben kann. Im Abschnitt III. erfolgt schließlich die Untersuchung des Begriffs „privater Träger von Berufsgeheimnissen" unter Berücksichtigung von § 53 StPO.

I. Elektronisch gespeicherte Daten

Von grundlegender Bedeutung ist der Begriff der „elektronisch gespeicherten Daten". Was genau die Bedeutung und die Reichweite des Datenbegriffs ist, ist nicht einfach zu bestimmen. Es ist dabei zu berücksichtigen, dass sich bei dieser Thematik Informatik und Rechtswissenschaft überschneiden. Zu prüfen ist daher, inwieweit beide Wissenschaften und insbesondere die StPO von einheitlichen Definitionen ausgehen und ob der Begriff der „Daten" mit dem Begriff der „Information" gleichgesetzt werden kann[19]. Die folgende Untersuchung beschäftigt sich daher mit der Bedeutung des Datenbegriffs in der Informatik (1.) und der Strafprozessordnung (2.).

---

[19] *Matzky*, Zugriff auf EDV, S. 254.

1. Bedeutung in der Informatik

Die Informatik[20] versteht unter Daten die zur Darstellung von Informationen, Sachverhalten u. a. dienenden Zeichenfolgen oder kontinuierliche Funktionen, die Objekte für den Arbeitsprozess einer Datenverarbeitungsanlage sein können[21]. Dem entspricht auch die Definition des Deutschen Instituts für Normung: Nach DIN 44300 Nr. 19 werden Daten in der Informationsverarbeitung als Zeichen oder kontinuierliche Funktionen definiert, die Informationen zur Verarbeitung auf der Basis von bekannten oder unterstellten Vereinbarungen darstellen[22].

a) Logische Betrachtung

Die Darstellung von Informationen erfolgt also mit Hilfe von Zeichen. Je nach dem ob hierfür Ziffern, Buchstaben, eine Kombination aus beiden oder Bildzeichen verwendet werden, spricht man von numerischen, alphabetischen, alphanumerischen oder ikonischen Daten[23]. Sämtliche Darstellungsformen lassen sich auf das Binary Digit (kurz: Bit), der kleinsten Speichereinheit in der Elektronischen Datenverarbeitung (EDV) zurückführen: Der Wert eines Bit kann 1 (wahr) oder 0 (falsch) betragen[24]. Im Unterschied zu analogen Werten, die aus einem beliebigen Intervall der reellen Zahlen bestehen können, ist der Zeichenvorrat bei den digitalen Werten begrenzt. Der Übergang zwischen den einzelnen Werten geschieht deshalb bei den digitalen Werten sprunghaft, während er bei den analogen Werten stufenlos vonstattengeht. Die EDV arbeitet mit Bits und daher ausschließlich mit digitalen Werten[25].

Das Bit stellt die Grundlage für den so genannten Binärcode dar. Dieser erlaubt es, durch eine Aneinanderreihung mehrerer Bits eine Vielzahl von Zuständen wiederzugeben. Jeder Zustand wird durch eine Anzahl von Nullen und Einsen angezeigt. Bei der Verwendung von lediglich drei Bits lassen sich bereits acht verschiedene Zustände beschreiben, angefangen von 000, 001,010,100 ... bis zu 111. Das deutsche Alphabet besteht jedoch aus 26 Buchstaben, die entweder klein oder groß geschrieben werden können. Hinzu kommt eine Vielzahl weiterer Zeichen wie bspw. die Umlaute, Satzzeichen, Klammern, Ziffern, etc. Um alle diese Zeichen darstellen zu können, werden 8 Bits oder ein Byte benötigt[26]. Mathematisch lassen sich damit 2^8, also insgesamt 256, Zustände wiedergeben. Diese angezeigten Zustände sind für den normalen Anwender aber nicht ohne weiteres lesbar

---

20 Der Begriff der Informatik wurde 1957 das erste Mal in Deutschland von Karl Steinbuch verwendet und ist aus den Wörtern Information und Automatik zusammengesetzt, *Balzert*, Grundlagen der Informatik, S. 20.

21 Brockhaus, Band 6, Stichwort „Daten".

22 Computer-Lexikon, Stichwort „Daten", S. 195.

23 Wirtschaftsinformatik-Lexikon, Stichwort „Daten", S. 166.

24 Computer-Lexikon, Stichwort „Bit", S. 116.

25 *Hansen/Neumann*, Wirtschaftsinformatik 1, S. 7.

26 Der Begriff „Byte" wurde von IBM 1956 aus dem englischen Wort „bite" zu deutsch „Happen" kreiert, um eine Verwechslung mit dem Wort „Bit" zu vermeiden, Computer-Lexikon Stichwort „Byte", S. 132.

und deshalb nur von begrenztem Wert[27]. Es bedarf daher einer Zuordnung der einzelnen Bit-Kombinationen zu einzelnen lesbaren Zeichen. Diese Zuordnung bezeichnet man als Code[28]. Am bekanntesten ist der 1968 von Bob Berner eingeführte American Standard Code of Information Interchange (ASCII). Die weiteste Verbreitung dürfte hingegen der von Windows und seinen Anwendungsprogrammen verwendete ANSI-Code erfahren haben[29].

b) Physikalische Betrachtung

Die Informatik behandelt das Datum physikalisch als spezielles Signal, weil die Datenverarbeitung in Computern durch elektrische Signale erfolgt[30]. Ein Signal ist die Darstellung einer Mitteilung durch die zeitliche Veränderung einer physikalischen Größe[31]. Signale müssen demzufolge eine elementar feststellbare Veränderung aufweisen, die sich physikalisch durch Messinstrumente wie bspw. einen Spannungsmesser, lichtempfindliche Zellen oder einem Gerät zur Feststellung von magnetischen Ablenkungen erfassen lässt. Dies ist bei den Bits ohne weiteres möglich, da die 1 und die 0 in der Elektronik durch Spannung vorhanden bzw. keine Spannung vorhanden realisiert werden.

Die Signalübertragung erfolgt durch ein Trägermedium, denn das Signal selbst hat keine körperliche Struktur. Dies wird besonders am Beispiel des Schalls deutlich. Dabei handelt es sich um hervorgerufene Schwingungen von Luftteilchen, die durch Anstoßen weiterer Luftteilchen die Schwingung weiter verbreiten, wobei sich die Stärke der neuen Schwingungen kontinuierlich abschwächt[32]. Wenn die Schallquelle verstummt, dann enden auch die Schwingungen. Bei elektrischen Impulsen geschieht aufgrund der Ladungsweitergabe durch einen elektrischen Leiter im Prinzip dasselbe. Auch hierbei gilt, dass durch das Abschalten der Stromquelle keine weiteren Signale übertragen werden, bzw. ein vorhandenes Signal verstummt. Durch die Ladungsweitergabe wird lediglich ein Datum kreiert, wonach der Stromkreis entweder geschlossen oder offen ist. Dies lässt sich ohne weiteres durch das Dazwischenschalten einer Glühbirne für den Menschen sichtbar machen. Ob dem Umstand, dass der Stromkreis geschlossen ist oder nicht, eine Bedeutung zukommt, ist eine andere Frage, deren Beantwortung sogleich vorgenommen wird. Elektrische Signale sind demnach unkörperlich und benötigen immer einen körperlichen Träger[33].

---

27 Der Binärcode im ASCII-Code: 01001011, 01101111, 01101101, 01101101, 01110011, 01110000, 00100000, 01100100, 01110101, 00111111 bedeutet bspw. im Klartext: „Kommst du?“, *Rechenberg*, Einführung in die Informatik, S. 23.

28 Nicht zu verwechseln mit der Verschlüsselungstechnik (Kryptographie).

29 ANSI steht für American National Standards Institute, eine dem Deutschen Institut für Normung entsprechende US-amerikanische, nichtstaatliche Behörde. Der ANSI-Code baut weitgehend auf dem ASCII-Code auf. Computer-Lexikon, Stichwort „ANSI-Zeichensatz“, S. 59.

30 *Goos*, Grundlagen, S. 1 ff.

31 *Goos*, Grundlagen, a. a. O.

32 *Goos*, Grundlagen, a. a. O.

33 Brockhaus, Band 25, Stichwort „Signal“.

c) Datum und Information

Es stellt sich somit die Frage, welche Bedeutung einem Datum zukommen kann. Die Informatik trennt dazu zwischen den Begriffen der „Information" und des „Datums"[34]. Bauknecht definiert Daten als die Beschreibung von Sachverhalten, wohingegen Informationen Antworten auf Fragestellungen seien.

Daten und Informationen sind daher nicht gleichwertig[35]. Aus Sicht des Anwenders sind Informationen erst das Ergebnis der Arbeit mit Datenbeständen und elektronische Daten somit nur die maschinenlesbare Repräsentation von Informationen. Dies ist vergleichbar mit der Brailleschrift. Ein Braille-Symbol ist zunächst nichts anderes als die Ansammlung von Punkten. Erst durch die richtige Interpretation wird es zu einem Buchstaben. Die Darstellung bzw. Repräsentation ist in der Informatik daher stets ein Phänomen der physikalischen Welt, wohingegen Informationen grundsätzlich abstrakte Ideen sind. Die Brücke zwischen beiden Begriffen schlägt dabei die Interpretation auf der Grundlage eines Bezugssystems[36]. Für die digitale Darstellung von Daten aus Einsen und Nullen bedeutet dies, dass erst bestimmte Abfolgen von geschlossenen und offenen Stromkreisen eine Bedeutung, wie bspw. die von Ziffern oder Buchstaben erlangen. Diese einzelnen Ziffern oder Buchstaben stellen damit die kleinste Form der Information dar.

Dies soll an folgendem Beispiel verdeutlicht werden. Die Kombination 01000001 stellt nach dem ASCII-Code ein „A" dar. Die Tatsache, dass es sich bei dem ausgegebenen Gebilde um ein „A" und damit um einen Buchstaben handelt, ist eine Information, die jedermann aufgrund seiner schulischen Ausbildung bekannt ist. Die dazu erforderliche Anzahl und Anordnung der geschlossenen und offenen Stromkreise sind die der Information „A" zugrunde liegenden binären Daten. Für den Alltagsgebrauch bedarf es selbstverständlich größerer und wesentlich komplexerer Informationsmengen. Dies wird durch weitere Vereinbarungen, wie bspw. der Orthographie erreicht, wodurch die Aneinanderreihung von Buchstaben weitere Bedeutungen erhält. Die Darstellung dieser komplexen Informationen beruht im Bereich der EDV auf dem Muster einer Vielzahl von geschlossenen und offenen Stromkreisen.

Dies entspricht auch der Definition des Deutschen Instituts für Normung, aus der sich für den Datumsbegriff zwei Merkmale ableiten lassen.

aa) Semantik

Als Erstes ist hier das semantische Merkmal zu nennen, das auf ein Kriterium der Information zurückzuführen ist[37]. Die Semantik[38] ist die Disziplinbezeichnung für

---

[34] *Pepper*, Grundlagen der Informatik, S. 19; *Zilahi-Szabó*, Wirtschaftsinformatik, S. 17 ff.; a. A. *Hansen/Neumann*, Wirtschaftsinformatik 1, S. 8: Der eine Abgrenzung zwischen Informationen und Daten für sachlich kaum mehr vornehmbar hält und in Wissenschaft und Praxis immer häufiger von Informationsverarbeitung anstelle von Datenverarbeitung gesprochen werde.

[35] *Bauknecht/Zehnder*, Grundlagen für den Informatikeinsatz, S. 34.

[36] *Pepper*, Grundlagen der Informatik, S. 20; *Goos*, Grundlagen, S. 3.

[37] Kilian/Heussen-*Scheffler* 102 Rn. 12.

alle Untersuchungen bezüglich der Bedeutung sprachlicher Ausdrücke. Daher geht es auf dieser Ebene um die Bedeutung oder genauer um die „innere Seite“ des Datums. Da Daten nur die Repräsentation von Informationen darstellen, stellt sich die Frage, was eigentlich der Inhalt von Informationen sein kann.

Der Informationsgehalt von Daten wird von Welp als die Kenntnisbeziehung zu jedem realen oder irrealen Gegenstand der Welt bezeichnet[39]. Diese Definition erweitert Schmitz, indem er zusätzlich jede beliebige Angabe über Zustände in den Informationsbegriff mit einbezieht[40]. Daraus wird deutlich, dass der Informationsbegriff nicht eingegrenzt werden kann, sondern allumfassend ist. Aus einer solchen Bestimmung des Bedeutungsgehalts von Daten folgt zugleich, dass ein menschlicher Bezug in keiner Weise erforderlich ist. Es kommt somit nicht darauf an, ob die Informationen geheim oder allgemein bekannt, personenbezogen oder anonym sind oder ob sie Gegenstand, Mittel oder Ergebnis einer Datenverarbeitung sind. Deshalb fallen auch die von Maschinen für andere Maschinen oder den eigenen Programmablauf erzeugten Daten unter den Informationsgehalt. Im Ergebnis folgt daraus, dass der Informationsgehalt grundsätzlich kein begrenzendes Kriterium für den Begriff der „elektronischen Daten“ darstellen kann.

bb) Syntax

Das zweite Merkmal stellt die Syntax dar. Darunter ist die Gesamtheit der Regeln für die Bildung erlaubter Wörter und Ausdrücke zu verstehen[41]. Auf die deutsche Sprache bezogen, beinhaltet das bspw. die Regeln über die Groß- und Kleinschreibung, die Interpunktion und die Orthographie. Bezogen auf elektronische Daten bedeutet das die Gesamtheit der für die Bildung von Zeichenfolgen erlaubten Regeln. Die Syntax bezieht sich damit auf die „äußere“ Repräsentation der Information. Denn die nach einer bestimmten Konvention festgelegten Zeichen bestimmen einen Code, der die Informationen darstellt. Dieser Code kann bspw. in einem Morsealphabet, dem normalen Schriftalphabet oder dem oben angesprochenen Binärcode bestehen[42] und stellt damit die Grundlage für verschiedene Programmiersprachen dar.

d) Datenspeicherung

Unter der Speicherung von Daten wird in der Informatik die Übertragung von digitalen Signalen auf Speichermedien einer Rechenanlage verstanden[43]. Dies dient hauptsächlich dem Zweck, die Daten über den Zeitpunkt der Abschaltung der Betriebsspannung hinaus haltbar zu machen, um sie zu einem späteren Zeitpunkt wieder aufrufen zu können[44]. Es kommt daher nicht darauf an, ob die Daten

---

38 Griechisch für „bezeichnen“ vgl. Brockhaus, Band 25, Stichwort „Semantik“.

39 *Welp* iur 1988, 445.

40 *Schmitz* JA 1995, 479.

41 Brockhaus, Band 26, Stichwort „Syntax“.

42 *Schmitz* a. a. O.

43 *Stahlknecht/Hasenkamp*, Wirtschaftsinformatik, S. 55 f.

44 Daneben gibt es allerdings auch so genannte flüchtige Speicher, deren Inhalte bei Abschaltung der Netzspannung verloren gehen, vgl. dazu B II 1 a).

auf dem Speichermedium für die menschlichen Sinne wahrnehmbar sind oder nicht, sondern allein darauf, ob die Speicherung und der erneute Zugriff automatisch durch eine Rechenanlage durchgeführt werden kann[45].

Das Verfahren der physikalischen Datenspeicherung ist dabei von dem jeweilig verwendeten Speichermedium abhängig. Unabhängig von der Art des Mediums werden Daten jedoch, sofern sie über vom Anwender initiierte, einfache Eingaben hinausgehen, üblicherweise in Dateien gespeichert. Diese bilden ein Konglomerat aus Befehlen, Zahlen, Wörtern oder Bildern, die zu einer kohärenten Einheit zusammengefasst werden und von dem Benutzer abgefragt, geändert, gelöscht, ausgedruckt oder gespeichert werden können[46]. Die Dateien ihrerseits werden dabei nicht gleichrangig nebeneinander abgelegt, weil dies zu extrem langen und unübersichtlichen Dateilisten führen würde. Vielmehr erfolgt eine Eingruppierung in einen Katalog für Dateinamen, dem so genannten Verzeichnis oder Ordner. Das Verzeichnis dient der Organisation der einzelnen Dateien[47]. Ausgehend von dem Hauptverzeichnis, dringen die diversen Unterverzeichnisse wie die Wurzeln eines Baumes in viele verschiedene untere Ebenen vor. Üblicherweise hat jedes Speichermedium ein solches Verzeichnis.

Um besonders wichtige Dateien vor ungewollter Veränderung oder Löschung zu bewahren, ist es zudem möglich, diese mit Attributen zu versehen. Dadurch kann z. B. eine Datei nur eingesehen, nicht aber verändert oder gelöscht werden, oder sie wird versteckt und erscheint somit nicht mehr im Verzeichnis, obwohl sie auf dem Speichermedium vorhanden ist. Außerdem können durch entsprechende Verschlüsselungsprogramme Dateien zwar eingesehen werden, doch ergibt ihr Inhalt erst bei Anwendung eines Schlüssels einen für die Rechenanlage und den Benutzer verwertbaren Sinn. Dies ist nur ein kleiner Ausschnitt möglicher Manipulationen des Originaldatenbestandes. Die mögliche Bandbreite von Veränderungen an digitalen Daten bzw. der Datenstruktur ist indessen sehr viel umfangreicher.

e) Zwischenergebnis

Elektronisch gespeicherte Daten sind in der Informatik somit die unkörperliche Repräsentation von Informationen, die von einer Rechenanlage auf der Basis von Mikrochips nur in digitaler Form verarbeitet werden können und auf einem Datenträger (Speichermedium) zur automatischen Wiederverwendbarkeit abgelegt sind.

2. Bedeutung in der StPO

Die Strafprozessordnung selbst enthält für den elektronischen Datenbegriff keine Definition, die auf die Beschlagnahme direkt Anwendung finden könnte. Der Begriff der „Daten“ wird in der StPO aber an mehreren Stellen ausdrücklich ver-

---

45 Deshalb gehören auch Strichcodes und Lochkarten zu den Speichermedien, vgl. *Hansen/Neumann*, Wirtschaftsinformatik 2, S. 103 f.

46 Ms-Computer-Lexikon, Stichwort „Datei“ S. 167.

47 Ms-Computer-Lexikon, Stichwort „Verzeichnis“, S. 720.

wendet. Er findet sich bspw. bei der Rasterfahndung nach §§ 98a, b StPO, dem Datenabgleich zur Aufklärung einer Straftat nach§ 98c StPO und der Schleppnetzfahndung gemäß § 163d StPO sowie in den Dateiregelungen der §§ 483 ff. StPO.

Die Schaffung dieser Tatbestände geht auf das Volkszählungsurteil des Bundesverfassungsgerichts[48] aus dem Jahr 1983 zurück[49]. Durch die genannten Fahndungsmaßnahmen werden in weitem Umfang auch unbescholtene Bürger betroffen, gegenüber denen ein Tatverdacht nicht besteht. Diese Personen werden durch die Maßnahmen, wie das Gericht ausführt, in ihrem aus Art. 2 I i. V. m. Art. 1 I GG folgenden Recht auf informationelle Selbstbestimmung verletzt[50]. Daher bestehe eine verfassungsrechtliche Notwendigkeit zur Schaffung von speziellen Ermächtigungsgrundlagen, die Art und Ausmaß des Eingriffs bestimmen. Vor der Einführung der speziellen Ermächtigungsgrundlagen durch das OrgKG im Jahre 1992[51] wurden die einzelnen Fahndungsmaßnahmen auf die allgemeinen Vorschriften der §§ 161, 163 I StPO gestützt. Die neu eingeführten Tatbestände unterscheiden zwar zwischen personenbezogenen und anderen Daten. Keines dieser Gesetze enthält aber eine ausdrückliche Definition des Datenbegriffs für die StPO.

Auch ein Rückgriff auf das StGB führt nicht weiter. Das Strafgesetzbuch enthält ebenfalls an zahlreichen Stellen Tatbestände mit dem Merkmal „Daten“. Zu nennen sind hier vor allem §§ 202a, 263a, 268, 269, 274, 303a und 303b StGB. Diese Tatbestände enthalten jedoch keine Legaldefinition des elektronischen Datenbegriffs, obwohl einige dieser Tatbestände speziell zum Zwecke der Bekämpfung der Computerkriminalität[52] in das Strafgesetzbuch aufgenommen wurden[53]. Den dagegen gerichteten Bedenken wurde im Gesetzgebungsverfahren vom Bundesministerium der Justiz entgegengehalten, dass man bewusst keine Definition geschaffen habe, weil der Begriff nicht neu sei und bereits im BDSG verwendet werde[54]. Für eine Begriffsbestimmung bestünde daher kein Bedarf[55].

Das BDSG definiert personenbezogene Daten nach § 3 I BDSG als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Wie schon der Wortlaut zeigt, folgt daraus keine allgemein gültige Definition von Daten, denn es werden nur Daten mit Personenbezug genannt[56]. Lässt man den Personenbezug weg, so wären Daten Einzelangaben über persönliche oder sachliche Verhältnisse. Dann müsste aber ermittelt

---

48 BVerfGE 65, 1 ff.

49 Teilweise geändert durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BGBl. I 2007, 3198 ff.

50 BVerfGE 65, 41 ff.

51 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität, BGBl. I 1992, 1302.

52 Computerkriminalität ist ein Sammelbegriff für strafwürdiges Verhalten, das mit Computern in irgendeiner Weise zusammenhängt, *Sieg* Jura 1986, 352.

53 Insbesondere enthält § 202a II StGB keine Definition des Datenbegriffs, sondern setzt diesen voraus, LK-*Schünemann* § 202a Rn. 3.

54 Kilian/Heussen-*Scheffler* 102 Rn. 8.

55 BT-Drucks. 10/5258 S. 29; dagegen Kilian/Heussen-*Scheffler* 102 Rn. 9.

56 *Gola/Schomorus* § 3 Rn. 2 f.; Simitis-*Damann* § 3 Rn. 3 ff.

werden, was eigentlich Einzelangaben sein sollen. Hierbei handelt es sich, wenn man die Intention des BDSG nach § 1 I BDSG zugrunde legt, nicht nur um Daten, sondern ebenso um Informationen, die gegen ungewollte Preisgabe geschützt sein sollen, um eine Beeinträchtigung des Persönlichkeitsrechts zu verhindern. Eine klare Trennung zwischen Informationen und Daten findet somit innerhalb des BDSG nicht statt. Vielmehr werden beide Begriffe synonym gebraucht und unter dem Begriff der Daten zusammengefasst. Wesentliches Merkmal für die Anwendung i. S. d. BDSG ist damit alleine, ob die Daten oder Informationen personenbezogen sind oder nicht. Das BDSG gebraucht den Datenbegriff damit wesentlich extensiver als die Informatik.

Fraglich ist, ob das Verständnis des Datenbegriffs des BDSG auch auf die StPO zutrifft. Zwar deuten die §§ 98a, b, c StPO zunächst auf den digitalen Datenbegriff der Informatik hin, weil sie insoweit von einem maschinellen Abgleich bzw. der Löschung von Datenträgern sprechen, doch geht der in der StPO verwendete Datenbegriff ebenfalls darüber hinaus und erfasst auch nicht maschinell gesammelte Daten, die keiner automatischen Datenverarbeitung zugänglich sind. Dies ergibt sich aus den Regelungen des 2. Abschnitts im 8. Buch der StPO, der die Gesetze über die Dateiregelungen beinhaltet. Die §§ 483 ff. StPO orientieren sich dazu an dem in § 3 II BDSG verwendeten Dateibegriff[57]. Demnach kann eine Datei nicht nur im Rahmen einer automatisierten Verarbeitung unter Einsatz von Datenverarbeitungsanlagen vorkommen, sondern auch dann, wenn keine automatisierte Sammlung von personenbezogenen Daten vorliegt.

3. Ergebnis

Der Begriff der Daten wird im juristischen Sinne wesentlich differenzierter und umfassender gebraucht als in der Informatik. Er ist insoweit keinesfalls nur auf elektronisch gespeicherte Daten begrenzt, wie der Verweis auf seine Verwendung im BDSG gezeigt hat. Im Ergebnis lässt sich damit feststellen, dass der an den technischen Gegebenheiten orientierte engere Begriff der „elektronisch gespeicherten Daten“ in der Informatik von dem weiteren Datenbegriff in der Strafprozessordnung umfasst wird.

II. Potentiell bedeutsame Beweisgegenstände

Nachdem der Begriff der „elektronisch gespeicherten Daten“ untersucht wurde, sollen in diesem Unterabschnitt die potentiell bedeutsamen Beweisgegenstände für eine Beschlagnahme bei privaten Trägern von Berufsgeheimnissen erörtert werden. Beweisbedeutung erlangt dazu jeder Gegenstand, der geeignet ist, die Aufklärung oder Ahndung einer Straftat zu fördern[58]. Wie die Untersuchung unter I. gezeigt hat, erfordern elektronisch gespeicherte Daten eine Verarbeitung durch

[57] *Meyer-Goßner* § 483 Rn. 1.
[58] LR-*Schäfer* § 94 Rn. 23.

eine EDV-Anlage auf der Basis von Mikrochips und eine Speicherung auf einem Datenträger. Daher kommen diesbezüglich als Gegenstände mit potentieller Beweisbedeutung die Speichermedien (1.), die diese verwendenden EDV-Anlagen (2.) und der Datenbestand an sich in Betracht (3.). Auf diese Gegenstände ist im Folgenden näher einzugehen, weil die genaue Bestimmung des Beschlagnahmegegenstandes für die weitere Untersuchung entscheidend für die Frage sein wird, ob eine Beschlagnahme rechtmäßig ist oder bspw. gegen das Übermaßverbot verstößt.

1. Speichermedien

Um eine Beschlagnahme von elektronisch gespeicherten Daten durchführen zu können, müssen bereits die Ermittlungsbehörden genau wissen, an welchen Orten sie danach suchen müssen und welche Gegenstände sie beschlagnahmen sollen. Für die potentielle Beweisbedeutung genügt insoweit, dass die Möglichkeit besteht, dass ein Gegenstand zu Untersuchungszwecken verwendet werden kann[59]. Die Beschlagnahme der gesamten zur Auffindung von Beweismitteln zu durchsuchenden Räumlichkeit durch Anlegung eines Siegels dürfte jedoch in aller Regel überzogen und deshalb unverhältnismäßig sein. Schon die richterliche Ausstellung eines Durchsuchungs- und Beschlagnahmebeschlusses erfordert eine genaue Bezeichnung der zu durchsuchenden Örtlichkeit und der zu beschlagnahmenden Gegenstände[60].

Es stellt sich damit die Frage, auf welchen Datenträgern elektronisch gespeicherte Daten eigentlich fixiert werden. Ein Datenträger ist ein zur dauerhaften Aufnahme von Daten geeignetes physikalisches Medium[61]. Grundsätzlich kann die Datenspeicherung elektronisch (a), magnetisch (b), optisch (c) oder aus einer Kombination dieser Arten (d) erfolgen. Deshalb werden im Folgenden die wichtigsten Speicherarten und Speichermedien kurz nach Aussehen, Bedeutung und Funktionsweise dargestellt, soweit sie für die Beschlagnahme von elektronisch gespeicherten Daten bei privaten Trägern von Berufsgeheimnissen relevant sein können. Dabei kann es sich hierbei nur um einen groben Überblick handeln, da ein genaues Eingehen auf die unterschiedlichen Speichermedien und Speichermethoden den Rahmen dieser Arbeit bei Weitem sprengen würde[62].

a) Elektronische Datenspeicherung

Die elektronische Datenspeicherung umfasst sämtliche Speichermedien, die Informationen in oder auf Basis von elektronischen Bauelementen speichern. Die elektronischen Datenträger verwenden hierzu Halbleiterbauelemente, die zumeist aus Silizium bestehen[63]. Die einzelnen Speichermethoden können hierbei nach der

---

59 *Meyer-Goßner* § 94 Rn. 6.
60 *Meyer-Goßner* § 105 Rn. 5.
61 *Hansen/Neumann*, Informationstechnik, S. 95.
62 Vgl. aber die ausführliche Darstellung bei *Matzy*, Zugriff auf EDV, S. 275 ff.
63 *Hansen/Neumann*, Informationstechnik, S. 165.

Charakteristik der Datenhaltung in flüchtige, permanente und semi-permanente Speichermedien unterschieden werden.

aa) Flüchtige elektronische Speichermedien

Die flüchtigen Speichermedien sind dadurch gekennzeichnet, dass ihre Inhalte mit Abschaltung des Stroms verloren gehen. Zu diesen Speichern zählen vor allem das Random Access Memory (RAM)[64], das SRAM[65] und das DRAM[66]. Dabei handelt es sich um eine Anzahl von Mikrochips, die auf einer kleinen Platine befestigt sind.

Sie werden in der Regel als Arbeitsspeicher für EDV-Anlagen verwendet; kommen aber auch als Bild- und Texturspeicher bei Grafikkarten zum Einsatz. Flüchtige Speicher können jedoch nur in Ausnahmefällen für die Beschlagnahme relevant werden, wenn der Beschuldigte bspw. auf frischer Tat betroffen wird, etwa wenn er sich gerade Bilder ansieht, die sexuelle Übergriffe auf Kinder darstellen. Dann müssen die Ermittlungsbehörden den Inhalt des flüchtigen Speichers auf ein anderes Speichermedium zur dauerhaften Archivierung übertragen[67].

bb) Permanente elektronische Speichermedien

Permanente elektronische Speicher zeichnen sich dadurch aus, dass sich in ihnen eine einmal gespeicherte oder festverdrahtete Information befindet, die nicht mehr verändert werden kann. Im Gegensatz zu den flüchtigen Speichern bleibt ihr Inhalt damit auch nach Abschalten der Betriebsspannung unbegrenzt erhalten[68]. Ihr Einsatzgebiet liegt hauptsächlich bei denjenigen Mikrochips, die für den Systemstart der EDV-Anlage verwendet werden, weil zu diesem Zeitpunkt ein Zugriff auf externe permanente Speicher noch nicht möglich ist. Für die weitere Untersuchung können diese Speichermedien außer Betracht bleiben, denn der Inhalt elektronischer, permanenter Speicher ist von dem Hersteller der entsprechenden Mikrochips fest vorgegeben und durch einen Berufsgeheimnisträger nicht beeinflussbar. Daher kann ein permanenter Speicher auch keine Geheimnisse eines privaten Trägers von Berufsgeheimnissen enthalten.

---

64 Zu deutsch bedeutet Random Access Memory: Speicher mit wahlfreiem Zugriff. Ein wahlfreier Zugriff liegt im Unterschied zum sequentiellen Zugriff dann vor, wenn jede Speicherzelle über ihre Speicheradresse direkt angesprochen und so direkt auf ihren Inhalt zugegriffen werden kann, ohne dass der Inhalt zuvor in Blöcken gelesen werden müsste. Ein typisches Beispiel für die Unterscheidung zwischen sequentiellem und wahlfreiem Zugriff bildet das antike Auf- oder Abrollen eines Pergaments (sequentiell) und das Buch (wahlfrei), bei dem jede beliebige Seite sofort aufgeschlagen werden kann, Ms-Computer-Lexikon, Stichwort „RAM“.

65 SRAM bedeutet Static Random Access Memory, zu deutsch: Statischer Speicher mit wahlfreiem Zugriff, Ms-Computer-Lexikon, Stichwort „statisches RAM“.

66 DRAM steht für Dynamic RAM oder dynamischer Speicher mit wahlfreiem Zugriff, Ms-Computer-Lexikon Stichwort „dynamisches RAM“.

67 Bär schlägt hierfür die Anfertigung einer Fotografie vor, *Bär*, Zugriff auf Computerdaten, S. 249.

68 *Matzky*, Zugriff auf EDV, S. 295.

cc) Semi-permanente elektronische Speichermedien

Die letzte und bei weitem wichtigste Gruppe für die Beschlagnahme von auf elektronischen Speichermedien befindlichen Daten bilden die semi-permanenten elektronischen Speicher. Sie speichern Informationen permanent, d.h. dass ihr Inhalt auch nach Abschalten der Betriebsspannung erhalten bleibt. Im Unterschied zu den nur permanenten Speichern können die gespeicherten Informationen aber je nach Bedarf auch verändert werden[69]. Bedeutung hat insoweit das Electrically Erasable Programmable Read Only Memory (EEPROM) erlangt[70].

Auf Grundlage dieser Technik haben sich vielfältige Anwendungsmöglichkeiten für den Einsatz von EEPROM ergeben. Zu nennen sind hier zunächst die Flash-Speicherkarten. Diese kleinen, externen Speichermedien werden in tragbaren Geräten wie z. B. Digitalkameras, Musikabspielgeräten, Mobilfunktelefonen und PDAs eingesetzt[71]. Die Lebensdauer dieser Speicherchips liegt bei ca. 100.000 Schreib- und Löschzyklen[72] und ihre Speicherkapazität beträgt derzeit zwischen 16 Megabyte und 32 Gigabyte[73]. Flash-Kartenspeicher haben keinen einheitlichen Standard. Es gibt sie deshalb in unterschiedlichen Größen, Formen und mit verschiedenen Schnittstellen, die untereinander meist inkompatibel sind. Um ihre Inhalte lesen bzw. beschreiben zu können, bedarf es daher eines speziellen Lese- und Schreibgeräts, in das die Flash-Speicherkarte eingelegt werden muss. Die Vorteile der Flash-Speicherkarte liegen im Verhältnis zu anderen Speichermedien in ihrer Winzigkeit, ihrem leichten Gewicht, ihrer einfachen Transportmöglichkeit, in ihrer völlig geräuschlosen Arbeitsweise bei gleichzeitig geringer Zugriffszeit und ihrer relativen Unempfindlichkeit gegenüber Umwelteinflüssen[74].

Eine besondere Ausprägung der Flash-Speicherkarten bildet der USB-Stick[75]. Er vereint die Vorteile einer Flash-Speicherkarte mit der Standard-Schnittstelle USB[76]. Im Gegensatz zu anderen Flash-Speicherkarten benötigt der USB-Stick keine zusätzlichen Geräte oder Adapter, um gelesen oder beschrieben zu werden, sondern ist mit dem Aufstecken auf die USB Schnittstelle sofort einsatzbereit.

---

69 *Matzky*, Zugriff auf EDV, S. 296 f.

70 Das EEPROM kann zwischen 1.000 – 100.000 mal elektrisch gelöscht und beschrieben werden. Es besteht dazu aus einer Feldeffekt-Transistorenmatrix, in der jeder Transistor ein Bit repräsentiert. Der Transistor kann dabei zwei Zustände annehmen. Er kann den Strom über das sog. Gate durchlassen oder ihn sperren. Die Sperrung erfolgt durch eine elektrische Ladung auf dem Gate. Die Daten werden dabei durch ein Bitmuster dargestellt, das sich daran orientiert, ob ein Transistor geladen oder ungeladen ist bzw. ob der Strom durchgelassen oder gesperrt wird.

71 *Hansen/Neumann*, Informationstechnik, S. 180.

72 *Hansen/Neumann*, Informationstechnik, S. 181.

73 Vgl. z. B. den Flash-Speicher von Samsung, der 32 GB Speicherkapazität aufweist, Spiegel-Online Artikel vom 21. März 2006.

74 *Hansen/Neumann*, Informationstechnik, S. 185.

75 Auch USB Memory Stick oder USB Flash Sticks genannt.

76 USB bedeutet Universal Seriell Bus und ist ein Verbindungssystem zwischen dem Computer und Zusatzsystemen. USB ermöglicht einen Gerätewechsel auch bei eingeschalteter Stromversorgung, Ms-Computer-Lexikon, Stichwort „USB“, S. 704.

Ein weiterer Anwendungsbereich von EEPROM-Speichern liegt in der Verwendung als Datenspeicher für Mikrochipkarten. Die Mikrochipkarte ist eine Plastikkarte mit einem integrierten Chip, der einen Mikroprozessor und einen Speicher enthält. Es gibt drei verschiedene Kartengrößen, die durch ISO 7816 normiert sind. Zum einen gibt es ein größeres Format (85,60 mm × 53,98 mm) für Ausweise, Kunden-, Bank-, Kredit- und viele andere Karten[77] und zum anderen ein kleineres Format (25mm × 15mm) für den Einsatz als SIM-Karte in Mobiltelefonen. Das mittlere Format (66mm × 33mm) hat bisher kaum Anwendung gefunden. Die Höhe aller drei Karten liegt bei exakt 0,76 mm. Neben den Maßen ist auch die Schnittstelle dieser Karten nach ISO 7816-2 genormt. Der Mikrochip ermöglicht die Geheimhaltung der auf der Karte befindlichen Daten durch die Eingabe eines Zugangscodes (PIN)[78] und einen weitgehenden Schutz vor fälschlichem oder unerlaubtem Überschreiben oder Löschen von Daten. Hinzu kommt, dass die Daten durch den Mikrochip verschlüsselt auf der Karte gespeichert werden können.

Die Verschlüsselung ist vor allem für die Verwendung von Subscriber Identity Module (SIM) Karten wichtig[79]. Das SIM ordnet die verschiedenen mobilen Telekommunikationseinrichtungen einem Nutzer zu und authentifiziert ihn. Dazu sind auf der SIM-Karte geheime Nummern und Algorithmen gespeichert. Diese dienen u. a. der Verschlüsselung der Sprach- und Signalisierungsdaten. Auf der SIM-Karte sind zudem ein RAM- und ein EEPROM-Speicher vorhanden, die zum Speichern von temporären, netzbezogenen Daten und bevorzugten und gesperrten Netzen benutzt werden. Darüber hinaus können durch das EEPROM ein Telefon- und Notizbuch und Kurzmitteilungen (SMS[80], MMS[81]) sowie die Telefonnummer der zuletzt ausgegangenen oder eingegangenen Anrufe dauerhaft gespeichert werden.

b) Magnetische Datenspeicherung

Die wohl derzeit noch am weitesten verbreitete Methode zur Datenarchivierung ist die magnetische Datenspeicherung. Dabei erfolgt die Speicherung durch einen oder mehrere Schreib- und Leseköpfe auf magnetisierbarem Material. Dieses kann als hauchdünne Schicht auf Plastikbändern, Karten, Papier oder Platten aufgebracht sein. Zu den magnetischen Speichermedien zählen vor allem die Diskette, das Magnetband und die Magnetplatten.

---

77 *Hansen/Neumann*, Informationstechnik, S. 165; zur missbräuchlichen Nutzung von solchen Karten siehe *Schnabel* NStZ 2005, 18 ff.

78 PIN = Personal Identification Number, eine eindeutige Codenummer, die einem berechtigten Benutzer zugewiesen ist, Ms-Computer-Lexikon, Stichwort „PIN".

79 Ms-Computer-Lexikon, Stichwort „SIM-Karte".

80 SMS steht für Short Message Service, Ms-Computer-Lexikon, Stichwort „SMS".

81 MMS steht für Multimedia Messaging Service. Eine Weiterentwicklung der SMS, Ms-Computer-Lexikon, Stichwort „MMS".

aa) Diskette

Eine Diskette ist ein Wechseldatenträger, der aus einer flexiblen, runden Kunststoffplatte besteht, die auf beiden Seiten mit einer magnetisierbaren Schicht (meist aus Eisenoxid) bedeckt ist[82]. Zum Schutz dieser Scheibe ist sie von einem Kunststoffgehäuse umgeben, das je nach Diskettenart biegsam oder starr sein kann. Die ersten Disketten kamen Mitte der 1970er Jahre auf den Markt und hatten eine Größe von 8 Zoll. Über 20 Jahre lang waren Disketten die am häufigsten verwendeten Datenträger, was nicht zuletzt an technischen Verbesserungen lag. So wurden die Disketten im Laufe der Zeit immer kleiner (5 ¼, 3 ½ und 2 Zoll) bei einer gleichzeitigen Erhöhung ihrer Speicherkapazität von anfangs 100 KB auf bis zu 2,8 MB[83]. In den letzten Jahren hat die Diskette aber viel von ihrer ursprünglichen Bedeutung verloren, weil ihre Vorteile wie bspw. die einfache Handhabung, Versendbarkeit, Wiederverwendbarkeit und Austauschbarkeit mit anderen Computern auch bei anderen Datenträgern wie bspw. den USB-Sticks vorhanden sind, die im Vergleich zu einer Diskette aber eine erheblich höhere Speicherkapazität aufweisen.

bb) Magnetband

Ein Magnetband ist ein dünnes Polyesterband, bei dem auf einer Seite eine magnetisierbare Schicht (meist Eisenoxyd)[84] aufgetragen ist, auf der die Daten durch Magnetisierung aufgezeichnet werden[85]. Zum Schutz vor Staub- und Fingerabdrücken steckt es meist in einer Datenkassette und erinnert in seinem Aufbau stark an eine übergroße Tonbandkassette.

Magnetbandeinheiten werden bei Großrechnern und bei Arbeitsplatzrechnern und lokalen Netzwerken verwendet. Sie dienen vorwiegend zur Sicherung und Ablage von Daten in größeren Mengen, weil sie trotz ihrer Empfindlichkeit gegen Staub, Feuchtigkeit, Wärme und magnetischen Umwelteinflüssen – bei sorgsamem Umgang – mit ca. 30 Jahren eine recht lange Haltbarkeit haben. Ein einzelnes 3592-Magnetband für einen Großrechner kann bis zu 300 Gigabyte an Daten speichern. Üblicherweise verwendet ein Großrechner eine Bibliothek, d. h. mehrere Laufwerke mit einer großen Anzahl von Fächern, in denen die Magnetbänder aufbewahrt werden. Dadurch lassen sich Kapazitäten von über 100 Terabyte erreichen. Die für den Arbeitsplatzrechner und kleinere lokale Netzwerke bestimmten Magnetbandeinheiten werden Streamer genannt, weil sie ausschließlich im Datenstrombetrieb arbeiten[86].

---

82 *Hansen/Neumann*, Informationstechnik, S. 118.

83 Computer Lexikon, Stichwort „Diskette“, S. 234.

84 *Zilahi-Szabó*, Lehrbuch Wirtschaftsinformatik, S. 43.

85 *Hansen/Neumann*, Informationstechnik, S. 113.

86 Auch Streamer werden vorwiegend zur Datenarchivierung eingesetzt. Ihre Zugriffszeiten sind aber wegen der sequentiellen Speicherung der Daten entsprechend lang, Computer Lexikon, Stichwort „Streamer“, S. 771.

cc) Magnetplatte

Die Magnetplattenspeicher sind die derzeit noch am häufigsten eingesetzten Speichermedien. Ein Magnetplattenspeicher ist ein Datenträger in Form einer oder mehrerer auf einer Achse übereinandergestapelter runder Platten[87]. Die einzelnen Platten bestehen aus einem Aluminium/Magnesium- oder Glassubstrat mit einer in der Regel auf beiden Seiten aufgebrachten magnetischen Beschichtung.

Magnetplatten gibt es in verschiedenen Größen, wobei der Trend hin zu immer kleineren und leistungsfähigeren Geräten geht. Während früher der Standard bei bis zu 14 Zoll und nur wenigen Megabyte pro Laufwerk lag, liegt er heute bei 3 ½ bis zu unter einem Zoll und einer Kapazität von mehreren Gigabyte. Es gibt Magnetplattenspeicher als fest eingebautes- (Festplatte), auswechselbares (Wechselplatte) oder externes Laufwerk mit einem oder mehreren verschiebbaren Leseköpfen und mit unterschiedlichen Aufzeichnungstechniken und -formaten[88].

c) Optische Datenspeicherung

Die optische Speicherung arbeitet mit Reflexions-, Filter- und Beugungseigenschaften von verschiedenen Materialien[89]. Es werden bspw. beim Film und in der Photographie farbfilternde Eigenschaften, bei CDs die Lichtreflexion und bei Hologrammen die lichtbeugenden Eigenschaften ausgenutzt. Zu den optischen Speichern zählen neben Lochkarten u. a. der Barcode, die Compact Disk (CD), die Digital Versatile Disk (DVD) und der Mikrofilm.

aa) CD

Das bekannteste optische Speichermedium ist die Compact Disk (CD)[90] in Form der Compact Disk – Read Only Memory (CD-ROM). Die CD-ROM ist eine optische Speicherplatte mit einer Speicherkapazität von 650-900 MB, wobei Speichermedien über 700 MB nicht von allen handelsüblichen Laufwerken gelesen werden können. Die metallisch glänzende Scheibe hat entsprechend ihrer Standardisierung nach dem „Red Book“ einen Durchmesser von 12 cm oder 8 cm und ist 1,2 mm dick[91]. Sie besteht aus einer durchsichtigen Polycarbonat-Platte und einer darauf befindlichen hauchdünnen Metallschicht. Die CD-ROM entspricht damit im Aufbau der Audio CD. Die Informationen werden durch mikroskopisch kleine Vertiefungen in der Metallschicht, den sog. „pits“, und den dazwischenliegenden Erhöhungen, den sog. „lands“, repräsentiert. Von den Vertiefungen fasst eine CD ca. 2 Milliarden Stück, die im Gegensatz zur Diskette nicht konzentrisch, sondern spiralförmig auf einer Spur angeordnet sind. Auf einem Inch liegen dabei 16.000 dieser Spuren nebeneinander. Das Lesen erfolgt durch einen Laser, der die Spur abtastet. Trifft er dabei auf ein „land“, so wird er reflektiert; trifft er dagegen auf

---

87 *Hansen/Neumann*, Informationstechnik S. 123.

88 *Hansen/Neumann*, Informationstechnik, S. 125.

89 *Hansen/Neumann*, Wirtschaftsinformatik 2, S. 141 ff.

90 Die CD wurde 1982 von Phillips und Sony zum Zwecke der digitalen Audiospeicherung eingeführt und sollte ursprünglich nur die Schallplatte ablösen, Brockhaus, Band 5, Stichwort „CD“.

91 *Hansen/Neumann*, Informationstechnik, S. 146.

eine Vertiefung, so wird er weitergeleitet. Die Reflektionsunterschiede werden von einer Photodiode aufgefangen und in elektrische Impulse umgewandelt. CDs eignen sich hervorragend zur Datensicherung und den Transport von mittelgroßen Datenbeständen. Neben der einfachen CD-ROM gibt es auch einmal und mehrmals wiederbeschreibbare CDs.

bb) DVD

Eine Weiterentwicklung der CD stellt die 1995 standardisierte Digital Versatile Disk (DVD) dar. Sie hat dieselben Maße wie eine CD, weist aber eine erheblich höhere Spur- und Pitdichte auf. Daher kann sie auf einer Seite bereits bis zu 4,7 Gigabyte speichern[92]. Durch den Einsatz einer zweiten Speicherschicht, die über einen variabel fokussierbaren Laser abgetastet werden kann, kann auf einer Seite bis zu 8,5 GB gespeichert werden. Im Unterschied zu CDs kann die DVD auch doppelseitig beschrieben werden. Damit ergibt sich eine maximale Speicherkapazität von 17,1 GB. DVDs können ähnlich wie CDs nur lesbar (DVD-ROM), beschreibbar (DVD-R) oder wiederbeschreibbar (DVD-RW, DVD+RW, DVD-RAM) sein. Die dazu eingesetzten Verfahren verwenden die Eigenschaften organischer Farbstoffe und die duale Phasentechnik[93].

cc) Blu Ray Disc und andere

Die Palette weiterer technischer Entwicklungen ist sehr weit reichend, und es kommen ständig neue Speichermedien hinzu. So stehen als Nachfolger der DVD die Professional Disc for Data (PDD), die Ultra Density Optical (UDO), die High Definition Digital Versatile Disc (HD-DVD), die Blu Ray Disc[94] und holographische Speicher im Gespräch[95]. Mit Ausnahme der noch in der Entwicklung befindlichen holographischen Speicher, für die ein Standard noch nicht festgelegt wurde, werden dabei stets runde Platten von 12 cm Durchmesser und 1,2 mm Dicke verwendet. Kennzeichnend für die weitere Entwicklung ist die immer höher werdende Speicherkapazität.

dd) Optische Speicherkarten

Optische Speicherkarten weisen dieselben äußeren Merkmale auf wie die Magnet- oder Mikrochipkarte. Sie sind 85,6 × 54,0 × 0,76 mm groß und entsprechen damit der herkömmlichen Scheck- oder Kreditkarte. Zur Datenspeicherung dient hier ein

---

92 Der Standard der DVD wurde 1995 durch ein Herstellerkonsortium festgelegt.

93 *Hansen/Neumann*, Informationstechnik, S. 146.

94 Die Blu Ray Disc arbeitet mit einem blauen Laser, der im Gegensatz zum sonst gebräuchlichen roten Laser eine geringere Wellenlänge aufweist. Dadurch kann die Spur- und Pitdichte enorm verkleinert werden. Bei einer einschichtigen Aufzeichnung erreicht die Blu Ray Disc eine Speicherkapazität von 27 GB, bei zweischichtiger Aufzeichnung sogar 54 GB. Die Zukunft wird aber den holographischen Speichern gehören. Ihre Technik soll es ermöglichen, bis zum Jahr 2010 ca. 1,6 Terabyte auf einem Datenträger speichern zu können, *Hansen/Neumann*, Informationstechnik, S. 209 ff.

95 Der Kampf der Formate dürfte allerdings zu Gunsten von Blu Ray (Sony) entschieden sein, nachdem vier der sechs größten Hollywoodstudios ihre Filme zukünftig nur noch auf Blu Ray Disc verkaufen wollen, Spiegel-Online Artikel vom 08. Januar 2008.

optischer Speicherstreifen, der mittels Laser beschrieben und gelesen werden kann. Die Kapazität liegt mit ca. 4 MB deutlich höher als bei der Magnet- oder Mikrochipkarte[96]. Eine Einsatzmöglichkeit könnte sich vor allem als Lebenskarte ergeben; einer Karte also, die sämtliche im Leben eines Individuums relevanten Daten auf einem Datenträger zusammenfasst wie bspw. die Krankenakte, biometrische Daten, finanzielle Transaktionen usw. Der Einsatz optischer Speicherkarten ist in Deutschland aber noch sehr selten.

d) Kombination verschiedener Arten der Datenspeicherung

Zum Teil werden die verschiedenen Arten der Datenspeicherung auch miteinander verbunden, um so neue und effizientere Speichermedien herzustellen. Dies ist vor allem bei der magneto-optischen Methode der Fall, welche die Vorzüge dieser beiden Speicherungsarten miteinander verbindet[97]. Dabei macht man sich den so genannten Kerr-Effekt zunutze[98]. Ein Speichermedium, das diese Methode verwendet, ist die Magneto-Optical Disc (MO-Disc)[99], die in den Formaten 3,5 und 5,25 Zoll mit einer Speicherkapazität von 128 MB bis 9,1 GB pro Platte auf dem Markt erhältlich ist[100]. Der Vorteil der magnetischen Speicherung liegt in der hohen Anzahl der Schreib- und Löschvorgänge, die bei der MO-Disc bei über einer Million liegt. Die optische Komponente ermöglicht hierbei das Schreiben und Lesen auf kleinstem Raum, was zu der hohen Speicherkapazität führt. MO-Discs eignen sich damit hervorragend zur Archivierung, zum Austausch und zur Speicherung von großen Datenbeständen.

2. EDV-Anlagen

Die eben genannten Speichermedien kommen bei verschiedenen Geräten, die mit elektronischen Daten arbeiten, zum Einsatz. Eine EDV-Anlage stellt deshalb nicht nur der Personalcomputer dar, sondern ist der Oberbegriff für alle elektrischen Maschinen, die Daten auf Grundlage von elektrischen Impulsen erfassen und

---

96 *Hansen/Neumann*, Informationstechnik, S. 141.

97 Kombinationen gibt es auch im elektronisch-optischen Bereich etwa bei Plastikkarten, die optische Daten und einen Mikrochip enthalten. Die Verbreitung dieser Karten kommt aber praktisch kaum vor, so dass sie für die weitere Untersuchung außer Betracht bleiben können.

98 Dieser besagt, dass bestimmte Substanzen unter dem Einfluss großer Hitze und starker Magnetfelder ihre Polarisationsrichtung ändern. Das Beschreiben eines Datenträgers erfolgt durch die Erzeugung eines Magnetfeldes und der Erhitzung bestimmter Bereiche des Datenträgers durch einen Laserstrahl. Diese Bereiche ändern ihre magnetische Ausrichtung dann entsprechend der Polarisation des vorgegebenen Magnetfeldes. Das Lesen erfolgt unter Verwendung eines schwächeren Laserstrahls, der aufgrund der Magnetisierung unterschiedlich reflektiert wird. Diese Unterschiede werden als 0 und 1 interpretiert und in die entsprechenden elektronischen Signale umgewandelt.

99 Auf dieser Basis arbeitet auch die MiniDisc, *Hansen/Neumann*, Informationstechnik, S. 164.

100 *Hansen/Neumann*, Informationstechnik, S. 163.

bearbeiten. Neben den Computeranlagen[101] im eigentlichen Sinn, die von einem einfachen Personalcomputer (PC) von der Größe eines Notebooks bis hin zu einem Großrechner reichen, der mehrere Stockwerke hoch und etliche Tonnen schwer sein kann, erfasst dieser Begriff deshalb auch andere Anlagen bzw. Geräte. Zu nennen wäre hier bspw. das Mobiltelefon und der Personal Digital Assistent (PDA) sowie der Videorekorder, Geräte für den Empfang von digitalem Fernsehen oder Radio und viele mehr. Interessant im Zusammenhang mit der Beschlagnahme elektronisch gespeicherter Daten bei privaten Trägern von Berufsgeheimnissen sind aber nur die Geräte, auf denen elektronische Daten typischerweise abgelegt und verändert werden können. Das sind neben dem PC im wesentlichen PDAs und Mobiltelefone[102].

Gerade Letztere haben eine weitgehende Verbreitung erfahren. Gab es vor 20 Jahren gerade mal ein paar wenige Technikbegeisterte, die sich ein solches Mobiltelefon von der Größe eines Aktenkoffers leisten konnten, so sind es heute statistisch gesehen ca. 100% der deutschen Bevölkerung[103]. Die Gründe hierfür liegen bei den relativ günstigen Preisen für die kleinen, hochwertigen Geräte und den mittlerweile moderaten Tarifen für das Telefonieren. Außerdem ist das Handy längst zu einem Statussymbol für die breite Masse avanciert, das neben dem einfachen Telefonieren auch über Organizerfunktionen, Internetzugang, Digitalkamera und MP3-Player[104] verfügen kann. Mobiltelefone werden aber nicht nur für den privaten Gebrauch, sondern vor allem auch für geschäftliche Zwecke eingesetzt. Es ist mit den neueren Mobiltelefonen bspw. möglich, Präsentationen zu entwerfen, zu speichern und zu halten, sowie Daten von Kunden oder Geschäftspartnern zu erhalten, die später auf einen PC übertragen werden können.

Diese Aufgaben können auch von PDAs erledigt werden. Sie sind mit Mobiltelefonen eng verwandt und bilden quasi das Bindeglied zwischen einem Personalcomputer und einem Mobiltelefon. Sie sind dementsprechend etwas größer als Mobiltelefone, passen aber immer noch bequem in eine Manteltasche und weisen dafür gegenüber dem Handy ein größeres Display auf. Die Funktionen ähneln dem eines Notebooks. Es können also Informationen eingegeben, verändert, gespeichert und gelöscht werden. Die Einsatzmöglichkeiten reichen vom Schreiben eines Briefes über Tabellenkalkulationen und die Erstellung von Präsentationen bis hin

---

[101] Vgl. zu den einzelnen Bestandteilen (Hardware) einer Computeranlage, *Wolf* JuS-Beilage 1997, B 4.

[102] Dies bedeutet aber nicht, dass im Einzelfall nicht auch andere EDV-Anlagen, wie ein Tonband oder eine Videokassette potentielle Beweisbedeutung erlangen könnten.

[103] Dabei muss berücksichtigt werden, dass die Grundlage für diesen Wert die Anzahl der Mobilfunkanschlüsse gemessen an der Gesamtbevölkerungszahl bildet. Unberücksichtigt bleiben daher Mehrfachanschlüsse einer einzelnen Person, „Monitoring Informationswirtschaft – 10. Faktenbericht 2007“, S. 123 ff.

[104] MP3-Player sind Geräte zum Abspielen von Audiodateien, die nach dem Komprimierungsalgorithmus „MPEG Audio Layer-3“ komprimiert wurden. Diese Dateien sind gegenüber herkömmlichen Audiodateien sehr klein, weil sie auf das Abspielen von Tönen, die das menschliche Gehör nicht wahrnehmen kann, verzichten, Ms Computer-Lexikon, Stichwort „MP3“, S. 462.

zum Telefonieren und Internetzugang. PDAs haben in der Regel eine weitaus größere Speicherkapazität als Mobiltelefone.

3. Zugriffsmöglichkeiten auf Datenbestände

Da es den Ermittlungsbehörden aber im Grunde genommen nicht auf die EDV-Anlagen bzw. die einzelnen Speichermedien, sondern lediglich auf deren Inhalt – also die durch elektrische Daten repräsentierten Informationen – ankommt[105], stellt sich die Frage, inwiefern sie tatsächlich Zugriff auf Datenbestände nehmen können. Bei der Beschlagnahme ist zu berücksichtigen, dass Datenbestände aufgrund ihrer Eigenschaft der Unkörperlichkeit ohne Qualitätsverlust übermittelt und kopiert werden können. Dieser Übermittlungsvorgang kann innerhalb eines örtlichen Netzwerks oder aber durch den Einsatz einer Datenfernübertragung (DFÜ) erfolgen. Damit lässt sich eine Einteilung in lokale und globale Daten vornehmen, je nachdem, ob der Zugriff auf die elektronischen Daten nur von innerhalb eines bestimmten Systems aus möglich ist oder ob der Zugriff auf den Datenbestand auch von außerhalb des Systems aus erfolgen kann[106]. Solche Zugriffe geschehen in der Regel über das öffentliche Kommunikationsnetz und sind daher weltweit möglich. Skizziert werden soll im Folgenden anhand von vier Grundkonstellationen, welche Probleme dabei für die Ermittlungsbehörden entstehen können. Die Erörterung dieser Problemkreise erfolgt dann im nächsten Kapitel anhand der jeweils einschlägigen Ermächtigungsgrundlage.

a) Lokale Daten

aa) Einzelplatzsystem

Relativ unproblematisch ist die Vorgehensweise der Ermittlungsbehörden bei der Beschlagnahme von lokalen Daten im Rahmen eines Einzelplatzsystems. Sie können hier einfach die externen Speichermedien und die EDV-Anlagen beschlagnahmen, was bei Computern, Mobiltelefonen und PDAs durch staatliche Ingewahrsamnahme in ein öffentlich-rechtliches Verwahrungsverhältnis erfolgt[107]. Schwierigkeiten könnten sich allenfalls bei einem PC ergeben. Dieser besteht in der Regel aus mehreren Geräten. Neben dem Monitor, der Zentraleinheit und der Tastatur gehören auch so genannte Peripheriegeräte wie bspw. Drucker, Scanner und Maus zu der Computeranlage. Eine Beschlagnahme all dieser Geräte wird jedoch in der Regel unverhältnismäßig sein, weil die Anschlüsse genormt sind und sie, abgesehen von Spezialanfertigungen, grundsätzlich durch behördeneigene Geräte ersetzt werden können[108]. Zudem enthalten die Peripheriegeräte ebenso wie Bildschirm und Tastatur keine elektronisch gespeicherten Daten, die für das konk-

---

105 *Bär*, Zugriff auf Computerdaten, S. 253.

106 *Wolf*, JuS-Beilage 1997, B 7.

107 KK-*Nack* § 94 Rn. 15 f.

108 Dies gilt natürlich nicht für extern angeschlossene Speichermedien, wie bspw. einer externen Festplatte.

rete Verfahren von Bedeutung sein könnten[109]. Insoweit kommt allenfalls der Zentraleinheit mit ihren fest integrierten Speichermedien eine potentielle Beweisbedeutung zu, weil ein Entfernen dieser Bestandteile eine Beschädigung der Hardware oder einen teilweisen Datenverlust zur Folge haben kann[110]. Auf eine Mitnahme der gesamten EDV-Anlage einschließlich der Peripheriegeräte kann deshalb in der Regel verzichtet werden. Dies gilt freilich nicht für die Fälle, in denen das Speichermedium nur im Zusammenspiel mit anderen Komponenten eines bestimmten Systems funktioniert bzw. dann, wenn die Computeranlage als Tatmittel der Einziehung gemäß §§ 74 ff. StGB unterliegt[111]. In diesen Fällen ist die Mitnahme der gesamten Computeranlage durchaus notwendig und verhältnismäßig.

Im Einzelfall dürfte es aber ebenso zweckmäßig sein, von einem Speichermedium lediglich eine Kopie anzufertigen und diese für die weiteren Ermittlungen zu verwenden oder das Original mitzunehmen und die Kopie dem Betroffenen bspw. zur Aufrechterhaltung seines Geschäftsbetriebes zur Verfügung zu stellen[112]. Zudem kann je nach der Art der gesuchten Information auch schon ein Ausdruck als Beweismittel ausreichen. Dies aber selbstverständlich nur dann, wenn der Ausdruck bereits vorhanden ist, weil sich die Beschlagnahme nur auf Gegenstände erstreckt, die zum Zeitpunkt der Anordnung bereits existent sind[113].

bb) Mehrplatzsystem

Erste Probleme ergeben sich aber dann, wenn sich die zu beschlagnahmenden Daten auf einem Mehrplatzsystem befinden. Typischerweise handelt es sich dabei um ein Local Area Network (LAN). Das LAN ist eine Gruppe von Computern und anderen Geräten, die über einen örtlich begrenzten Bereich verteilt und durch Kommunikationsleitungen miteinander verbunden sind, die jedem Gerät die Interaktion mit jedem anderen Gerät ermöglicht[114]. Der Sinn solcher Netzwerke besteht darin, den Datentransfer durch externe Datenträger zu vermeiden und damit eine Beschleunigung der Arbeitsvorgänge zu erreichen. In einem Firmennetzwerk kann so bspw. von jedem Arbeitsplatz aus auf einen zentralen Hochleistungsdrucker zugegriffen werden oder auf Datenbestände, die auf einem zentralen Speichermedium abgelegt sind. Es ist dabei möglich, den Zugriff von bestimmten Personen auf bestimmte Rechner und Ordner im Netzwerk zu limitieren. Dies erfolgt für gewöhnlich durch die Einrichtung von Benutzerkonten mit unterschiedlichen Freigabelevels bzw. Berechtigungsstufen.

Für die Ermittlungsbehörden stellte sich diesbezüglich ein Problem, weil der Durchsuchungs- und Beschlagnahmebeschluss sich üblicherweise nur auf die verdächtige Person und deren Arbeitsplatz bzw. dessen Räume bezieht. Ursächlich hierfür ist die Bestimmtheit des Durchsuchungs- und Beschlagnahmebeschlusses.

---

109 *Bär*, Zugriff auf Computerdaten, S. 261.

110 LR-*Schäfer* § 94 Rn. 25.

111 Zu denken ist in diesem Zusammenhang vor allem an Raubkopiererfälle, auf die § 110 UrhG Anwendung findet.

112 Dies gebietet der Verhältnismäßigkeitsgrundsatz, s. dazu D II 3.

113 *Bär*, Zugriff auf Computerdaten, S. 262.

114 Ms-Computer Lexikon, Stichwort „LAN“, S. 408.

Der anordnende Richter muss durch geeignete Formulierungen sicherstellen, dass der Grundrechtseingriff in Art. 13 I und Art. 14 GG, den jede Durchsuchung von Räumen und Beschlagnahme von Gegenständen mit sich bringt, angemessen begrenzt, messbar und kontrollierbar bleibt[115]. Bei mehreren kleineren Unternehmen, die sich ein LAN teilen, kann es bei der Durchsicht der Datenträger aber zu einer Durchsuchung von anderen Räumen kommen, wenn sich die zentrale Speichervorrichtung an einem Ort befindet, der nicht in dem Durchsuchungsbeschluss genannt wird. Es müssen dann die Voraussetzungen für die Durchsuchung von anderen Personen gemäß §§ 103, 105 StPO vorliegen. Bezieht sich der Durchsuchungsbeschluss auf das gesamte Unternehmen etwa im Falle einer Bürogemeinschaft, weil hier von vornherein mit einem LAN zu rechnen ist, kann die Staatsanwaltschaft unproblematisch die gesamte Computeranlage untersuchen. Üblicherweise geschieht das, wie bereits eben beim Einzelplatzsystem dargelegt, durch die Anfertigung einer Kopie des Datenbestandes, der Mitnahme der Speichermedien oder der Mitnahme der Computeranlage.

Bezieht sich der Durchsuchungs- und Beschlagnahmebeschluss hingegen nicht auf sämtliche Räume, dann war das weitere Vorgehen bisher schwierig, weil der Beschuldigte belastende Daten im LAN – bis die Staatsanwaltschaft mit einem neuen Durchsuchungsbefehl zurückkommt – selbst oder durch einen Dritten löschen lassen konnte. Dabei hilft auch die Überlegung, dass die Löschungen durch geeignete Maßnahmen von Kriminaltechnikern in vielen Fällen rückgängig gemacht werden können, nicht weiter. Denn zum einen sind solche Maßnahmen sehr kostenintensiv und zeitaufwendig, und zum anderen könnte der Beschuldigte den belastenden Datenträger auch einfach verschwinden lassen und durch einen anderen „sauberen" Datenträger ersetzen oder ihn zerstören oder den Datenträger mit Hilfe einer Spezialsoftware löschen, die eine Wiederherstellung der gelöschten Daten verhindert. Die Bandbreite möglicher Verdunklungs- und Manipulationshandlungen ist dabei weit gefächert.

Zudem ist in diesen Fällen auch zu bedenken, dass die Verdunklungsgefahr durch die Durchsuchung enorm ansteigt, weil der Beschuldigte nun vorgewarnt ist und mit einer weiteren Durchsuchung rechnen muss. Der zuständige Staatsanwalt hat in diesen Fällen zwar die Möglichkeit, bei Gericht telefonisch eine Erweiterung des Durchsuchungsbeschlusses zu beantragen. Der Richter kann diesem Antrag noch am Telefon nachkommen, weil es einer schriftlichen Form in Eilfällen nicht zwingend bedarf[116]. Sollte ein Richter allerdings nicht zu erreichen sein, dann könnte der Staatsanwalt trotz der potentiell bestehenden Verdunklungsgefahr grundsätzlich nicht wegen Gefahr in Verzug selbst die weitere Durchsuchung anordnen. Das Bundesverfassungsgericht stellt in jüngerer Zeit erhöhte Anforderungen an die Begründung der Gefahr in Verzug, weil der Richtervorbehalt nach Art. 13 II GG Verfassungsrang genießt[117]. Danach sind Spekulationen, hypothetische Erwägungen und auf kriminalistische Erfahrung beruhende fallunabhängige

115 *Meyer-Goßner* § 105 Rn. 5.
116 KK-*Nack* § 105 Rn. 3, BGH 28, 57, 59; *Hellmann* S. 147.
117 BVerfGE 103, 142, 155; vgl. auch *Jahn* NStZ 2007, 259.

Vermutungen als Grundlage für die Annahme von Gefahr in Verzug nicht ausreichend[118].

Aus diesen Gründen hat der Gesetzgeber § 110 III StPO geschaffen und in die Strafprozessordnung eingefügt. Dieser soll den Ermittlungsbehörden den Online-Zugriff auf die mit dem Computer vernetzten Speichermedien des von der Durchsuchung Betroffenen gestatten[119]. Erlaubt wird hierdurch aber nicht die Beschlagnahme des entfernten Speichermediums sondern lediglich seine Durchsicht und gegebenenfalls das Herunterladen von Daten zum Zwecke der Ermittlung ihrer Relevanz für das weitere Verfahren. Wollen die Ermittlungsbehörden hingegen das entfernt befindliche Speichermedium selbst beschlagnahmen, dann bedarf es wie bisher einer Erweiterung des bestehenden oder den Erlass eines neuen Durchsuchungs- und Beschlagnahmebeschlusses.

b) Globale Daten

Globale Daten zeichnen sich dadurch aus, dass ihr Zugriff von außerhalb des sie beherbergenden Systems aus möglich ist[120]. Ein Benutzer kann also bspw. in Köln sitzen und Zugriff auf elektronisch gespeicherte Daten nehmen, die in Berlin auf einem Server gespeichert sind. Ebenso kann der Zugriff von Köln aus aber auch auf Daten, die auf einem Server in New York gespeichert sind, erfolgen. Diese Möglichkeit, Daten über weite Strecken zwischen zwei grundsätzlich unabhängigen Systemen zu übertragen, wird Datenfernübertragung (DFÜ) genannt.

aa) National

Diese Form der Datenkommunikation wird häufig von großen Firmen verwendet, um Daten zentral an einem bestimmten Ort wie bspw. dem firmeneigenen Rechenzentrum oder der Hauptverwaltung speichern zu können. Sämtliche Filialen haben dann Zugriff auf die gespeicherten Daten.

Hierfür brauchte die Staatsanwaltschaft vor Einführung[121] des § 110 III StPO einen Durchsuchungsbeschluss, der sich auf den Standort des entfernt liegenden Speichermediums bezog. Dies war jedoch schon deshalb mit Schwierigkeiten behaftet, weil der Server nicht in der gleichen Stadt stehen muss wie das durchsuchte System. Dann aber war für die Erteilung eines Durchsuchungsbeschlusses auch ein anderes Gericht örtlich zuständig[122].

Dem hat der Gesetzgeber nun durch die Einführung[123] des § 162 I StPO entgegengewirkt und eine örtliche Zuständigkeitskonzentration bei dem Amtsgericht, in dessen Bezirk die Staatsanwaltschaft oder ihre Zweigstelle ihren Sitz hat, begrün-

---

118 *Beulke* Rn. 258.

119 § 110 III StPO ist allerdings wegen seines unpräzisen und weiten Wortlauts verfassungsrechtlich bedenklich, vgl. C II 3 c).

120 Zu Fragen der Beweisgewinnung vgl. *Marberth-Kubicki* StraFo 2002, 280 ff.

121 Vgl. Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BGBl. I 2007, 3198 ff.

122 Vgl. § 162 StPO a. F.

123 BGBl. I 2007, 3198, 3204.

det. Im Zusammenspiel mit § 110 III StPO kann daher im Rahmen einer so genannten Online-Durchsuchung von dem zu durchsuchenden Computer aus Zugriff auf den Datenbestand des Servers genommen werden[124].

bb) International

Am schwierigsten gestaltet sich die Beschlagnahme von globalen Daten, die außerhalb von Deutschland gespeichert sind. Ein Beispiel dafür bildet der Fall, in dem die Staatsanwaltschaft Frankfurt ermittelt hatte[125]. Dabei stand ein Unternehmen im Verdacht, einen Kapitalanlagebetrug begangen zu haben[126]. Bei der daraufhin durchgeführten Durchsuchung wurde lediglich ein Computerterminal – ohne eigenen Datenspeicher – mit Anschluss an das öffentliche DFÜ-Netz gefunden. Wie sich im Laufe der weiteren Ermittlungen herausstellte, wurden die gesamten relevanten Geschäftsdaten von einem Drittunternehmen auf einem Server in der Schweiz gespeichert. Die Staatsanwaltschaft Frankfurt versuchte in diesem Fall, die Beschlagnahme der Speichermedien im Wege der Rechtshilfe zu erreichen. Als die schweizerischen Kollegen diesem Ersuchen aber endlich nachkamen, war zuvor bereits die Löschung der Unterlagen durch die in Monaco sitzende Hauptverwaltung des Unternehmens, gegen das sich die Ermittlungen richteten, veranlasst worden.

Dies ist nicht weiter verwunderlich, da das betroffene Unternehmen aufgrund der durchgeführten Durchsuchung vorgewarnt war und das Verfahren bei der Rechtshilfe tendenziell recht langwierig und kompliziert ist. Bereits in Deutschland muss das konkrete Rechtshilfeersuchen von justizministeriellen und diplomatischen Stellen geprüft werden, bevor es dann über das Außenministerium an das Außenministerium des ersuchten Staates weitergeleitet wird[127]. Hier erfolgt dann die Prüfung in umgekehrter Reihenfolge, bis schließlich von der im Zielstaat zuständigen Behörde die begehrte Zwangsmaßnahme durchgeführt wird.

Aufgrund dieses Verfahrens, dessen Ineffektivität wegen der Langwierigkeit und der vielen Personen, die mit dem Ersuchen beschäftigt sind, vorbestimmt ist[128], versuchen die Ermittlungsbehörden neuerdings, dem beweisrelevanten Material durch eine Online-Durchsuchung im Ausland habhaft zu werden. Dabei treten aber weitere Probleme auf. Zu denken ist dabei in erster Linie an die Verletzung des Souveränitätsgrundsatzes anderer Staaten, weil sich die Ermittlungsbehörden von deutschem Boden aus in ausländische Rechner begeben. Zudem stellen sich Fragen nach einer eventuellen Strafbarkeit der Ermittlungsbeamten nach Tatbeständen des jeweils einschlägigen ausländischen Strafrechts[129]. Diese Problemkreise sind jedoch nicht Gegenstand der vorliegenden Arbeit, da es für die

---

124 Zu den dabei auftretenden Problemen vgl. *Hofmann* NStZ 2005, 121 ff.

125 92 Js 34528/87.

126 Vgl. ausführlich zu diesem Fall *Bär*, Zugriff auf Computerdaten, S. 41 f., sowie *Bär* CR 1995, 159.

127 Vgl. dazu Müller/Wabnitz/Janovsky S. 285 ff.

128 *Bär* CR 1995, 233.

129 Bspw. gegen das Bankgeheimnis, das in der Schweiz durch Art. 47 Schweizer Bankgesetz geschützt ist.

Untersuchung allein auf elektronisch gespeicherte Daten im Inland ankommen soll.

III. Private Träger von Berufsgeheimnissen

Weder die StPO noch das StGB enthalten explizit die Tatbestandsmerkmale des „privaten Trägers von Berufsgeheimnissen“ oder den des „Berufsgeheimnisträgers“. Diese aus der Rechtspraxis stammenden Begriffe werden jedoch im Zusammenhang mit § 203 StGB und § 53 StPO gebraucht. Wie die Begrifflichkeiten schon andeuten, bedarf es dazu eines Geheimnisses und eines bestimmten Trägerkreises, der aufgrund seiner beruflichen Rolle mit den Geheimnissen anderer Personen in Berührung kommt. Die nun folgende Untersuchung soll diese Merkmale eingehend erörtern.

1. Der Begriff des Geheimnisses

Allgemein ist unter dem Begriff „Geheimnis“ das noch nicht Erkannte, Erforschte wie auch das, was rationaler Erfassung grundsätzlich entzogen ist, bzw. nach dem jeweiligen Stand der Wissenschaft der verstandesmäßigen Erkenntnis entzogen scheint oder wofür – im religiösen Bereich – die Vernunfterkenntnis als nicht zureichend erachtet wird, zu verstehen[130].

Der Begriff des Geheimnisses findet sich auch in zahlreichen Gesetzen. Die Verfassung enthält bspw. in Art. 10 GG das Brief-, Post- und Fernmeldegeheimnis. Damit soll die Vertraulichkeit bestimmter Kommunikationsformen geschützt werden, die wegen der räumlichen Distanz und der Zugriffsmöglichkeiten Dritter besonders gefährdet sind[131]. Das Verwaltungsrecht enthält den Anspruch auf Geheimhaltung nach § 30 VwVfG, dem Beamte und öffentliche Bedienstete unterliegen[132]. Es soll die Vertraulichkeit dienstlicher Vorgänge und persönlicher Daten schützen. Zu nennen ist ferner das Steuergeheimnis, das in § 30 AO enthalten ist und die Finanzbehörden daran hindert, Erkenntnisse, die sie aus einem Verfahren in Steuersachen gewinnen, an Dritte weiterzugeben. Durch die Schaffung der §§ 93, 95, 97, 97a, 97b, 202, 203, 204, 206 und § 353b StGB hat der Begriff des „Geheimnisses“ auch Eingang in das Strafgesetzbuch gefunden[133]. Dabei ist zwischen Staatsgeheimnissen, Dienstgeheimnissen und Privatgeheimnissen zu differenzieren.

---

130 Brockhaus, Band 10, Stichwort „Geheimnis“.

131 *Pieroth/Schlink*, Staatsrecht II, Rn. 762 ff.

132 *Knack* § 30 VwVfG; *Maurer* § 19 Rn. 22; Wolff/Bachhof/Stober-*Kluth* § 59 Rn. 22.

133 Geschäfts- und Betriebsgeheimnisse werden in Fällen der Wirtschaftsspionage zudem von § 17 UWG und § 266 StGB sowie im Einzelfall von § 120 BetrVG, § 69 SchwbG, § 404 AktG, § 85 GmbHG, § 151 GenG, § 138 VAG, § 333 HGB und § 43 BDSG geschützt, vgl. *Kiethe/Hohmann* NStZ 2006, 185 ff.

a) Staats- und Dienstgeheimnisse

Staatsgeheimnisse sind nach § 93 I StGB Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheim gehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden[134]. Dienstgeheimnisse i. S. d. § 353b StGB sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis bekannt und zugänglich sind und ihrer Natur nach oder auf Grund einer Rechtsvorschrift oder besonderen Anordnung der Geheimhaltung bedürfen[135]. Entscheidend für den Geheimnisbegriff der §§ 93, 353b StGB ist damit, dass die Tatsachen, Gegenstände oder Erkenntnisse nicht allgemein, sondern nur einem begrenzten Personenkreis bekannt sind.

b) Privatgeheimnisse

Privatgeheimnisse werden von § 203 StGB geschützt[136]. Der Tatbestand stellt die Verletzung von zum persönlichen Lebensbereich gehörenden Geheimnissen oder die Offenbarung von Betriebs- oder Geschäftsgeheimnissen unter Strafe[137]. Die materielle Bedeutung des § 203 StGB ist für eine Vielzahl von prozessualen Normen der Anknüpfungspunkt für die Annahme von Zeugnisverweigerungsrechten. Zu nennen sind hier bspw. § 53 StPO und § 383 I Nr. 6 ZPO, auf den die §§ 46 II S. 1 ArbGG, 98 VwGO und § 118 I S. 1 SGG verweisen sowie § 84 FGO i.V.m. § 102 AO. Eine Legaldefinition enthält der Tatbestand des § 203 StGB für den Begriff des „Privatgeheimnisses" indessen nicht[138].

Nach allgemeiner Ansicht umfassen fremde Geheimnisse i. S. v. § 203 StGB Tatsachen, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung der Geschützte ein sachlich begründetes Interesse hat[139]. Gegenstand des Geheimnisbegriffs nach § 203 StGB sind damit allein Tatsachen, die sich einer bestimmten Person zuordnen lassen[140]. Die Grenze ist nach der Faustformel von Bockelmann[141] immer dann erreicht, „wenn das Geheimnis so vielen anderen bekannt geworden ist, das es nichts mehr verschlägt, wenn noch weitere davon erfahren."

Unter Tatsachen sind alle konkreten vergangenen oder gegenwärtigen Geschehnisse oder Zustände der Außenwelt und des menschlichen Innenlebens zu verstehen[142]. Demzufolge scheiden Werturteile und unrichtige personenbezogene

---

134 *Tröndle/Fischer* § 93 Rn. 2.

135 *Lackner/Kühl* § 353 b Rn. 6.

136 Vgl. zu weiteren Straftaten mit Computerbezug die Aufstellung bei *Möhrenschläger*, wistra 1991, 324 ff.

137 Eingehende Untersuchung des § 203 StGB bei *Schmitz*, JA 1996, 772 ff.

138 MK-StGB-*Cierniak* § 203 Rn. 11.

139 *Rengier*, S. 234 Rn. 34.

140 *Tröndle/Fischer* § 203 Rn. 4; MK-StGB-*Cierniak* § 203 Rn. 12; *Lackner/Kühl* § 203 Rn. 14.

141 *Bockelmann*, BT 2, S. 176.

142 Schönke/Schröder-*Cramer/Perron* § 263 Rn. 8.

Informationen als Gegenstand von Geheimnissen aus[143]. Die Tatsachen können alle Bereiche des Lebens betreffen und insbesondere, wie in § 203 I StGB ausdrücklich genannt, den persönlichen Lebensbereich oder die berufliche oder geschäftliche Sphäre berühren. An der Personenbezogenheit der Daten fehlt es jedoch, wenn anonymisierte Daten verwendet werden, die keinen Rückschluss auf den Betroffenen zulassen[144]. Neben der Personenbezogenheit von Tatsachen enthält der Geheimnisbegriff des § 203 StGB drei weitere Elemente. Ein Geheimnis erfordert demnach das Geheimsein, den Geheimhaltungswillen und das objektive Geheimhaltungsinteresse[145].

c) Berufsgeheimnis nach der StPO

Der Begriff des Berufsgeheimnisses ist in der StPO ebenso wenig wie im StGB legal definiert. Trotzdem ist er auch im Zusammenhang mit der StPO nicht unbekannt und wird von Meyer-Goßner[146] sogar als nichtamtliche Überschrift für § 53 StPO benutzt, wohingegen die meisten anderen Kommentare die Überschrift des „Zeugnisverweigerungsrechts aus beruflichen Gründen“ verwenden[147]. Die in § 53 StPO genannten Berufsgruppen haben gemein, dass gesetzliche Vorschriften oder Berufs- und Standesregeln eine berufsbezogene Schweigepflicht begründen, die einen genuinen Bestandteil der eingenommenen Rolle darstellen[148], weil die Inanspruchnahme ihrer Hilfe und Sachkunde nur aufgrund eines Vertrauensverhältnisses zu ihren jeweiligen Mandanten, Patienten, Klienten usw. möglich ist[149]. Anderenfalls könnte sich der Rat- und Hilfesuchende an einer rückhaltlosen Offenbarung durch die Besorgnis behindert fühlen, dass die Vertrauensperson das ihr Anvertraute als Zeuge einmal preisgeben müsste[150].

Der Grund für die Privilegierung bestimmter Berufsgruppen durch § 53 StPO liegt in dem Umstand, dass ihre Tätigkeit stärker und häufiger Bereiche berührt, in denen schutzwürdige Geheimhaltungsinteressen des Einzelnen Beachtung verlangen[151]. Dies ist bei den in § 53 I StPO genannten Berufen deshalb der Fall, weil ihre Ausübung typischerweise Leistungen einschließt, die sich als individuelle Beratung in persönlichen, rechtlichen, finanziellen und wirtschaftlichen Angelegenheiten oder aber als unmittelbarer Dienst an der Gesundheit des Menschen kennzeichnen lassen[152].

Daher gewährt § 53 StPO den in seinem Tatbestand genannten Berufsgruppen ein Zeugnisverweigerungsrecht für Tatsachen, die ihnen bei der Berufsausübung

---

143 LK-*Schünemann* § 203 Rn. 20; a.A. *Tröndle/Fischer* § 203 Rn. 10b.
144 *Tröndle/Fischer* § 203 Rn. 3.
145 OLG Hamm NJW 2001, 1957, 1958; LK-*Schünemann* § 203 Rn. 19; *Lackner/Kühl* § 203 Rn. 14; *Tröndle/Fischer* § 203 Rn. 15 f.; MK-StGB-*Cierniak* § 203 Rn. 11.
146 *Meyer-Goßner* § 53 S. 183.
147 KK-*Senge* § 53 S. 293; LR-*Dahs* § 53; *Pfeiffer* § 53.
148 SK-StPO-*Rogall* § 53 Rn. 2.
149 *Meyer-Goßner* § 53 Rn. 1.
150 *Pfeiffer* § 53 Rn. 1.
151 BVerfGE 38, 312, 323.
152 BVerfGE a. a. O.

anvertraut oder bekannt geworden sind. Der Berufsausübende darf deshalb über die ihm anvertrauten oder bekannt gewordenen Tatsachen vor Gericht das Zeugnis verweigern, sofern er nicht nach § 53 II StPO von der Verpflichtung zur Verschwiegenheit entbunden wurde oder ein Fall des § 53 II S. 2 StPO vorliegt. Die in § 53 I StPO genannten Berufsgruppen haben damit die Möglichkeit, Informationen von oder über ihre Mandanten, Klienten, Patienten usw. geheim zu halten. Eine Verpflichtung besteht hierzu indessen nicht. Dies zeigt schon der Umstand, dass von dem Zeugnisverweigerungsberechtigten gemachte Aussagen vom Gericht ohne weiteres verwertet werden dürfen[153]. Evident ist damit, dass das Zeugnisverweigerungsrecht des § 53 StPO nicht bloß die prozessuale Umsetzung der materiell-rechtlichen Schweigepflicht nach § 203 StGB ist[154].

aa) Umfang der geheim zu haltenden Tatsachen

Grundsätzlich können die in § 53 StPO genannten Berufsträger das Zeugnis verweigern, wenn es sich um anvertraute oder bekannt gewordene Tatsachen handelt.

(1) Anvertraute Tatsachen

Tatsachen sind dem Berufsträger anvertraut worden, wenn sie unter Verlangen oder stillschweigender Erwartung der Geheimhaltung gemacht wurden[155]. Von Letzterem ist auszugehen, wenn sich dies aus den Umständen oder aus der Natur der Sache ergibt[156]. Demnach ist unerheblich, ob die Tatsachen mündlich oder schriftlich mitgeteilt wurden oder lediglich dem Berufsausübenden Gelegenheit zur Beobachtung und Untersuchung gegeben wird, wie dies bspw. bei einer Untersuchung durch einen Arzt regelmäßig der Fall ist[157]. Dementsprechend müssen dem Anvertrauenden die festzustellenden Tatsachen nicht selbst bekannt sein, sondern es genügt, dass der Zeuge sie aufgrund seiner Erfahrung und besonderen Sachkunde aufdecken kann[158]. Ebenfalls gleichgültig ist, ob der Beschuldigte oder ein Dritter die Tatsachen dem Berufsträger anvertraut hat und ob sie der Geheimnissphäre des Beschuldigten oder eines Dritten angehören[159].

(2) Bekannt gewordene Tatsachen

Tatsachen gelten als bekannt geworden, wenn sie der Berufsausübende von dem Beschuldigten oder einem Dritten erfahren hat, ohne dass sie ihm anvertraut worden sind[160]. Dazu gehören bspw. der Inhalt beruflicher Gespräche, Mitteilungen von Kollegen oder den Berufskammern oder Wahrnehmungen an einem Bewuss-

---

153 St. Rspr. des BGH, vgl. BGHSt. 9, 59, 62; 15, 200, 200; ebenso *Meyer-Goßner* § 53 Rn. 6; KK-*Senge* § 53 Rn. 9; LR-*Dahs* § 53 Rn. 14.

154 So aber *Foth* JR 1976, 7; a. A die h. M. SK-StPO-*Rogall* § 53 Rn. 4; KK-*Senge* § 53 Rn. 4; *Meyer-Goßner* § 53 Rn. 4; LR-*Dahs* § 53 Rn. 9; *Eisenberg* Rn. 1264.

155 RG 66, 273, 274; OLG Köln NStZ 1983, 412.

156 LR-*Dahs* § 53 Rn. 17.

157 BGH 38, 369, 370.

158 LR-*Dahs* § 53 Rn. 16.

159 *Meyer-Goßner* § 53 Rn. 8; LR-*Dahs* a. a. O.

160 *Meyer-Goßner* § 53 Rn. 9.

tlosen[161]. Das Tatbestandsmerkmal ist zwar weit auszulegen[162], so dass auch zufällig erlangtes Wissen eine bekannt gewordene Tatsache darstellen kann; jedoch nur, wenn es im Zusammenhang mit dem Vertrauensverhältnis erworben wurde[163]. Schließlich muss es sich bei den bekannt gewordenen Tatsachen nicht um Privatgeheimnisse i. S. des § 203 StGB handeln, weil der Tatbestand des § 53 StPO durch die Formulierung: „... über das, was ihnen ... bekannt geworden ist." über Privatgeheimnisse hinausgehen kann[164]. Somit können unter das Berufsgeheimnis auch allgemein bekannte Tatsachen fallen.

bb) Vergleich zu § 203 StGB

Flankiert wird dieses Recht des Zeugnisverweigerungsberechtigten durch die Verpflichtung zur Geheimhaltung gemäß § 203 StGB, wonach bei Vorliegen der entsprechenden Voraussetzungen Privatgeheimnisse durch den Berufsträger nicht offenbart werden dürfen. Dabei ist jedoch zu beachten, dass § 53 StPO und § 203 StGB keinesfalls deckungsgleich sind, auch wenn sie sich teilweise entsprechen[165].

Schon ein Vergleich zwischen dem Tatbestand des § 53 StPO und dem des § 203 StGB zeigt, dass beide Tatbestände hinsichtlich ihrer persönlichen Reichweite zwar weitgehend übereinstimmen, aber nicht vollkommen deckungsgleich sind. § 203 StGB enthält die Berufsgruppen der Tierärzte, Sozialarbeiter, Sozialpädagogen und die Angehörigen eines privaten Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle. Diese Berufsgruppen werden in § 53 StPO dagegen nicht aufgeführt. Zudem werden einige Berufsgruppen nur teilweise oder unter bestimmten Bedingungen als zeugnisverweigerungsberechtigt nach § 53 StPO anerkannt. Dazu zählen die Organe und Organmitglieder des § 203 Nr. 3 StGB, die nur dann auch ein Zeugnisverweigerungsrecht nach § 53 StPO haben, wenn sie selbst einen Beruf nach § 53 I Nr. 3 StPO ausüben. Auch Berufspsychologen[166] haben nur dann ein Zeugnisverweigerungsrecht, wenn sie in einer Beratungsstelle tätig sind oder ihren Beruf als psychologische Psychotherapeuten oder als Kinder- und Jugendpsychotherapeuten ausüben[167]. Außerdem enthält § 53 StPO umgekehrt Personengruppen, die in § 203 StGB nicht aufgenommen wurden. Zu nennen sind hier bezüglich der privaten Träger von Berufsgeheimnissen Geistliche nach § 53 I Nr. 1 StPO und die Medienmitarbeiter nach § 53 I Nr. 5 StPO.

---

161 LR-*Dahs* § 53 Rn. 18.
162 BGH MDR 78, 281.
163 LG Karlsruhe StV 83, 149.
164 LR-*Dahs* § 53 Rn. 18.
165 *Meyer-Goßner* § 53 Rn. 4; KK-*Senge* § 53 Rn. 3.
166 Unter Ausschluss der von § 203 I Nr. 2 StGB erfassten Diplom-Psychologen, BGH NStZ 2006, 509.
167 SK-StPO-*Rogall* § 53 Rn. 13.

2. Erlangung in beruflicher Eigenschaft

Das Recht zur Geheimhaltung bestimmter Tatsachen trifft nach § 53 StPO nicht jedermann, sondern nur die Angehörigen bestimmter Berufsgruppen. Der Grund hierfür liegt in dem spezifischen Vertrauensverhältnis, das zwischen dem Geheimnisgeschützten und dem Schweigeberechtigten bei manchen Tätigkeiten zwangsläufig zur erfolgreichen Ausübung des Berufes bestehen muss[168]. Der Geheimnisgeschützte hat in diesen Fällen z. T. auch keine Alternativmöglichkeit zu der Inanspruchnahme der bestimmten Berufsgruppe[169]. Deutlich wird dies besonders bei den klassischen Berufsgeheimnisträgern, wie bspw. dem Verteidiger im Verhältnis zu seinem Mandanten oder dem Arzt im Verhältnis zu seinen Patienten. Wären Ärzte bspw. nicht zur Zeugnisverweigerung berechtigt und verpflichtet, dann hätte das für die Patienten mitunter peinliche Folgen, etwa wenn der Gynäkologe in der Hauptverhandlung über die Krankheit einer Patientin erzählen würde, die bei ihm in Behandlung war. Neben Peinlichkeiten können aber auch strafrechtliche und wirtschaftliche Konsequenzen für den Geheimnisgeschützten drohen, etwa dann, wenn der Unfallarzt bei dem Opfer eines Unfalls Drogen in erheblichem Umfang findet oder ein Wirtschaftsprüfer, der über die Aktiva und Passiva eines Unternehmens Andeutungen macht und dadurch dessen Kreditwürdigkeit gefährdet.

Entscheidend ist dabei, dass der Berufsgeheimnisträger die Tatsachen nicht nur als Privatperson erlangt hat, sondern gerade in seiner Funktion als Angehöriger einer durch § 53 StPO besonders berechtigten Berufsgruppe[170]. Welche Tatsachen in beruflicher Eigenschaft erfahren werden, kann nicht generell bestimmt werden, sondern ist im Einzelfall nach dem jeweiligen Berufsbild des Zeugnisverweigerungsberechtigten zu entscheiden. Ein Vertrag oder eine zivilrechtliche Sonderbeziehung sind hierfür aber nicht erforderlich[171]. Unzureichend ist auch das Abstellen auf Sprechzeiten oder Dienststunden für die Annahme einer beruflichen Natur[172]. Einigkeit besteht aber insoweit, dass Straftaten und die Teilnahme an solchen stets berufsfremd sind[173].

Für einige Berufsgruppen bestehen Gebührenordnungen, sodass als Anhaltspunkt für die Abgrenzung berufsmäßig bzw. berufsfremd auf die darin aufgeführten Tätigkeiten abgestellt werden kann, weil sich diese an dem jeweiligen Berufsbild orientieren[174]. Ein Rechtsanwalt, der im Zusammenhang mit einer Mandatserteilung Geheimnisse erfährt, hat daher in berufsmäßiger Funktion Kenntnisse an

---

168 *Tröndle/Fischer* § 203 Rn. 2.

169 Anders bei der Konsultation eines Heilpraktikers, der nicht in § 203 StGB aufgeführt ist, weil der Geheimnisgeschützte auch einen Arzt aufsuchen könnte. Die Konsultation eines Heilpraktikers sei hingegen eine Luxushandlung, die einen strafrechtlichen Schutz nicht erfordere, LK-*Schünemann* § 203 Rn. 16.

170 KK-*Senge* § 53 Rn. 2; *Meyer-Goßner* § 53 Rn. 7.

171 LR-*Dahs* § 53 Rn. 15.

172 *Meyer-Goßner* a.a.O.

173 BVerfGE 32, 373, 381.

174 LK-*Schünemann* § 203 Rn. 35.

diesen Tatsachen erlangt[175]. Nicht dazu zählen dementsprechend die Tätigkeiten eines Rechtsanwalts als Heiratsvermittler, Vermittler von Grundstücksgeschäften oder als Gesellschafter[176]. Die Ausrichtung an den in der Gebührenordnung aufgeführten Tätigkeiten ist aber keinesfalls abschließend, denn häufig erfordert die Bildung eines Vertrauensverhältnisses zwischen dem Berufsgeheimnisträger und dem Geheimnisgeschützten auch das Eingehen auf die allgemeinen Sorgen und Nöte, die mit der eigentlichen beruflichen Tätigkeit nichts zu tun haben. Daher unterliegen auch diesbezügliche Angaben dem Schweigerecht und stellen somit ein Berufsgeheimnis dar.

3. Betroffener Personenkreis

Zu untersuchen ist, welcher Personenkreis zu den privaten Trägern von Berufsgeheimnissen zu zählen ist. Nach § 53 I StPO kann dies nur sein, wer zu einer der im Gesetz näher bezeichneten Personen gehört. Die dort vorgenommene Aufzählung ist grundsätzlich abschließend[177] und kann nur in sehr seltenen Ausnahmefällen und unter besonders strengen Voraussetzungen unmittelbar aus Art. 2 I i.V.m. Art. 1 I GG auf Einzelfälle[178] erweitert werden.

a) Berufsgruppen des § 53 I StPO

Nach § 53 I Nr. 1 StPO dürfen Geistliche über das, was ihnen in ihrer Eigenschaft als Seelsorger anvertraut worden ist, das Zeugnis verweigern. Mit Geistlichen i. S. d. § 53 I Nr. 1 StPO werden nur diejenigen Kleriker der christlichen Kirche[179] und der sonstigen öffentlich-rechtlichen[180] Religionsgemeinschaften erfasst[181]. Dazu zählen allerdings auch Laien, die keine kirchlichen Weihen erhalten haben, aber im Auftrag der Kirche hauptamtlich und selbständig Aufgaben wahrnehmen, die zum unmittelbaren Bereich seelsorgerischer Tätigkeiten gehören[182]. Dabei ist

---

[175] BGH NJW 2001, 2462, 2463; dazu zählt auch schon die Tatsache der Inanspruchnahme anwaltlicher Dienste, *Streck* NJW 2001, 3605.

[176] KK-*Senge* § 53 Rn. 1; vgl. für die ähnliche Problematik bei § 203 StGB: LK-*Schünemann* § 203 Rn. 35.

[177] Um die Funktionsfähigkeit der Strafrechtspflege in Gestalt der umfassenden Wahrheitserforschungspflicht gemäß § 244 II StPO zu gewährleisten, *Jahn* JuS 2007, 584, 585.

[178] Kein Zeugnisverweigerungsrecht haben bspw. Bankangestellte im Hinblick auf das sog. Bankgeheimnis, LG Hamburg NJW 1978, 958; Betriebsräte BVerfGE 1979, 1286; Tierärzte, BVerfGE 38, 312.

[179] Art. 9 des Reichskonkordats zwischen dem Heiligen Stuhl und dem Deutschen Reich, RGBl. 1933 S. 679. Gilt aus Gründen der Parität auch für die evangelische Kirche, LR-*Dahs* § 53 Rn. 21.

[180] Vgl. Art. 140 GG i. V. m. Art. 137 V WRV.

[181] Nicht dazu zählen bspw. die „Zeugen Jehovas“, BGH Urteil vom 5.5. 1953, 1 StR 194/53.

[182] Insoweit liegt eine Art Stellvertretung für geweihte Kleriker vor, wodurch die Laien denselben schwierigen seelsorgerischen Situationen ausgesetzt sind. BGH NStZ 2007,

unerheblich, ob den Geistlichen auch eine kirchenrechtliche Pflicht zur Verschwiegenheit, bspw. nach kanonischem Recht trifft[183]. Der Geistliche darf aber ausweislich des Wortlauts des Gesetzes nur über die Tatsachen schweigen, die ihm als Seelsorger anvertraut wurden. Nicht dazu zählen Geheimnisse, die er ausschließlich bei karitativen, erzieherischen oder verwaltender Tätigkeit erfahren hat[184].

Gemäß § 53 I Nr. 2 StPO sind Verteidiger des Beschuldigten berechtigt, über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekannt geworden ist, das Zeugnis zu verweigern. Nummer zwei erlangt vor allem für Verteidiger Bedeutung, die keine Rechtsanwälte sind und somit nicht unter § 53 I Nr. 3 StPO fallen[185]. Dabei kann es sich bspw. um einen von dem Beschuldigten gewählten oder vom Gericht bestellten Verteidiger nach den §§ 137, 138 oder 142 StPO handeln. Der Verteidiger darf das Zeugnis über Tatsachen verweigern, die ihm in dieser Eigenschaft in dem vorliegenden oder einem anderen Strafverfahren desselben Beschuldigten oder eines anderen Beschuldigten bekannt geworden sind[186].

Nach § 53 I Nr. 3 StPO dürfen Rechtsanwälte, Patentanwälte, Notare, Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater und Steuerbevollmächtigte, Ärzte[187], Zahnärzte, Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten[188], Apotheker und Hebammen[189] über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekannt geworden ist, das Zeugnis verweigern. Rechtsanwalt ist, wer nach § 12 BRAO als Rechtsanwalt zugelassen wurde. Dazu gehören auch die ausdrücklich erwähnten Kammerrechtsbeistände und ausländischen Rechtsanwälte, wenn sie nach §§ 206, 207 BRAO in einem EG-Mitgliedsstaat zugelassen sind. Ferner gehören amtlich bestellte Vertreter nach § 53 BRAO und Abwickler nach § 55 BRAO sowie Syndikusanwälte nach § 46 BRAO dazu, wenn sie mit typisch anwaltlichen Aufgaben befasst sind[190].

Gemäß § 53 I Nr. 3a StPO ist Berufsgeheimnisträger, wer Mitglied oder Beauftragter einer anerkannten Beratungsstelle (für Sexualaufklärung, Verhütung, Familienplanung, Schwangerschaft) nach den §§ 3 und 8 Schwangerschaftskonfliktgesetz ist[191].

---

275 ff.; bestätigend BVerfG mit Beschluss vom 25. 1. 2007 Az. 2 BvR26/07; vgl. *Jahn* JuS 2007, 584 ff.

183 *Lenckner* NJW 1965, 322.

184 *Meyer-Goßner* § 53 Rn. 12; KK-*Senge* § 53 Rn. 12; LR-*Dahs* § 53 Rn. 25; SK-StPO-*Rogall* § 53 Rn. 70.

185 *Meyer-Goßner* § 53 Rn. 13.

186 LR-*Dahs* § 53 Rn. 26.

187 Arzt ist, wer im Inland als Arzt approbiert ist, *Meyer-Goßner* § 53 Rn. 17.

188 §§ 1, 2 des Gesetzes über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendpsychotherapeuten vom 01.01.1999, zuletzt geändert Art 5 XVI G vom 15.12.2004 BGBl. I S. 3396.

189 §§ 1 I, 2 des Gesetzes über den Beruf der Hebamme und des Entbindungspflegers vom 01.07.1985, zuletzt geändert durch Art. 2 V vom 22.10.2004 BGBl. I S. 2657.

190 *Meyer-Goßner* § 53 Rn. 15.

191 Nicht unter § 203 I Nr. 4a StGB fällt die Beratung einer Mutter nach der Geburt ihres Kindes hinsichtlich eines "Babyklappen-Projekts", LG Köln NJW 2002, 909.

Nach § 53 I Nr. 3b StPO werden Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt sind, erfasst. Die Anerkennung erfolgt in der Regel durch Landesrecht[192]. Es genügt allerdings auch eine kirchliche Anerkennung. Nicht anerkannt sind dagegen die Beratungsstellen, die von freien Trägern angeboten werden. Dies gilt selbst dann, wenn sich öffentliche Stellen dieser Beratungsstellen zur Erfüllung ihrer Aufgaben bedienen[193].

Nach § 53 I Nr. 4 StPO dürfen Mitglieder des Bundestages, eines Landtages oder einer zweiten Kammer über Personen, die ihnen in ihrer Eigenschaft als Mitglieder dieser Organe oder denen sie in dieser Eigenschaft Tatsachen anvertraut haben sowie über diese Tatsache selbst, das Zeugnis verweigern. Für die Bundestagsabgeordneten ergibt sich das bereits aus Art. 47 S. 1 GG[194]. Im Unterschied zu den anderen Berufsgruppen ist bei § 53 I Nr. 4 StPO eine Befreiung von dem Zeugnisverweigerungsrecht ausgeschlossen[195].

§ 53 I Nr. 5 StPO berechtigt schließlich Personen zur Verweigerung des Zeugnisses, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken oder mitgewirkt haben. Geschützt wird dadurch das Vertrauensverhältnis zwischen der Presse und den privaten Informanten[196]. Dieser Schutz ergibt sich bereits aus Art. 5 I S. 2 der Verfassung. Berufsmäßig mitgewirkt haben nicht nur die Journalisten, Redakteure, Intendanten, Sendeleiter und Archivare, sondern auch Justitiare und die Mitarbeiter des redaktionellen, kaufmännischen und technischen Bereichs einschließlich der Hilfspersonen, wie der Stenotypistin, dem Setzergehilfen und Volontären, soweit sie aufgrund ihrer beruflichen Stellung von der Person des Verfassers, Einsenders oder Gewährsmann oder dem Inhalt der gemachten Mitteilung Kenntnis erlangt haben können[197].

b) Gehilfenregelung des § 53a StPO

In den meisten Fällen sind nicht nur die in § 53 StPO genannten Berufsgeheimnisträger mit den vertraulich gemachten Informationen befasst, sondern auch das von ihnen beschäftigte Personal[198]. Um eine Umgehung von § 53 StPO durch die Vernehmung von Personen, die für den privaten Berufsgeheimnisträger arbeiten, zu verhindern, weitet § 53a StPO das Zeugnisverweigerungsrecht auf seine Gehilfen und die bei ihm zum Zwecke der Vorbereitung auf ihren Beruf tätigen Personen

---

192 BT-Drucks. 7/1261 S. 15.

193 *Meyer-Goßner* § 53 Rn. 22; LK-*Schünemann* § 203 Rn. 67.

194 Vgl. für die Mitglieder des Europäischen Parlaments § 6 EuAbgG.

195 *Meyer-Goßner* § 53 Rn. 24.

196 *Meyer-Goßner* § 53 Rn. 26.

197 LR-*Dahs* § 53 Rn. 51.

198 Vgl. z. B. das Zeugnisverweigerungsrecht einer Rechtsanwaltsfachangestellten hinsichtlich der Frage, ob eine Mandatierung durch eine bestimmte Person vorliegt, LG Dresden NJW-RR 2008, 62 f.; LG Dresden NJW 2007, 2789 f.

aus[199]. Zu den Gehilfen zählen bspw. die Sekretärin, die Sprechstundenhilfe[200], rechtskundige Mitarbeiter des Rechtsanwalts und das Kanzleipersonal[201]. Entscheidend für die Gehilfeneigenschaft ist, dass die betreffende Person dem Berufsgeheimnisträger unmittelbar unterstützend zuarbeitet[202]. Dazu gehören auch ehrenamtliche und nur gelegentlich tätige Helfer, weshalb Familienangehörigen und insbesondere der mithelfenden Ehefrau ein Zeugnisverweigerungsrecht zustehen kann[203]. An dem Kriterium des unmittelbaren Zusammenhangs mit der berufsmäßigen Tätigkeit fehlt es dagegen regelmäßig bei Reinigungskräften, Pförtnern, Boten, Hausangestellten und Chauffeuren[204]. Ihre Dienstleistungen mögen für den reibungslosen Geschäftsablauf zwar unentbehrlich sein, doch kommen sie dadurch nicht mit den Tatsachen der Mandanten, Klienten, Patienten etc. unmittelbar in Berührung. Ohne das Erfordernis eines unmittelbaren Zusammenhangs würde aufgrund der arbeitsteiligen Organisation der meisten Unternehmen die Ausdehnung des Zeugnisverweigerungsrechtes des § 53a StPO ins Uferlose führen. Daher fallen externe Zulieferer- und Dienstleistungsbetriebe wie bspw. Schreibdienste und Buchführungsstellen in der Regel nicht unter den Gehilfenbegriff des § 53a StPO[205].

Schließlich statuiert § 53a StPO ein Zeugnisverweigerungsrecht für Personen, die bei einem Berufsgeheimnisträger zur Vorbereitung ihres Berufes tätig sind. Dazu zählen bspw. die Rechtsreferendare, der famulierende Medizinstudent und die Lehrschwester im Krankenhaus[206].

Die Hilfspersonen haben kein selbständiges, sondern nur ein von dem Berufsträger abgeleitetes Zeugnisverweigerungsrecht[207]. Über die Ausübung des Zeugnisverweigerungsrechts entscheidet nach § 53a I S. 2 StPO der Berufsgeheimnisträger, weil er alleine in der Lage ist, die Tragweite der Aussage richtig zu beurteilen[208]. Weigert sich der Gehilfe trotz einer entsprechenden Anweisung durch den Berufsgeheimnisträger auszusagen, so kann das Gericht – wie bei jedem anderem Zeugen, der seine Pflichten verletzt – die Zwangs- und Beugemittel des § 70 StPO anwenden[209]. Im umgekehrten Fall, in dem die Hilfsperson aussagt,

---

199 *Meyer-Goßner* § 53a Rn. 1; KK-*Senge* § 53a Rn. 1; LR-*Dahs* § 53a Rn. 1.

200 *Meyer-Goßner* § 53a Rn. 5; LR-*Dahs* § 53a Rn. 6.

201 LR-*Dahs* § 53a Rn. 4; *Meyer-Goßner* § 53a Rn. 4.

202 KK-*Senge* § 53a Rn. 2.

203 Dies ist im Strafrecht bei dem entsprechenden Tatbestand des § 203 III S. 2 StGB nicht unstreitig, weil dieses Gesetz insoweit von berufsmäßig tätigen Gehilfen spricht, vgl. *Lackner/Kühl* § 203 Rn. 11b, MK-StGB-*Cierniak* § 203 Rn. 116; a. A. Schönke/Schröder-*Lenckner* § 203 Rn. 64; LK-*Schünemann* § 203 Rn. 82; *Tröndle/Fischer* § 203 Rn. 21; Maurach/Schröder/Maiwald BT 1 § 29 III Rn. 37; differenzierend SK-StGB-*Hoyer* § 203 Rn. 49.

204 *Meyer-Goßner* § 53a Rn. 2.

205 Anders u. U. bei der Beauftragung eines Computerserviceunternehmens, LK-*Schünemann* § 203 Rn. 41; LR-*Dahs* § 53 a Rn. 3.

206 KK-*Senge* § 53a Rn. 5.

207 BGH 9, 61.

208 LR-*Dahs* § 53a Rn. 8.

209 KK-*Senge* § 53a Rn. 6.

obwohl ihr das von dem Berufsgeheimnisträger untersagt wurde, ist die Aussage vom Gericht verwertbar[210]. Der Verstoß gegen die Weisung des Berufsträgers kann jedoch arbeitsrechtliche und u. U. wegen Verstoßes gegen § 203 III S. 2 i. V. m. Absatz I StGB strafrechtliche Konsequenzen haben.

c) Private und öffentliche Träger von Berufsgeheimnissen

Grundsätzlich könnten Berufsgeheimnisträger nicht nur die in § 53 StPO genannten Personen, sondern auch die in § 203 StGB und § 54 StPO aufgeführten Berufsgruppen sein. Für eine Beschlagnahme von elektronisch gespeicherten Daten kann es aber nur darauf ankommen, wer nach der StPO als Träger von Berufsgeheimnissen anzusehen ist, weil die Tatbestände des StGB nicht unmittelbar auf die StPO übertragbar sind. Zwar weisen die Tatbestände des § 203 StGB und des § 53 StPO Übereinstimmungen hinsichtlich ihrer persönlichen und sachlichen Reichweite auf, so dass teilweise von den gleichen Voraussetzungen auszugehen ist, doch kann dies nicht darüber hinwegtäuschen, dass für die strafprozessuale Maßnahme der Beschlagnahme nur Tatbestände der StPO maßgeblich sind. Auf § 203 StGB kommt es folglich nicht an.

Wenn aber für die Beschlagnahme von elektronisch gespeicherten Daten grundsätzlich nur Tatbestände der StPO Bedeutung erlangen, müsste untersucht werden, ob auch die in § 54 StPO genannten Richter, Beamte und anderen Personen des öffentlichen Dienstes Träger von Berufsgeheimnissen sind. Diese wohl zu bejahende Frage kann aber dahingestellt bleiben, weil es darauf entsprechend dem Titel der vorliegenden Arbeit nicht ankommt. Danach kommt es ausschließlich auf die Beschlagnahme von elektronisch gespeicherten Daten bei privaten Trägern von Berufsgeheimnissen an. Privat bedeutet, dass die Träger von Berufsgeheimnissen der Privatwirtschaft und damit gerade nicht dem öffentlichen Dienst zuzurechnen sind. Dieses Kriterium erfüllen jedoch nach dem Vorstehenden nur die in § 53 I StPO genannten Berufsgruppen[211].

d) Ergebnis

Private Träger von Berufsgeheimnissen sind die in § 53 I StPO aufgeführten Berufsgruppen sowie die nach § 53a StPO genannten Hilfspersonen.

IV. Zusammenfassung

In diesem Kapitel wurden die Grundbegriffe für die Beschlagnahme von elektronisch gespeicherten Daten bei privaten Trägern von Berufsgeheimnissen untersucht. Im Abschnitt I. wurden dazu die Begriffe der „elektronisch gespeicherten Daten“ analysiert. Es wurde festgestellt, dass diese Begriffe in der Informatik und

---

[210] KK-*Senge* § 53a Rn. 8.

[211] Dies ist für Abgeordnete gemäß § 53 I Nr. 4 StPO durchaus zweifelhaft. Sie haben jedoch eine Sonderstellung, da sie als Teil der Legislative nicht Teil des Öffentlichen Dienstes sind.

der Rechtswissenschaft unterschiedlich beurteilt werden[212]. Die Informatik versteht unter solchen Daten die unkörperliche Repräsentation von Informationen, die von Mikrochips verarbeitet werden können, was regelmäßig nur auf digitale Daten zutrifft[213]. Die Strafprozessordnung verwendet den Datenbegriff im Gegensatz dazu wesentlich umfassender und erfasst auch analoge und manuelle Angaben[214].

Da elektronisch gespeicherte Daten unkörperlich sind, bedarf es zu ihrer dauerhaften Fixierung eines Datenträgers (Speichermediums). Dieser Datenträger kann u. U. Bestandteil einer EDV-Anlage sein. Daher wurde in Abschnitt II. auf die für eine Beschlagnahme potentiell in Betracht kommenden Beweisgegenstände eingegangen, weil eine genaue Bestimmung des Beschlagnahmegegenstandes für die weitere Untersuchung entscheidend für die Beantwortung der Frage ist, ob eine Beschlagnahme rechtmäßig ist oder gegen den Verhältnismäßigkeitsgrundsatz verstößt. Untersucht wurden zunächst die Speichermedien[215], die sich nach elektronischer, magnetischer, optischer und einer Kombination dieser Speicherungsarten unterscheiden lassen. Daran schloss sich die Erörterung der EDV-Anlagen an. Es wurde aufgezeigt, dass EDV-Anlagen keineswegs nur mit Personalcomputern gleichzusetzen sind, sondern darunter eine Vielzahl von Geräten zu verstehen ist, die auf der Basis von Mikrochips arbeiten[216]. Für die weitere Untersuchung sind aber nur der PC, das Mobiltelefon und der PDA von Interesse, da diese typischerweise von privaten Trägern von Berufsgeheimnissen zur Datenarchivierung und Datenbearbeitung verwendet werden. Schließlich wurde skizziert, welche Probleme sich bei dem Zugriff auf lokal[217] und global gespeicherte elektronische Datenbestände[218] ergeben können. Dazu wurde für lokale Daten zwischen Einzel- und Mehrplatzsystemen unterschieden und bei den globalen Daten zwischen national und international zugänglichen Datenbeständen getrennt.

In Abschnitt III. erfolgte die Untersuchung der Begriffe der „privaten Träger von Berufsgeheimnissen“. Es wurde festgestellt, dass eine Legaldefinition hierfür weder im Strafgesetzbuch noch in der Strafprozessordnung enthalten ist[219]. Daher musste zunächst der Geheimnisbegriff erörtert werden. In Betracht kamen dazu vor allem § 203 StGB und § 53 StPO. Beide Tatbestände regeln den Umgang mit Geheimnissen für bestimmte Berufsgruppen. Da es sich bei der Beschlagnahme allerdings um eine strafprozessuale Zwangsmaßnahme handelt, musste nur § 53 StPO eingehend untersucht werden, weil Tatbestände des StGB für die StPO grundsätzlich nicht maßgeblich sind. Berufsgeheimnisse i. S. des § 53 StPO sind daher nicht nur Privatgeheimnisse des Mandanten, Patienten, Klienten usw., sondern auch sonstige allgemein bekannte Tatsachen, wenn sie der Betreffende in Ausübung seiner beruflichen Rolle erlangt hat[220]. Neben den Berufsgeheimnisträ-

212 B I.
213 B I 1 e).
214 B I 2.
215 B II 1.
216 B II 2.
217 B II 3 a).
218 B II 3 b).
219 B III.
220 B III 1.

gern zählen zu den privaten Trägern von Berufsgeheimnissen auch deren Hilfspersonen nach § 53 a StPO[221]. Der in § 54 StPO genannte Personenkreis gehört hingegen nicht mehr zu den privaten Berufsgeheimnisträgern, da es sich bei ihnen um Richter, Beamte und andere im öffentlichen Dienst Beschäftigte und somit nicht um Personen aus der Privatwirtschaft handelt.

[221] B III 3 b).

http://www.springer.com/978-3-540-88748-5

Die Beschlagnahme elektronisch gespeicherter Daten
bei privaten Trägern von Berufsgeheimnissen
Korge, T.
2009, XVII, 173 S., Softcover
ISBN: 978-3-540-88748-5