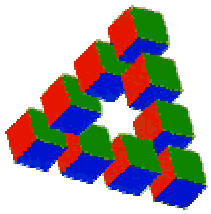
Dieter Kochheim



Durchsuchung und Beschlagnahme.

Verfahrensrecht des Ermittlungsverfahrens

Hannover, 18.05.2003

Vorbemerkung

Seit dem Ende der achtziger Jahre haben sich die Anforderungen an die Bearbeitung von Wirtschaftsstrafsachen deutlich geändert. Diesen Zeitraum überblicke ich aufgrund eigener praktischer Erfahrungen. Die Änderungen betreffen nicht nur die Erscheinungsformen der Wirtschaftskriminalität, sondern vor allem die Anforderungen an die Ermittlungsbeamten, mit einer strenger gewordenen und strenger werdenden Rechtsprechung umzugehen, neue Informations- und Kommunikationstechniken zu nutzen und wegen ihrer Beweismittelbedeutung zu beurteilen.

Das zentrale Instrumentarium für die Ermittlungen in Wirtschaftsstrafsachen ist sicherlich die Durchsuchung mit der abschließenden Beschlagnahme von Geschäftsunterlagen, anderen Beweisstücken (z.B. Raubkopien und Datenträger) und Vermögenswerten für die Rückgewinnungshilfe für Geschädigte.

Die hier zusammengestellten Texte betreffen in ihrem Schwerpunkt die Beweismittelbehandlung im Ermittlungsverfahren, wobei neben den Praxisproblemen bei der Durchsuchung und Beschlagnahme auch die Besonderheiten im Umgang mit elektronischen Daten in den Vordergrund gerückt werden. Ausgeklammert habe ich die Aspekte der Vermögensermittlungen mit den Zielen der Einziehung, des Verfalls, der Rückgewinnungshilfe und der Verfolgung von Geldwäsche und Korruption. Wegen dieser Themen sind andere Kollegen berufen, die seit etlichen Jahren erfolgreich in diesen Ermittlungssparten arbeiten und tiefe praktische Erfahrungen gesammelt haben, die mir fehlen.

Die Texte dieser Sammlung entstammen dem www.**EDV-Workshop**.de und wurden für diese Publikation so überarbeitet, dass ihr Zusammenhang deutlich wird. Dadurch ist zwar kein in sich geschlossenes Werk, jedoch eine strukturierte Materialsammlung entstanden.

Mein zentrales Publikationsmedium ist und bleibt die Website „CyberFahnders EDV-Workshop“. Als Internetprojekt muss es sich auf die Abhandlung einzelner knapp gehaltener Themen beschränken; dies leistet vor allem das ***Lexikon*** im EDV-Workshop. Schon die Bereitstellung von Aufsätzen mit bis zu 40 oder 50 Seiten Drucktext in den ***Themen*** des EDV-Workshops widerspricht dem Bedürfnis von Internetnutzern an kurzen und einfach zugänglichen Texten. Sie haben nur deshalb eine Berechtigung, weil sie mit vielen internen Links (zielgerichtete Querverweise) und externen Links zu Quellen an anderen Stellen des Internets versehen sind und zudem über ausgefeilte Navigationshilfen verfügen, die von einer Gesamtübersicht (Sitemap), über Navigationsseiten bis hin zu einer Suchwortrecherche verfügen.

Den besonderen Charme von HTML-Seiten mit ihren Hyperlinks zu anderen Stellen des eigenen Angebots und besonders zu externen Quelle (und sei es auch nur, um einen behandelten Gesetzestext anzeigen zu können) kann eine auf den Druck optimierte Publikation wie vorliegende nicht erreichen. Eine Optimierung der Druckversion hätte ich dadurch erreichen können, dass ich ein eigenes Inhaltsverzeichnis und ein aufwändiges Bezugssystem entwickelt hätte. Das ist der Angelpunkt: „aufwändig“. Mein vorrangiges Interesse (meines Hobby) ist die Website selber, die ich auf den aktuellen Stand zu halten und mit interessanten Neuerungen zu

erweitern versuche. Die vorliegende Textsammlung ist eine Momentaufnahme, die neben dem anderen (Haupt-) Projekt nicht weiter gepflegt und aktualisiert werden kann.

Der EDV-Workshop stellt Informationen und Werkzeuge für Ermittler bereit, die das Internet für ihre Recherchen nutzen wollen. Er EDV-Workshop wird seit Januar 2000 im Internet präsentiert und bietet Linklisten, Aufsätze und ein Lexikon - alles mit dem Schwerpunkt Strafverfahrens-, Straf- und Telekommunikations-/Multimediarecht und -technik. Die hier dokumentierten Texte finden Sie dort mit vielen ergänzenden Quer- und Verweisen zu fremden Quellen.

Dieter Kochheim

Autor

Bis 2001 war ich als Staatsanwalt in der Zentralstelle für Wirtschaftsstrafsachen der Staatsanwaltschaft Hannover tätig. Seit Dezember 2001 leite ich die IuK-Stelle (Informations- und Kommunikationstechnik) der Generalstaatsanwaltschaft Celle. Diese Stelle ist zuständig für den strategischen Einsatz der EDV- und Netztechnik für den geschäftsmäßigen Betrieb aller Staatsanwaltschaften in Niedersachsen.

Seit 1991 unterrichte ich in Fortbildungsmaßnahmen der Polizei, Steuerfahndung und Justiz.

Als "CyberFahnder" betreibe ich seit Januar 2000 die Website EDV-Workshop.

Themenüberblick

CyberFahnders EDV-Workshop

Teil 1: Strafverfahren

Durchsuchung und Beschlagnahme

Die §§ 94 ff. StPO regeln die Zwangsmaßnahmen zur Sicherung und Erlangung von Beweisen, Verfalls- und Einziehungsgegenständen, zur Ergreifung des Beschuldigten - und im Fall des § 111a StPO (Vorläufige Entziehung der Fahrerlaubnis) - zur Vorwegnahme von Urteilsfolgen. Ergänzt werden diese Vorschriften um die Regelungen zur Rückgewinnungshilfe (§ 111b StPO) [1].

Alle genannten Zwangsmaßnahmen stellen Eingriffe in den grundrechtlich geschützten Privatbereich des Beschuldigten oder dritter Personen dar. Dies zwingt in jedem Fall auch zur Abwägung zwischen der Eingriffsintensität und dem Vorgehen einerseits sowie der Bedeutung der Ermittlungshandlung andererseits, also zur Anwendung des Verhältnismäßigkeitsgrundsatzes [2].

Zu den Begriffen:

Die Einsichtnahme in Räumlichkeiten oder sonstige Sachen ist solange keine Durchsuchung, wie sie freiwillig gestattet wird. **Durchsuchung** ist nur die zwangsweise Inaugenscheinnahme zum Zweck des Auffindens von Gegenständen, die der Beschlagnahme unterliegen. **Nachschau** ist die Inaugenscheinnahme, die ausschließlich dem Auffinden des Beschuldigten dient (§ 103 Abs. 1 S. 1 StPO).

Jede Entgegennahme von Beweismitteln durch Ermittlungsbeamte ist eine amtliche Inverwahrnahme, also bereits eine **Sicherstellung** (§ 94 Abs. 1 StPO). In jedem Fall sollte deshalb ein Verzeichnis über die sichergestellten Gegenstände angelegt werden.

Gerade in umfangreichen Verfahren bereitet es Schwierigkeiten, nach Abschluss des gerichtlichen Verfahren alle Sicherstellungsgegenstände, die Jahre vorher zu den Vorgängen gelangt sind, sicher den letzten Gewahrsamsinhabern zuzuordnen. Sicherstellungsverzeichnisse sollten deshalb in geeigneten Fällen auch angelegt werden, wenn z.B. ein Zeuge im Rahmen seiner Vernehmung Schriftstücke übergibt. In solchen Großverfahren kann es sich darüber hinaus empfehlen, ein eigenständiges "Sicherstellungsheft" anzulegen, das eine Kontrolle über den Verbleib sichergestellter Gegenstände erleichtern kann. [3]

Eine Beschlagnahme findet nur bei der nicht freiwilligen Herausgabe statt (§ 94 Abs. 2 StPO) und stellt eine zwangsweise, förmliche Sicherstellung und damit eine zwangsweise Überführung des Gegenstandes in den amtlichen Gewahrsam dar.

---

[1] Dieser Text beruht auf dem Arbeitspapier "Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen" aus dem Jahr 1996. Er wurde für das Lexikon des EDV-Workshops im Oktober 2002 überarbeitet und aktualisiert.

[2] ständige Rechtsprechung des Bundesverfassungsgerichts, z.B. BVerfG NJW 91, 690 f.; NStZ 92, 91 ff.

[3] Siehe auch den Beitrag über die Aktenführung im Teil 3

Beschlagnahmefähig sind nur solche Gegenstände, die eine **potentielle Beweisbedeutung** haben (§ 94 Abs. 1 StPO). Das heißt, dass der Gegenstand grundsätzlich - zulässigerweise - zu Untersuchungszwecken verwendet werden kann und hierzu geeignet ist. Bei der Inverwahrnahme braucht aber die Beweisführung im einzelnen noch nicht feststehen. An einer Beweisbedeutung fehlt es jedenfalls dann, wenn voraussehbar ist, dass es zu keinem Gerichtsverfahren kommen wird. Gleichwohl ist eine Beschlagnahme auch nicht ausgeschlossen, soweit noch behebbare Verfahrenshindernisse bestehen, wie z.B. bei fehlenden Strafanträgen.

Untersuchung ist das gesamte Ermittlungs- und Strafverfahren mit Ausnahme der Vollstreckung.

Eine **Sicherstellung in anderer Weise** (§ 94 Abs. 1 StPO) erfordert eine förmliche Beschlagnahme. So können Grundstücke, Gebäude und Räume durch Absperrung, Versiegelung und einem Verbot zum Betreten gesichert werden. Auch sonstige Gegenstände können z.B. durch ein Verbot zur Herausgabe, Vernichtung oder Verfügung in "anderer Weise" sichergestellt werden. Hingegen ist bei Schriftstücken die Anfertigung von Ablichtungen gegen Herausgabe des Originals ein Sicherstellungsersatz (Sicherstellungssurrogat) und keine Sicherstellung in anderer Weise.

Sicherstellungssurrogate haben einen geringeren Beweiswert als die Originaldokumente. Im Rahmen der Verhältnismäßigkeitsprüfung kann sich ein Verzicht auf die Sicherstellung der Originale dann anbieten, wenn ihr Beweiswert nicht stark von dem des Surrogats abweicht. Physikalisch-technische Untersuchungen auf Fingerspuren oder am Material (Papier und Schreibpasten) lassen sich hingegen nur am Original vornehmen. Im Zweifel sind deshalb die Originale sicherzustellen.

Grundsätzlich gilt, dass Beweiserhebungsverbote nicht zwangsläufig zu Beweisverwertungsverboten führen. In Extremfällen können jedoch die bei einer Durchsuchung beigezogenen Beweismittel einem Verwertungsverbot unterliegen und müssen zurückgegeben werden, wenn die prozessualen Verstöße bei der Abfassung des Durchsuchungsbeschlusses oder der Durchführung der Durchsuchung so schwerwiegend gewesen sind, "dass nach Abwägung aller Umstände das Interesse des Staates an der Tataufklärung gegenüber dem Interesse des betroffenen Bürgers am Schutz seiner Persönlichkeitssphäre zurücktreten muss". Diese Entscheidung ist lange Zeit ein Einzelfall geblieben [4]. Erst 2002 hat das Bundesverfassungsgericht dann ein Verwertungsverbot bei beschlagnahmten Zufallsfunden angenommen, wenn die zugrunde liegende Durchsuchungsanordnung rechtswidrig war [5].

Hinzuweisen ist auch auf den Ermittlungsrichter beim BGH [6], der den Generalbundesanwalt verpflichtet hat, die weitere Sichtung nach § 110 StPO abzubrechen und die

---

4 LG Wiesbaden StV 88, 292 f.

5 Eine solche "systematische Suche nach Zufallsfunden" ist von der Rechtsprechung und Literatur schon seit Jahrzehnten als Rechtswidrig bezeichnet worden. Warum bedurfte es überhaupt einer Entscheidung des BverfG?

6 Ermittlungsrichter BGH StV 88, 90; diese Entscheidung gilt insbesondere für das Sichtungsverfahren gemäß § 110 StPO; siehe unten "Sichtung gemäß § 110 StPO. Papiere und Daten"

vorläufig sichergestellten Computerdisketten unausgewertet herauszugeben.

Durchsuchungsvoraussetzungen

Die §§ 102 und 103 StPO gestatten die Durchsuchung von Wohnungen, Räumen, Person und Sachen des Verdächtigen oder anderer Personen.

Dabei setzt die Durchsuchungsanordnung gegen den Verdächtigen nach § 102 StPO voraus, dass aufgrund bestimmter Anhaltspunkte die Wahrscheinlichkeit besteht, dass eine bestimmte Straftat bereits begangen wurde und nicht etwa bloß straflos vorbereitet worden ist. Es reicht der einfache Tatverdacht aus, so dass es in diesem Fall nicht erforderlich ist, den Betroffenen formell als Beschuldigten zu behandeln (vergleichbar der Verdächtigeneigenschaft nach § 55 StPO; diese macht aber bereits eine Belehrung über das Auskunftsverweigerungsrecht erforderlich). Um einen "förmlichen" Beschuldigten handelt es sich erst, wenn gegen ihn das Ermittlungsverfahren von der Polizei oder von der Staatsanwaltschaft förmlich eingeleitet wurde. Nur dann, wenn eine Strafanzeige oder ein Strafantrag vorliegt, muss der bezeichnete Verdächtige auch von vornherein als Beschuldigter behandelt werden.

Solange eine Mehrzahl von Verdächtigen besteht, unterliegt zum Beispiel die "informatorische Befragung" (am Unfallort, in einer Firma oder Behörde zur Feststellung der "Verantwortlichen") den Anforderungen einer Zeugenvernehmung. Seit dem Beschluss des BGH vom 27.02.1992 - 5 StR 190/91 - sind jedoch erhöhte Anforderungen an die Belehrung (§§ 136 Abs. 1 S. 2 i.V.m. 163a Abs. 4 S. 2 StPO) gesetzt worden: Ist der Vernehmung des Beschuldigten, so heißt es in den Leitsätzen, durch einen Polizeibeamten kein Hinweis darauf vorausgegangen, dass es dem Beschuldigten freistehe, sich zu der Beschuldigung zu äußern oder nicht zur Sache auszusagen, so dürfen Äußerungen, die der Beschuldigte in dieser Vernehmung gemacht hat, auch nicht verwertet werden. Dies gilt aber nicht, wenn feststeht, dass der Beschuldigte sein Recht zu schweigen ohne Belehrung gekannt hat, wenn der nicht von einem Rechtsanwalt vertretene Angeklagte vom Gericht belehrt wird, wenn der verteidigte Angeklagte in der Hauptverhandlung ausdrücklich der Verwertung zustimmt oder ihr nicht bis zu dem in § 257 StPO genannten Zeitpunkt widersprochen hat (unmittelbar nach Vernehmung der Polizeibeamten, die über den Vernehmungsinhalt aussagen).

Für den Inhalt des Durchsuchungsbeschlusses oder der Durchsuchungsanordnung bei Gefahr in Verzug folgt daraus, dass zwar immer ein durch tatsächliche Anhaltspunkte begründeter Tatverdacht bestehen muss, der Tatvorwurf gegen den Verdächtigen aber noch nicht im einzelnen konkretisiert werden braucht oder durch andere Beweismittel konkret belegt ist. Es empfiehlt sich aber in den meisten Fällen, zu Beginn der Durchsuchung den Grund der Maßnahme und eine allgemeine Belehrung über das Schweigerecht vorzunehmen. Dies ist in den Akten zu vermerken, damit später keine Zweifel darüber entstehen. Einer wiederholten Belehrung bedarf es hingegen nicht.

Die weitere Voraussetzung ist, dass Anhaltspunkte nach kriminalistischer Erfahrungen die Vermutung rechtfertigen, dass der Zweck der Durchsuchung erreicht werden kann. Dabei ist der "Zweck der Durchsu-

chung" vom Untersuchungsgegenstand bestimmt und darauf beschränkt, welche Beweismittel nach kriminalistischer Erfahrung bei dem Verdächtigen im Zusammenhang mit der Tat, wegen der die Ermittlungen eingeleitet wurden und für die konkrete Anhaltspunkte bestehen, gefunden werden könnten. Zur bloßen Ausforschung oder allein mit dem Ziel, Zufallsfunde zu erreichen, darf die Durchsuchung nicht durchgeführt werden.

Die Durchsuchung bei dem unbeteiligten Dritten gemäß § 103 StPO stellt strengere Anforderungen als die Durchsuchung bei dem Verdächtigen. Zu ihrer Anordnung reichen nicht nur die kriminalistischen Erfahrungswerte aus, dass die Durchsuchung Erfolg haben wird, sondern es müssen tatsächliche Anhaltspunkte dafür vorliegen, dass bestimmte Beweisgegenstände (oder der Beschuldigte, nicht nur Verdächtige) beim Betroffenen zu finden sind.

Eine Durchsuchung bei strafunmündigen Personen, also bei Kindern vor vollendetem 14. Lebensjahr oder bekanntermaßen infolge Krankheit nicht zurechnungsfähigen Personen, ist nur unter den strengeren Voraussetzungen des § 103 StPO zulässig. Ähnliche Einschränkungen gelten auch für Abgeordnete: Eine Durchsuchung gemäß § 103 StPO beim tatunverdächtigen Abgeordneten ist (genauso wie die Beschlagnahme) uneingeschränkt erlaubt, die beim verdächtigen Abgeordneten nur unter den strengen Voraussetzungen für den Verdacht und die Erfolgserwartung nach § 103 StPO und dann erlaubt, wenn die Beschränkungen des Art. 46 Abs. 1 GG nicht durchgreifen.

Die Durchsuchung von Wohnungen, Geschäftsräumen und befriedeten Besitztümern darf gemäß § 104 StPO grundsätzlich nicht zur Nachtzeit erfolgen, es sei denn, sie dient der Verfolgung auf frischer Tat, zur Wiederergreifung eines Gefangenen oder ist wegen Gefahr im Verzug geboten. Nach einer Entscheidung des Bundesverfassungsgerichts darf eine schon begonnene Durchsuchung während der Nachtzeit fortgesetzt werden. Dieselbe Entscheidung bestimmt aber auch, dass die Durchsuchungen so frühzeitig begonnen werden sollen, dass sie erfahrungsgemäß bis zur Nachtzeit abgeschlossen sein werden.

Zufallsfunde dürfen gemäß § 108 StPO gleichermaßen beim Verdächtigen wie beim Unverdächtigen beschlagnahmt werden. Die Voraussetzung ist nur, dass diese Gegenstände auf die Verübung einer anderen Straftat hindeuten; diese muss noch nicht im einzelnen konkretisierbar sein.

Besondere Bestimmungen enthält § 103 Abs. 2 StPO. Die Räume, in denen der Beschuldigte ergriffen wurde oder die er während der Verfolgung betreten hat, dürfen mit dem Zweck, Beweismittel zu sichern, auch durchsucht werden, ohne dass konkrete Anhaltspunkte für das Vorhandensein bestimmter Beweismittel vorliegen müssen; das Ziel darf sich darauf beschränken, Personen aufzufinden, die als Zeugen in Betracht kommen.

Nur zum Zweck des Auffindens von Beschuldigten, die einer Straftat nach § 129a StGB oder einer dort bezeichneten Straftat verdächtig sind, dürfen auch ganze (aus mehreren Wohnungen bestehende) Gebäude nach § 103 Abs. 1 S.2 StPO durchsucht werden. In diesem Fall ist die Beschlagnahme von Zufallsfunden ausgeschlossen. Werden aber Gegenstände gefunden, die als Beweismittel für eine konkrete andere Straftat von potentieller Beweisbedeutung

sind, so kann gemäß § 94 StPO deren Beschlagnahme angeordnet werden (z. B. bei "herrenlosen" Schusswaffen, Tatbeute, BtM).

Die körperliche Durchsuchung der Person des Unverdächtigen ist ebenso zulässig wie die des Verdächtigen. Für weitergehende Spurensicherungen sind die Voraussetzungen der §§ 81a (körperliche Untersuchung), 81b (erkennungsdienstliche Behandlung) und 81c StPO einzuhalten. § 81d StPO, wonach körperliche Untersuchungen einer Frau, die das Schamgefühl der Frau verletzen können, nur von einer Frau (oder einem Arzt) durchgeführt werden dürfen, gilt auch für die körperliche Durchsuchung nach §§ 102, 103 StPO. Grundsätzlich dürfen andererseits auch nur Männer von Männern körperlich untersucht werden. Zur Durchführung der körperlichen Durchsuchung darf im Zweifel auch körperlicher Zwang angewendet werden und wenn es geboten erscheint, darf der Betroffene auch kurzfristig festgenommen und auf der Wache durchsucht werden.

Durchsuchungsanordnung

Grundsätzlich werden Durchsuchungen vom Richter angeordnet. Bei Durchsuchungsbeschlüssen, in denen zugleich mit der Durchsuchungsanordnung auch die Beschlagnahme bestimmt wird, ist zu beachten, dass nur solche Gegenstände beschlagnahmt werden können, die individuell und unverwechselbar und vollständig beschrieben werden können. So ist zwar ein bestimmter Kraftfahrzeugbrief oder eine bestimmte Vertragsurkunde im voraus individualisierbar, nicht aber die nicht näher beschriebene "Firmenbuchführung", weil diese Formulierung Zweifel darüber offen lässt, ob Gegenstände von der Beschlagnahme erfasst sind oder nicht [7] und nicht sichergestellt ist, dass der Eingriff in die Grundrechte messbar und kontrollierbar bleibt [8]. Ist die Beschlagnahmeanordnung unbestimmt, so ist sie auch unwirksam [9]. In diesem Fall umgrenzt die Nennung von Beweismitteln zwar den Umfang der erlaubten Durchsuchung. Im Zweifelsfall muss der Durchsuchungsbeamte aus eigener Anordnungsbefugnis prüfen, ob Gefahr im Verzug besteht, und die Beschlagnahme zum Abschluss der Durchsuchung selber bestimmen.

Bei Gefahr im Verzug sind die Staatsanwaltschaft oder ihre Hilfsbeamten auch zur Anordnung der Durchsuchung berechtigt (§ 105 Abs. 1 StPO). Gefahr im Verzug besteht nach dem eigenen pflichtgemäßen Ermessen des Beamten dann, wenn eine richterliche Anordnung nicht eingeholt werden kann, ohne dass der Zweck der Maßnahme gefährdet wird [10].

Keiner Anordnung bedarf es, wenn sich der Betroffene der Maßnahme freiwillig unterzieht. Eine ausdrückliche, eindeutige und aus freiem Entschluss erteilte Einwilligung macht auch die Anordnung körperlicher Untersuchungen entbehrlich und ermöglicht gesundheitsbeeinträchtigende Eingriffe (§§ 81a, 81c StPO).

Bei jeder Durchsuchung soll, wie bei allen anderen strafprozessualen Maßnahmen

---

7 BVerfG NStZ 92, 91, 92

8 BVerfG NJW 94, 3281, 3282

9 OLG Düsseldorf StV 82, 513; BVerfG NStZ 92, 91, 92

10 zur aktuellen Rechtsprechung des Bundesverfassungsgerichts siehe unten "Gefahr im Verzug, Durchsuchungsanordnung"

auch, erfragt werden, ob sie freiwillig geduldet werden.

Durchführung der Durchsuchung

Der Umfang der Durchsuchung richtet sich nach den Beweismitteln, die als gesuchte Gegenstände im Durchsuchungsbeschluss bezeichnet sind. Darüber hinaus ist das Gericht auch berechtigt, die Art und Weise, die einzelnen Orte und die Zeit einer Durchsuchung zu regeln [11]. Die Durchsuchungspersonen haben auch noch während der Durchsuchungsmaßnahme zu prüfen, ob sich die sachliche Entscheidungsgrundlage so maßgeblich geändert hat, dass sich eine weitere Vollstreckung verbietet.

Nach einer Entscheidung des Bundesverfassungsgerichts [12] können auch abgeschlossene Durchsuchungsmaßnahmen richterlich überprüft werden. Das Gericht verlangt eine wirkliche Kontrolle von grundrechtseingreifenden Maßnahmen und spricht deshalb nach den Grundsätzen der Rechtsweggarantie aus Art. 19 Abs. 4 GG den Betroffenen das Recht zu, "in Fällen tiefgreifender, tatsächlich jedoch nicht mehr fortwirkender Grundrechtseingriffe auch dann die Berechtigung des Eingriffs gerichtlich klären zu lassen, wenn die direkte Belastung durch den angegriffenen Hoheitsakt sich nach dem typischen Verfahrensablauf auf eine Zeitspanne beschränkt, in welcher der Betroffene die gerichtliche Entscheidung in der von der Prozessordnung gegebenen Instanz kaum erlangen kann".

Das BVerfG reagiert mit dieser Entscheidung auf die Besonderheiten der Durchsuchungsanordnung im Ermittlungsverfahren, die einerseits von einem erheblichen Eingriff in Grundrechte geprägt ist und andererseits - ihrer Natur nach - ohne rechtliches Gehör ergeht (§ 33 Abs. 4 StPO), so dass der Betroffene allein auf die tatsächliche Durchführung der Maßnahme mit rechtsstaatlichen Mitteln reagieren kann. Mit der richterlichen (oder staatsanwaltlichen oder polizeilichen) Eingriffsentscheidung wird er zugleich mit ihrer Durchführung konfrontiert, er kann sie nicht verhindern, kaum steuern und ist nach bisheriger Praxis sogar von der nachträglichen richterlichen Überprüfung ausgeschlossen gewesen.

Der gerichtliche Durchsuchungsbeschluss darf dann nicht mehr vollstreckt werden, wenn die zwischenzeitlich erhobenen Beweise eine andere Sachbeurteilung zulassen. Darüber hinaus ist die Staatsanwaltschaft auch berechtigt, einen Durchsuchungsbeschluss gar nicht zu vollziehen. Dieses Ermessen gilt nicht für Hilfsbeamte und auch nicht für Durchsuchungsbeschlüsse, die das Gericht nach Erhebung der Anklage im Zwischen- oder Hauptverfahren erlässt.

Das BVerfG hat auch bestimmt [13], dass ein Durchsuchungsbeschluss spätestens nach Ablauf eines halben Jahres seine "rechtfertigende Kraft", also seine Wirksamkeit verliert [14]. Zur Begründung hebt das Gericht hervor, dass der Richter eine Durchsuchung nur anordnen darf, "wenn er sich aufgrund eigenverantwortlicher Prüfung der Ermittlungen überzeugt hat, dass die Maßnahme verhältnismäßig ist". Mit zunehmendem

---

11 ausdrücklich BVerfG NStZ 92, 91, 92; BVerfG NJW 94, 3281, 3282

12 BVerfG wistra 97, 219 ff.

13 BVerfG wistra 97, 223 ff.

14 BVerfG ebd., S. 225

Zeitablauf könnte sich nicht nur die Beurteilungsgrundlage geändert haben, sondern würde "die konkrete richterliche Beschränkung des Grundrechtseingriffs zu einer Blankettermächtigung geworden" sein (BVerfG ebd.). Von dem Vollzug der Durchsuchungsanordnung könne zwar vorläufig abgesehen werden. Dies dürfe aber nicht dazu führen, "dass der Staatsanwalt sich eine Durchsuchungsanordnung gewissermaßen auf Vorrat besorgt oder diese doch vorrätig hält" [15]. Deshalb ist "spätestens nach Ablauf eines halben Jahres ... davon auszugehen, dass die richterliche Prüfung nicht mehr die rechtlichen Grundlagen einer beabsichtigten Durchsuchung gewährleistet und die richterliche Anordnung nicht mehr den Rahmen, die Grenzen und den Zweck der Durchsuchung im Sinne eines effektiven Grundrechtsschutzes zu sichern vermag" [16].

Nach Beendigung der Durchsuchung ist der Durchsuchungsbeschluss verbraucht. Für eine weitere Durchsuchung muss ein neuer erwirkt werden.

Durchsuchungen von Wohnungen, Gebäuden und befriedeten Besitztümern sollen, sofern kein Richter oder Staatsanwalt (auch Amtsanwälte, nicht aber Wirtschaftsreferenten) anwesend ist, im Beisein eines Gemeindebeamten oder von zwei Gemeindebewohnern (die keine Hilfsbeamten der Staatsanwaltschaft und auch nicht der Betroffene selber sein dürfen) durchgeführt werden. Diese Bestimmung des § 105 Abs. 2 StPO ist keine reine Formvorschrift, sondern eine "wesentliche Förmlichkeit" der Durchsuchung, die auch dem Schutz der Beamten vor unberechtigten Vorwürfen dient. "Unmöglich" ist die Zuziehung von Zeugen, wenn der eintretende Zeitverlust den Erfolg der Durchsuchung vereiteln würde. Auf die Zuziehung kann der Betroffene wirksam verzichten. Es wird aber auch - zu recht - die Meinung vertreten, dass es des ausdrücklichen Verzichts des Durchsuchungsbeamten bedarf, weil auch die Ermittlungsbeamten durch die Anwesenheit von unbeteiligten Zeugen vor unberechtigten Vorwürfen geschützt werden sollen. Im Zweifelsfall sollte auf die Anwesenheit von Durchsuchungszeugen von den Polizeibeamten nicht verzichtet werden, wenn unberechtigte Vorwürfe des Durchsuchungsbetroffenen zu erwarten sind.

Nach § 106 Abs. 1 StPO darf der Inhaber der zu durchsuchenden Räume oder Gegenstände der Durchsuchung beiwohnen. Ist er abwesend, so ist nach Satz 2 dieser Vorschrift - wenn möglich - ein Vertreter oder erwachsener Angehöriger u.a. zuzuziehen. Diese Formvorschrift ist im Gegensatz zu § 105 Abs. 2 StPO keine zwingende, sondern eine Ordnungsvorschrift.

Ist der Beschuldigte der Inhaber, kann er sich von seinem Verteidiger vertreten lassen. Verzichtet der Vertreter, brauchen keine weiteren Personen zugezogen werden. Stört der Inhaber, Vertreter usw., so kann er entfernt und "wenn möglich" durch eine der anderen Personen ersetzt werden. Ist der Beschuldigte nicht der Inhaber der Wohnung, so haben weder er noch sein Verteidiger ein Anwesenheitsrecht.

Gegen Störer bei Amtshandlungen kann der Beamte gemäß § 164 StPO die Festnahme anordnen, bis die Amtshandlung beendet ist (nicht aber über den nächstfolgenden Tag hinaus). Störer haben ihr Anwesenheitsrecht bei Durchsuchungen verwirkt. Reichen weniger einschneidende Maßnahmen aus,

---

15 BVerfG ebd.

16 BVerfG ebd., S. 226

müssen diese zunächst angewendet werden.

Nur dem Unverdächtigen steht nach § 106 Abs. 2 StPO das Recht zu, über den Zweck der Durchsuchung informiert zu werden. Wird dadurch der Untersuchungszweck nicht gefährdet, sollte auch dem Verdächtigen der Durchsuchungszweck mitgeteilt werden. Ein Recht auf die Aushändigung des Durchsuchungsbeschlusses besteht grundsätzlich nicht. In der Praxis hat sich die Aushändigung jedoch bewährt, weil der Betroffene dadurch die vollständige Beschlusslage zur Kenntnis erhält [17].

Zur Durchsicht von Papieren gegen den Willen des Betroffenen ist nur die Staatsanwaltschaft berechtigt (§ 110 Abs. 1 StPO [18]). Ohne Einwilligung ist die Durchsicht, d.h. die inhaltliche Prüfung von Schriftstücken darauf, ob sie beschlagnahmt oder zurückgegeben werden sollen, auch die sogenannte "Grobsichtung", unzulässig. Hilfsbeamte, die die Durchsuchung ohne einen Staatsanwalt durchführen, dürfen insoweit Schriftstücke nur nach äußeren Merkmalen (Aufbewahrungsort, Ordnerbeschriftung, Betreffangabe im Schreiben) danach aussondern, ob eine inhaltliche Auswertung durch den Staatsanwalt geboten erscheint [19].

In diesen Fällen ist nach § 110 Abs. 2 und 3 StPO zu verfahren: Die ausgesonderten Schriftstücke werden in einen verschlossenen Umschlag genommen und bei größeren Mengen in einen Karton. Der Umschlag wird sodann von der Polizei versiegelt und der Betroffene ist berechtigt, seinerseits einen Siegel anzubringen. Vom Staatsanwalt ist schließlich ein Termin zur Sichtung zu bestimmen, an dem der Betroffene teilnehmen darf, aber nicht teilnehmen muss. Der Sichtungstermin kann im Büro des Staatsanwalts genauso durchgeführt werden wie in anderen Räumen, z.B. denen der Polizei. Bei der Sichtung während der Durchsuchung oder im gesonderten Verfahren nach § 110 StPO kann sich der Staatsanwalt der Polizeibeamten, Dolmetscher und Sachverständigen (z.B. Wirtschaftsreferenten oder EDV-Sachständige) als "Sichtungshelfer" bedienen. In besonderen Fällen dürfen auch Mitarbeiter des Anzeigeerstatters oder Geschädigten hinzugezogen werden, wenn keine anderen sachkundigen Personen (z.B. zur Identifizierung gestohlener Gegenstände) oder Sachverständige (z.B. zu Produktionsabläufen oder chemischen Prozessen in Patentsachen) zur Verfügung stehen. Hierbei muss aber ausgeschlossen werden, dass Betriebsgeheimnisse des Betroffenen seinen Wettbewerbskonkurrenten bekannt werden oder er in unzumutbarer Weise bloßgestellt wird. Die Unparteilichkeit dieser Durchsuchungshelfer muss von den Polizeibeamten und der Staatsanwaltschaft gesichert und schon bei der Auswahl berücksichtigt werden [20].

Nach dem Abschluss der Durchsuchung (oder der Sichtung nach § 110 StPO) werden die als Beweismittel benötigten Schriftstücke in ein Sicherstellungsprotokoll aufgenommen und sichergestellt. Bei Widerspruch gegen die Sicherstellung sind die

---

17 nach meiner Auffassung handelt es sich bei der Aushändigung des Durchsuchungsbeschlusses nicht um eine Art der Akteneinsicht (§ 147 StPO), sondern um eine Zustellung (§§ 36 ff. StPO)

18 siehe den gesonderten Beitrag zur Sichtung unten

19 wegen der Einzelheiten siehe den gesonderten Aufsatz zur "Sichtung gemäß § 110 StPO"

20 OLG Hamm NStZ 86, 326 f., siehe unten "Sachverständige im Ermittlungsverfahren"

Gegenstände zu beschlagnahmen. Besteht keine Gefahr im Verzug, z.B. nach einer Sichtung nach § 110 StPO, wenn sich die Beweismittel schon - vorläufig - im amtlichen Gewahrsam befinden, ist die richterliche Beschlagnahmeanordnung einzuholen.

Bei der vorläufigen Sicherstellung nach § 110 StPO handelt es sich noch nicht um eine förmliche Beschlagnahme nach den allgemeinen Regeln der StPO, sondern um eine vorübergehende amtliche Inverwahrnahme zur Sicherung des ordnungsgemäßen Abschlusses der Durchsuchung. Im Interesse der Aktenklarheit empfehle ich, auch die "versiegelten Umschläge", wegen der die spätere Sichtung erfolgen soll, auf einem gesonderten Blatt des Sicherstellungsprotokolls zu vermerken.

Nach § 107 StPO muss dem Betroffenen auf Verlangen (sollte aber auch ansonsten regelmäßig) eine schriftliche Mitteilung über den Grund der Durchsuchung ausgestellt werden. Dabei würde bereits die abstrakte Angabe des Durchsuchungszwecks reichen (Auffinden von Beweisgegenständen). Dem Verdächtigen ist insofern auch eine Mitteilung über die zugrunde liegende Straftat zu machen. Diese Mitteilung braucht keine konkreten Einzelheiten enthalten, muss ihn aber in die Lage versetzen, den Umfang und die Art der ihm vorgeworfenen Handlungen zu erkennen.

Meine Ausführungen fußen auf den alten Entscheidungen des LG Stuttgart und des LG Oldenburg [21].

Zuletzt hat das BVerfG am 05.05.2000 - 2 BvR 2212/99 - beschlossen, dass die Beschränkung darauf, es handele sich um eine "Ermittlungssache... wegen Steuerhinterziehung", den gebotenen Anforderungen an einen richterlich gestaltenden Grundrechtseingriff nicht genügt.

Neben der "schriftlichen Mitteilung" ist auf Verlangen eine Aufstellung der beschlagnahmten Gegenstände oder eine Negativbescheinigung zu erstellen. Für die Akten muss auf jedem Fall ein genaues Verzeichnis über die sichergestellten Gegenstände erstellt werden (§ 109 StPO). Eine Durchschrift hiervon genügt den Anforderungen des § 107 StPO. Die Gegenstände selber sind ebenfalls "durch amtliche Siegel oder in sonst geeigneter Weise" zu kennzeichnen.

Beschlagnahme

Jede "amtliche Inverwahrnahme" von Beweismitteln ist eine Sicherstellung. Auch wenn z.B. im Rahmen einer Vernehmung ein Zeuge Unterlagen vorlegt, die als Originale oder Ablichtungen zu den Akten genommen werden, sollte deshalb eine Niederschrift i.S.v. § 109 StPO angefertigt werden (dient im wesentlichen der Aktenklarheit).

Nach § 94 StPO können alle als Beweismittel bedeutenden Gegenstände für die "Untersuchung" sichergestellt werden und unterliegen in dem Fall, dass sie nicht freiwillig herausgegeben werden, nach § 94 Abs. 2 StPO der Beschlagnahme. § 95 Abs. 1 StPO bestimmt als weniger einschneidendes Mittel eine Herausgabepflicht und für den Fall der Weigerung die Anordnung von Zwangsmitteln (Ordnungsgeld und Erzwingungshaft) entsprechend § 70 StPO.

"Beweismittel" sind alle beweglichen oder unbeweglichen Sachen, die unmittelbar oder mittelbar für die Tat oder die Umstände ihrer

[21] LG Stuttgart StV 86, 471 f.; LG Oldenburg wistra 87, 38

Begehung Beweis erbringen. Dazu gehören bewegliche Sachen jeder Art (auch Magnetbänder und sonstige Datenträger) und unbewegliche Sachen (auch Leichen, Leichenteile, Föten, Prothesen), also inhaltlich Tatbeute, Tatwerkzeuge, Tatprodukte und Taträume sowie Beweismittelträger, von denen die Beweise nicht oder nur schwer getrennt werden können (z.B. Kleidung mit Blut oder Sperma).
Insbesondere bei schriftlichen Unterlagen ist aus Gründen der Verhältnismäßigkeit zu prüfen, ob auf Kosten des Betroffenen eine Ablichtung als Sicherstellungsersatz zu fertigen ist. Im Zweifelsfall sind die Originale sicherzustellen.

Nach § 96 StPO sind auch Behörden zur Herausgabe der bei ihnen verwahrten Akten und Schriftstücke verpflichtet (Art. 35 Abs 1 GG; Amtshilfe). Erfolgt von deren obersten Dienstbehörde kein Sperrvermerk und wird die Herausgabe gleichwohl verweigert, darf im Einzelfall auch die Beschlagnahme und zu deren Ausführung die Durchsuchung angeordnet werden (die Durchsuchung ist gemäß § 103 StPO auch zulässig, soweit der Beschuldigte oder nicht von der Behörde verwahrte Gegenstände gesucht werden).

Zeugnisverweigerungsberechtigte Personen sind nicht zur Herausgabe verpflichtet, können also auch nicht nach § 95 Abs. 2 StPO zur Herausgabe gezwungen werden. Konkret sind aber nur die Gegenstände beschlagnahmefrei, die von § 97 StPO als solche bezeichnet werden: Schriftliche Mitteilungen zwischen Beschuldigtem und Vertrauensperson, deren Aufzeichnungen über solcherart Mitteilungen und schließlich sonstige Gegenstände, beispielsweise ärztliche Untersuchungsbefunde, Blutproben usw., soweit sie sich im Gewahrsam der zeugnisverweigerungsberechtigten Person (§§ 52, 53 StPO) befinden. Diese Einschränkungen gelten nicht, wenn die zeugnisverweigerungsberechtigte Person ihrerseits der Teilnahme, Begünstigung, Strafvereitelung oder Hehlerei an der die Untersuchung betreffenden Tat verdächtig ist.

Eine Erweiterung des Schutzbereichs findet gemäß § 148 StPO nur in dem Verhältnis zwischen Beschuldigtem und seinem Verteidiger statt: Schriftliche Mitteilungen usw. dürfen auch dann nicht beschlagnahmt werden, wenn sie sich nicht im Gewahrsam der zeugnisverweigerungsberechtigten Person befinden. Hingegen dürfen sonstige Gegenstände wie Schriftverkehr, Jahresabschlüsse, Tatwaffen usw. auch beim zeugnisverweigerungsberechtigten "Berufshelfer" beschlagnahmt werden, wenn sie nicht das Vertrauensverhältnis zwischen ihm und dem Beschuldigten betreffen. In der Hauptsache kommen solche Beschlagnahmen beim Steuerberater in Betracht, wenn sich in seinem Gewahrsam allgemeine Buchführungsunterlagen befinden, die regelmäßig nicht dem besonders geschützten Verhältnis der "Steuerberatung" zugehören (wenn der Steuerberater auch Buchführungs- und Lohnabrechnungsaufgaben übernimmt, so handelt es sich um zusätzliche, nicht aber um steuerberatende Tätigkeiten). Hieraus folgt, dass zwar eine Durchsuchungsanordnung, die nur auf das Auffinden beschlagnahmefreier Gegenstände gerichtet ist, unzulässig wäre, hingegen eine Durchsuchungsanordnung, die sich auf andere Gegenstände bezieht, zulässig ist (z.B. auf Buchführungsunterlagen und Jahresabschlüsse beim Steuerberater). Aber auch Verteidigerschriftverkehr kann dann beschlagnahmefähig sein, wenn sich aus ihm der Hinweis auf eine Teilnahme oder Strafvereitelung ergibt.

Jede Form der amtlichen Inverwahrnahme stellt eine Sicherstellung dar. Einer förmlichen Beschlagnahme gemäß § 98 StPO bedarf es nur bei einer Verweigerung der freiwilligen Herausgabe. Die Beschlagnahme darf grundsätzlich nur der Richter, bei Gefahr im Verzug auch der Staatsanwalt oder der Hilfsbeamte anordnen. Erfolgt die Beschlagnahme ohne richterliche Anordnung und ist weder der Betroffene noch ein erwachsener Angehöriger anwesend gewesen oder hat der Betroffene oder sein erwachsener Angehöriger ausdrücklich der Beschlagnahme widersprochen, so soll binnen 3 Tage die richterliche Bestätigung beantragt werden. Ungeachtet dessen hat der Beschlagnahmebetroffene das Recht, die richterliche Entscheidung über die Herausgabe von Beschlagnahmegegenstände zu beantragen.

(eine erweiterte, mit Quellen und Links versehene Fassung dieses Textes finden Sie im Lexikon des www.EDV-Workshop.de)

Sichtung gemäß § 110 StPO. Papiere und Daten

Bedeutung und Regelungsgehalt

§ 110 StPO regelt die Art und Weise der Durchsuchung und hat nur Einfluss auf die Durchsuchung selber und auf das ggf. an sie anschließende Sichtungsverfahren [22].

Danach darf während einer Durchsuchung grundsätzlich nur ein Staatsanwalt die inhaltlich würdigende und wertende Durchsicht von Schriftstücken vornehmen (Briefe, Tagebuchaufzeichnungen, Buchführungswerke usw.; dies gilt aber nicht für Druckwerke, also verlegte Bücher, Kataloge u.ä.). Dieses Recht steht gemäß § 404 Abgabenordnung auch den Steuer- und Zollfahndern zu.

Die Sichtungsbefugnis des Staatsanwalts gilt auch für die ihn begleitenden Polizeibeamten, soweit und solange er am Durchsuchungsort körperlich anwesend ist - sie sind quasi die Augen und Ohren des Staatsanwalts. Dies geht so weit, dass auf einem Firmengelände, das als Einheit umfriedet und umgrenzt ist, die Polizeibeamten nicht den Beschränkungen des § 110 StPO unterliegen, auch wenn kein direkter Ruf- und Sichtkontakt zwischen ihnen und dem Staatsanwalt besteht. Allein die Erreichbarkeit des Staatsanwalts per Telefon reicht hingegen nicht.

Wird die Durchsuchung allein von Polizeibeamten durchgeführt, so findet § 110 Abs. 2, Abs. 3 StPO Anwendung. Gestattet der Durchsuchungsbetroffene die Durchsicht seiner Papiere, dann dürfen die Polizisten natürlich eine vollständige, inhaltlich ins Einzelne gehende Sichtung vornehmen.

Fehlt die Gestattung oder ist der Betroffene oder sein Vertreter (erwachsene Familienangehörige, leitender Mitarbeiter, bevollmächtigter Rechtsanwalt) bei der Durchsuchung nicht anwesend, so müssen die Beamten "die Papiere, deren Durchsicht sie für geboten erachten", in einen Umschlag nehmen und versiegeln. "Umschlag" im Sinne der Vorschrift können auch größere Behältnisse sein, also z.B. Umzugskartons.

Gemäß § 109 StPO ist ein Verzeichnis über die in amtliche Verwahrung genommenen Gegenstände zu erstellen. Die Verwahrung im Rahmen einer § 110-Maßnahme ist keine formlose oder gestattete Sicherstellung, sondern eine Maßnahme mit Zwangs-Charakter und damit der Beschlagnahme ähnlich. Mit anderen Worten: Die Mitnahme von Papieren unter den Voraussetzungen des § 110 StPO ist eine vorläufige Beschlagnahme zum Zweck der Prüfung der potenziellen Beweismitteleignung durch den durchsichtberechtigten Staatsanwalt. Als Beschlagnahme ist sie eine amtliche Inverwahrnahme und deshalb sind die verwahrten Gegenstände gemäß § 109 StPO zu protokollieren. Lassen sich die betroffenen Papiere mit einfachen Worten beschreiben, so sollten sie im Interesse der Aktenklarheit unverwechselbar beschrieben werden. Ist dies aufgrund der Menge oder der beschränkten Lesebefugnis der allein handelnden Polizeibeamten nicht möglich, so muss wenigstens der "Umschlag" unverwechselbar protokolliert werden.

---

[22] Dieser Aufsatz wurde erstmals im März 2001 im EDV-Workshop veröffentlicht. Er wurde seither ständig aktualisiert.

Aus praktischen Gesichtspunkten empfehle ich, verschiedene Verzeichnisse für "normale" und für die Durchsicht erfordernde Papiere anzulegen. Dies macht in der Praxis keine Schwierigkeiten, weil dazu einfach ein weiteres Blatt des Sicherstellungsprotokolls "Teil B" (Formular der niedersächsischen Polizei) anzulegen ist.

Die "Grobsichtung"

Ohne Durchsichtsberechtigung sollen die Polizeibeamten jene "Papiere, deren Durchsicht sie für geboten erachten", separieren und der Staatsanwaltschaft vorlegen.

Wie soll der Beamte das feststellen können? Jedenfalls nicht in der Weise, dass er Papiere überhaupt nicht berühren und ansehen dürfte.

In der juristischen Literatur ist der Begriff der "Grobsichtung" aufgetaucht, der die Abgrenzung zwischen erlaubtem und nicht erlaubtem Handeln der Polizei recht gut kennzeichnet. Von anderen Kommentatoren wird der Begriff jedoch vehement angegriffen.

Einigkeit besteht hingegen darüber, dass der Polizeibeamte eine oberflächliche Inaugenscheinnahme durchführen darf. Dies bedeutet einerseits, dass er selbstverständlich Aktenordner öffnen und darauf untersuchen darf, welche Art von Schriftstücke sie enthalten und ob das, was auf den Aktenrücken vermerkt ist, sich auch tatsächlich in dem Ordner befindet. Ich nenne das die Nutella-Prüfung.

Andererseits umfasst die oberflächliche Inaugenscheinnahme nach Rechtsprechung und Literatur noch mehr: Der Polizeibeamte darf die Kopfangaben der Schriftstücke lesen, also Absender und Empfänger, Datum, Betreff, Anrede und Unterschrift. Anhand dieser Angaben soll er entscheiden, ob das Schriftstück von vornherein beim Durchsuchungsbetroffenen verbleiben kann oder dem Staatsanwalt zur inhaltlichen Durchsicht vorgelegt werden soll.

Die nachträgliche Durchsicht des Staatsanwalts

Grundsätzlich soll die "Entsiegelung und Durchsicht" in Anwesenheit des Durchsuchungsbetroffenen erfolgen. Dies ergibt sich schon aus der Gesetzesformulierung, dass er, "wenn möglich, zur Teilnahme aufzufordern" ist. Dieselbe Folgerung ergibt sich aus dem verfassungsrechtlichen Gebot des rechtlichen Gehörs (Art. 103 Abs. 1 Grundgesetz), das durch § 33 StPO seine Umsetzung im Strafverfahrensrecht gefunden hat, und aus dem Anwesenheitsrecht des Durchsuchungsbetroffenen gemäß § 106 Abs. 1 StPO. Die Ausnahme, die in § 33 Abs. 4 StPO formuliert ist, greift bei der nachträglichen Durchsicht nicht, weil eine Gefährdung des Untersuchungszwecks nicht bestehen kann, wenn bereits eine amtliche Verwahrung erfolgt.

Nicht möglich ist die Aufforderung zur Teilnahme, wenn der Betroffene flüchtig oder in Haft ist. Es handelt sich auch um keine zwingende Formvorschrift, so dass dem Staatsanwalt ein eingeschränkter Ermessensspielraum bleibt (z.B. zur Vermeidung einer übermäßigen Verfahrensverzögerung).

Bei seiner Durchsicht darf sich der Staatsanwalt Durchsuchungshelfer bedienen, also z.B. Polizeibeamte, Sachverständige und Dolmetscher beiziehen. Die Papiere, die

nach inhaltlicher Prüfung von potenzieller Beweisbedeutung sind (§ 94 Abs. 1 StPO), sind in einem Verzeichnis aufzuführen (§ 109 StPO). Soweit der Betroffene einer amtlichen Inverwahrnahme nicht zustimmt, ist vom Staatsanwalt gemäß § 94 Abs. 2 StPO die richterliche Beschlagnahme zu beantragen (§ 98 Abs. 1 StPO).

Die gesetzliche Definition für Beweismittel geht sehr weit und umfasst alle "Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können" (§ 94 Abs. 1 StPO). Eine vorläufig abschließende Beschreibung des Untersuchungsgegenstandes erfolgt mit der Anklageerhebung (§ 200 Abs. 1 StPO). Die darin vorgenommene Beschreibung des Lebenssachverhalts ist für das Gericht bindend (§ 264 StPO; in seiner rechtlichen Beurteilung des Sachverhalts ist das Gericht hingegen frei).

Die erste Umschreibung des Untersuchungsgegenstandes erfolgt durch den Staatsanwalt, indem er gemäß § 152 Abs. 2 StPO ein Ermittlungsverfahren einleitet und die gebotenen Ermittlungen anordnet. Weil er jedoch "wegen aller verfolgbaren Straftaten" tätig werden muss, kann bis zum Abschluss der Ermittlungen noch keine vollständige und bindend begrenzende Beschreibung des Untersuchungsgegenstandes erfolgen. Ausgeschlossen sind insoweit nur solche Untersuchungen, denen Rechtsgründe entgegen stehen (z.B. strafunmündige Täter, verfolgungsverjährte Taten) oder die nach den Denkgesetzen in keinem Zusammenhang mit den aufgekommenen Vorwürfen stehen können.

Als Beweismittel geeignet sind somit alle Gegenstände, die mit Tat und Täter in Verbindung stehen und zu den Umständen des erhobenen Vorwurfs Auskunft geben. Hierbei kann es sich auch um sehr alte Urkunden handeln, wenn ihr Inhalt für die Straftat bedeutsam ist, die in jüngerer, nicht verfolgungsverjährter Zeit begangenen wurde. Daneben kann es sich auch um Beweismittel handeln, die nicht über die Straftat, wohl aber über die Lebensverhältnisse des Täters Auskunft geben, weil diese ebenfalls - zur Beurteilung der individuellen Schuld - Gegenstand der strafrechtlichen Untersuchung sind.

Verhältnismäßigkeit und Surrogate

Jede strafprozessuale Zwangsmaßnahme ist darauf zu überprüfen, ob sie dem Gebot der Verhältnismäßigkeit entspricht. Bei dieser Prüfung sind die Interessen

der Öffentlichkeit an einer funktionierenden und effektiven Strafverfolgung

- insoweit auch orientiert an den mutmaßlichen Kosten der Maßnahmen -

sowie die Schwere des Vorwurfs

- insoweit auch orientiert an dem Grad des Verdachts -

einerseits

und die Interessen des Betroffenen, insbesondere die Stärke und Nachhaltigkeit des Eingriffs in seine Grundrechte,

sowie die Interessen von Opfern und Geschädigten

andererseits

gegeneinander abzuwägen.

Wegen der Art der Beweismittel heißt das, dass die Strafverfolgungsbehörden zunächst einmal ein Anrecht auf das Original des schriftlichen Beweismittels haben.

Dies ergibt sich nicht nur daraus, dass die §§ 94 ff. StPO Kopien, Abschriften und Abbildungen von Original-Beweisstücken unerwähnt lassen, sondern auch aus physikalisch-technischen sowie anderen wissenschaftlichen Erwägungen:

Nur die Originale lassen sich auf eine Urheberschaft hin untersuchen.

Bei Papieren lässt sich anhand ihrer Zusammensetzung prüfen, wann sie hergestellt wurden. Dasselbe gilt für die verwendeten Tinten, Schreibpasten und Tonersubstanzen. Auch aus der Veränderung ihrer physikalischen und chemischen Struktur lassen sich begrenzte Rückschlüsse ziehen (Verfärbungen, Farbverläufe, Strukturänderungen - also Alterungserscheinungen, die allerdings im besonderen Maße von den Lagerungsumständen abhängen: Lichteinfall, Raumtemperatur und -feuchtigkeit). Die Reihenfolge des Farbauftrags lässt sich feststellen (z.B. bei der Frage, ob eine Unterschrift auf den gedruckten Text oder vorher aufgebracht wurde).

Handschriften lassen sich Urhebern mit verschiedenen Wahrscheinlichkeitsgraden zuordnen.

Für den Betroffenen können von besonders wichtigen Dokumenten beglaubigte Ablichtungen gefertigt werden, die einen dem Original vergleichbaren Beweiswert haben. Nur in echten Ausnahmefällen bedarf der Betroffene des Originals (Inhaberpapiere, Wechsel).

Im übrigen gilt nach herrschender Rechtsprechung, dass sich der Betroffene von seinen Schriftstücken auf eigene Kosten Ablichtungen anfertigen (lassen) darf.

Als Faustformel für die Praxis gilt aus meiner Sicht, dass sich die Strafverfolgungsbehörden nur im Ausnahmefall auf Surrogate (Ablichtungen u.ä.) beschränken dürfen, nämlich dann, wenn gutachtliche Untersuchungen am Material nicht zu erwarten sind und gleichzeitig ein besonderes Interesse des Betroffenen am Besitz des Originals dargelegt ist und nachvollzogen werden kann.

Daten sind Papiere

Nach anfänglichen Unsicherheiten in Literatur und Rechtsprechung besteht nunmehr die einhellige Meinung, dass elektronische Daten im Zusammenhang mit dem § 110 StPO Papiere im Sinne dieser Vorschrift sind.

Daraus folgt, dass die Polizeibeamten, die eine Durchsuchung ohne einen Staatsanwalt durchführen, zwangsweise nur einen beschränkten Zugriff auf EDV-Daten nehmen dürfen.

Wenn es ihnen aber gestattet ist, Papiere oberflächlich in Augenschein zu nehmen, so gilt dies auch für EDV-Daten. Eine entsprechende technische Kompetenz vorausgesetzt, darf der Polizeibeamte

- den vorgefundenen Computer in Betrieb setzen,
- die vorhandenen Dateiverzeichnisse und deren Inhalte auflisten,
- die Datenspeicher - besonders die Festplatten - nach gelöschten Dateien untersuchen und diese wieder sichtbar machen,

feststellen, welche Anwenderprogramme vorhanden sind, und nach Dokumenten mit den dazugehörenden Extensionen suchen und selbst einzelne Text- oder Tabellen-Dokumente aufrufen und nach den Merkmalen untersuchen, die für Papiere gelten: Die oberflächliche Inaugenscheinnahme wegen der Adress-, Datums- und Betreff-Daten ist erlaubt. Nicht erlaubt ist die inhaltliche Prüfung des individuellen Textes

Computer als Hilfsmittel der Suche

Wolfgang Bär hat in seiner Doktorarbeit [23] zu Recht darauf hingewiesen und belegt, dass Computern nicht nur die Eigenschaft eines Beweismittels haben, sondern während der Durchsuchung auch ein technisches Hilfsmittel für die Suche nach Beweismitteln sind. Sie dürfen von den Polizeibeamten - ggf. in den Grenzen des § 110 StPO - deshalb auch während der Durchsuchung benutzt werden.

Praktisch bedeutet das, dass zunächst einmal alle örtlich vorhandenen Speichermedien mittels des vorgefundenen Computers auf beweisrelevante Daten untersucht werden dürfen. Dies schließt Suchvorgänge nach Suchworten ein, um solche Dateien zu erkennen, die sofort oder später genauer auf ihre Beweismittelbedeutung untersucht werden dürfen.

Für die inhaltliche Datenauswertung während der Durchsuchung gelten die Grenzen, die bereits wegen der oberflächlichen Inaugenscheinnahme skizziert worden sind.

DFÜ-Verbindungen

Keine einheitliche Meinung gibt es dazu, ob bei einer Durchsuchung der vorgefundene Computer auch dazu benutzt werden darf, Datenfernübertragungen zum Internet oder zu anderen Netzen vorzunehmen. In der Praxis können sowohl Homebanking-, auf Internet-Servern abgelegte Daten des Betroffenen oder Leitungsverbindungen zwischen Filialen und Hauptsitzen von Firmen von Interesse sein.

Nach wörtlicher Maßgabe der Vorschriften zur Durchsuchung müsste gegen eine solche Suche eingewandt werden, dass sie den durch den Durchsuchungsbeschluss gekennzeichneten Ort verlässt und auf andere Orte - Serverstandorte - erweitert.

Ich bin der Meinung, dass die Nutzung der DFÜ-Verbindungen des Betroffenen während einer Durchsuchung so weit erlaubt ist, wie dies mit den Zugangsrechten und den technischen Möglichkeiten des Betroffenen möglich ist. [24]

Sind die Zugangsdaten des Betroffenen auf dem Gerät gespeichert oder an seinem Arbeitsplatz notiert, so sind diese Daten normale Beweismittel im Sinne von § 94 Abs. 1 StPO. Ihre Verwendung mit dem vorgefundenen Computer stellt eine Suche mit den örtlich vorhandenen Möglichkeiten dar. Können bei dieser Suche Daten erhoben wer-

[23] Wolfgang Bär, Der Zugriff auf Computerdaten im Strafverfahren, Köln, Berlin pp. 1992

[24] hierin werde ich bestärkt von dem Kollegen Dieter Kesper (GenStA Köln), der in einem demnächst erscheinenden Werk die Meinung vertreten wird, dass der Richtervorbehalt des § 105 StPO bevorzugt dem Schutz der Wohnung gilt (Art. 13 GG) und es deshalb wegen ausgelagerter Dateien dann keiner eigenständigen Durchsuchungsanordnung bedarf, wenn der Dritte als Host-Provider auftritt und nicht in eigenen Rechten verletzt wird - also keine Geheimnisse des Dritten tangiert und gesichert werden.

den, die auf ihre Beweismitteleignung geprüft werden müssen, so sollen sie m.E. gesichert und - unter den Beschränkungen des § 110 StPO - im gesonderten Sichtungsverfahren geprüft werden.

Was nicht geschehen darf, sind die Anwendung von Zwang oder Tricks, um mehr oder andere Daten bei der Suche zu erhalten als die, die der Betroffene aufgrund seiner Zugangsrechte beziehen darf.

Werden dabei Daten aus dem Ausland bezogen, ist vom Staatsanwalt zu prüfen, ob im Wege der internationalen Rechtshilfe die nachträgliche Erlaubnis zur Erhebung der Daten und die Erlaubnis zur Verwendung der Daten im Strafverfahren einzuholen sind. Während des laufenden Rechtshilfeersuchens dürfen die davon betroffenen Daten nicht ausgewertet werden. Öffentlich zugängliche Daten aus dem Ausland, die ohne Überwindung von Sicherungsvorkehrungen erreichbar sind, unterliegen nicht einem solchen Schutz [25].

Einsatz von Suchprogrammen.
Beispiel: Perkeo

Perkeo ist ein Datenscanner zur Erkennung kinder- und tierpornographischer Dateien, der von der Firma Autem in enger Zusammenarbeit mit dem Bundeskriminalamt und den Landeskriminalämtern entwickelt worden ist.

Das Programm vergleicht - ähnlich wie ein Virenscanner - die zu untersuchenden Dateien mit den in seiner Datenbank gespeicherten "digitalen Fingerabdrücken" (Signaturen). "Die Datenbank", so heißt es in dem im Internet veröffentlichten Handbuch, "wird in Zusammenarbeit mit dem BKA Wiesbaden erstellt und beinhaltet nur digitale Fingerabdrücke von eindeutig kinder- und tierpornographischen Objekten".

Die erforderliche Suche nach Signaturen ist m.E. auch unter den Beschränkungen des § 110 StPO erlaubt, weil - wie bei der Suche nach Suchworten auch - nur identische Zeichenfolgen gesucht werden. Die inhaltlich wertende Frage, ob es sich bei den gefundenen Dateien tatsächlich um unerlaubte Darstellungen handelt, also die von § 110 StPO gemeinte Durchsicht, muss zu einem späteren Zeitpunkt geleistet werden.

Werden aber übereinstimmende Signaturen gefunden, so gibt das einen hinreichenden Anlass, die EDV-Anlage zunächst vorläufig sicher zu stellen und ihren Datenbestand nach richterlicher Beschlagnahme gezielt und inhaltlich wertend zu untersuchen.

Ungeachtet der hier entwickelten Lösung sind Zweifel daran angebracht, ob die von Perkeo gesuchten Dateien tatsächlich dem besonderen prozessualen Schutz des § 110 StPO unterliegen. Im Gegensatz zu individuell gefertigten Schriftstücken (Briefe, Aufzeichnungen, Tagebücher) unterliegen näm-

[25] siehe auch die vorausgegangene Fußnote (Kesper-Standpunkt)

lich massenhaft produzierte Druckwerke (Bücher, Zeitschriften, Kataloge, Prospekte) den Einschränkungen der Sichtung durch Polizeibeamte nicht.

Aufgrund dieser Überlegung kann man auch mit guten Gründen die Auffassung vertreten, dass die Programmbestandteile eines Computers, empfangene Newsletter oder gesammelte Grafiken (die dem BKA bereits bekannt sind) eher als "durchsichtfreie" Druckwerke anzusehen sind und insoweit nicht den Beschränkungen des § 110 StPO unterliegen.

Durchsicht von EDV-Sachverständigen

Dem reinen Wortlaut nach muss der Staatsanwalt die wertende Durchsicht persönlich durchführen.

Fehlt es ihm hierzu an technischem Wissen, so darf er sich zur Vorbereitung seiner wertenden Entscheidung der Hilfe von Sachverständigen bedienen, die ihm die Daten so aus dem sichergestellten Bestand herauslösen und aufbereiten, dass er seine inhaltlich wertende Aufgabe ausführen kann.

Dies ergibt sich aus der einhelligen Rechtsprechung zum Einsatz von Übersetzern im Rahmen des § 110 StPO. Ist der Staatsanwalt nicht der verwendeten Fremdsprache mächtig, so darf er selbstverständlich zunächst eine Übersetzung in Auftrag geben, die er dann anstelle des Originals auf die Beweiserheblichkeit prüft.

Auf elektronische Daten übertragen heißt das, dass im Sichtungsverfahren gemäß § 110 StPO auch technische Sachverständige eingesetzt werden dürfen, die dem Staatsanwalt die Daten so aufbereiten (auflisten, ausdrucken), dass er seine wertende Prüfung durchführen kann. Die Benennung von z.B. Suchworten oder von Merkmalen der gesuchten Informationen obliegt dem Staatsanwalt.

Weitergehende Sachverständigenaufträge, insbesondere die Übertragung seiner inhaltlich wertenden Kompetenz, darf der Staatsanwalt im Sichtungsverfahren nicht erteilen. Soll der Sachverständige in Abwesenheit des Staatsanwalts tätig werden, so unterliegt er der Beschränkung auf die oberflächliche Inaugenscheinnahme.

(eine erweiterte, mit Quellen Links versehene Fassung dieses Textes finden Sie unter den Aufsätzen im www.EDV-Workshop.de)

Behandlung von Computerkomponenten und Datenträgern im Ermittlungsverfahren

Besondere Vorschriften über die Behandlung von digitalisierten Daten sind in der Strafprozessordnung nicht geregelt. Ihre prozessuale Behandlung muss deshalb im wesentlichen aus den allgemeinen Vorschriften über Aktenbestandteile, Akteneinsicht, Sicherstellung und Beschlagnahme entwickelt werden. [26]

1. sichergestellte digitalisierte Daten

Sichergestellte Zentraleinheiten, Festplatten oder andere, fest eingebaute Speichermedien und Disketten oder andere auswechselbare, einmalig oder mehrmalig beschreibbare Datenträger sind Beweismittel im Sinne von § 94 Abs. 1 StPO. Im wesentlichen gehören hierzu interne Speichermedien wie Festplatten und externe wie Disketten, Sicherungsbänder (hierfür kommen neben speziellen kleinen Kassetten mit festem Metallboden auch klassische Audiokassetten und sogar Videobänder in Betracht), Wechselfestplatten sowie ZIP-Disketten mit großer Speicherkapazität, die den Disketten sehr ähnlich sehen, und individuell beschreibbare CD-Rs.

Ohne praktische Bedeutung sind inzwischen Lochkarten und -bänder, die "weichen" 5 1/4 Zoll-Disketten und voluminösen Datenträger, die in den achtziger Jahren des letzten Jahrhunderts verwendet wurden. Inzwischen verliert auch die 3 ½ Zoll-Diskette als Datenträger an Bedeutung; sie wird von USB-Speichersticks verdrängt werden.

"Datenträger" im engeren Sinne sind auch die Speicherchips des Arbeitsspeichers auf der Hauptplatine im Inneren des Computers. Sie verlieren aber in aller Regel ihren "Dateninhalt", wenn ihre Stromzufuhr abgeschaltet wird. Sie können eine selbständige Beweisbedeutung haben, also beschlagnahmefähig sein, wenn es um ihre Beschaffenheit geht (z.B. in Fällen der Produktpiraterie). Für sie gilt wie für alle anderen fest in ein Computergehäuse eingebauten elektronischen Teile, dass die Gefahr der Zerstörung des technischen Geräts bei unfachmännischer Demontage viel zu groß ist, so dass im Zweifelsfall die gesamte Zentraleinheit (also der eigentliche Computer in seinem festen Gehäuse) sicherzustellen ist. Daneben sind auch die Peripheriegeräte (Tastatur, Maus, Bildschirm, Drucker, Modem usw.) beschlagnahmefähig, weil ohne sie eine funktionsfähige Wiederinbetriebnahme in aller Regel erschwert, wenn nicht ausgeschlossen ist.

---

[26] Bei diesem Text handelt es sich um eine aktualisierte Fassung des Kapitels "Behandlung von Computerkomponenten, Datenträgern und Datenverarbeitungsprozeduren" aus meinem Aufsatz Durchsuchung in Wirtschaftsstrafsachen aus dem Jahr 1996. Sechs Jahre der Entwicklungen im Bereich der EDV-Technik und des Rechts haben seither einige Klärungen, aber auch viele neu Fragen aufgeworfen, mit denen sich andere Beiträge im EDV-Workshop befassen. Bei der Bearbeitung bin ich behutsam vorgegangen und habe nur die Passagen ergänzt, korrigiert oder gekürzt, die nicht mehr dem aktuellen Stand von 2002 entsprechen.

Der Text behandelt quasi die Grundprobleme, die sich in der Anfangszeit der Computerkultur für die Ermittlungsverfahren stellten und deren Lösungen bis heute gelten.

Besondere Schwierigkeiten bestehen dann, wenn die Arbeitsdaten des Durchsuchungsbetroffenen gar nicht auf dem Computer an seinem Arbeitsplatz gesichert werden, sondern per Modem und Telefonnetz auf einen anderen Rechner, zum Beispiel auch im Ausland, übertragen werden. Neben spezialisierten "Mailboxen" kann jeder Host-Speicherplatz im Internet zur Datenablage verwendet werden [27].

Eine lange Zeit ungeklärte Frage war, ob ein kompetenter Polizeibeamter den Computer des Betroffenen nicht nur in Betrieb nehmen, sondern auch die DFÜ-Programme des Geräts starten darf (eMail-, Newsgroups- usw. Browser, FTP-Programme). Ich vertrete die Auffassung, dass er das grundsätzlich darf, weil die EDV-Anlage des Betroffenen nicht nur als technisches Gerät beweismittelfähig ist, sondern auch als Hilfsmittel zur Suche nach Beweismitteln (Daten) den Durchsuchungsbeamten zugänglich ist. Die Detailprobleme werden an anderer Stelle angesprochen [28].

Hoheitlicher Eingriffe und Anordnungen sind selbstverständlich dann nicht erforderlich, wenn der Betroffene an der Datenbeschaffung freiwillig mitwirkt und die ausgelagerten Daten mit seinem Computer und seinen privatrechtlichen Zugangsrechten zu seinem Rechnern zurückholt. Befinden sich die Daten dann wieder auf dem Rechner des Betroffenen, so können sie von dort aus auch wie in den übrigen Fällen sichergestellt werden.

Der Betroffene ist nicht verpflichtet, die Durchsuchungsbeamten zu unterstützen oder selbst Datensammlungen zu editieren (z.B. Datenbankabfragen). Die von ihm verwendeten Programme zur Zusammenstellung und Formatierung sind hingegen grundsätzlich beschlagnahmefähig.

Die Frage nach der Beschlagnahmefähigkeit eingesetzter Programme wird sich in den meisten, also in den Standardfällen nicht stellen (Standardformate, die programmübergreifend verarbeitet werden können). Der Gesetzgeber hat in § 45 Urhebergesetz die Nutzung von geschützten Werken in behördlichen und gerichtlichen Verfahren zugelassen, so dass auch die Beschlagnahme von Computerprogrammen für die Zwecke des einzelnen Ermittlungsverfahrens zulässig ist [29].

Anhang:
§ 45 UrhG, Rechtspflege und öffentliche Sicherheit

> (1) Zulässig ist, einzelne Vervielfältigungsstücke von Werken zur Verwendung in Verfahren vor einem Gericht, einem Schiedsgericht oder einer Behörde herzustellen oder herstellen zu lassen.
>
> (2) Gerichte und Behörden dürfen für Zwecke der Rechtspflege und der öffentlichen Sicherheit Bildnisse vervielfältigen oder vervielfältigen lassen.
>
> (3) Unter den gleichen Voraussetzungen wie die Vervielfältigung ist auch die Verbreitung, öffentliche Ausstellung und öffentliche Wiedergabe der Werke zulässig.

---

27 siehe oben den Beitrag zur Sichtung von Papieren und Daten

28 siehe ebenda

29 vergl. Ermittlungsrichter BGH StV 88, 90, der die beschlagnahmefähigen Gegenstände auch auf die verwendete Hardware erstreckt

1.1. Verfahren der Sicherstellung

Nach einer freiwilligen Herausgabe von Datenträgern erfolgt die Sicherstellung nach den allgemeinen Grundsätzen des § 94 Abs. 1, Abs. 2 StPO (amtliche Inverwahrnahme). Werden Datenträger nicht freiwillig herausgegeben, bedarf es einer Beschlagnahme (§ 94 Abs. 2 StPO). Der Beschlagnahme muss in diesem Fall eine förmliche Durchsicht im Sinne von § 110 StPO vorausgehen. Zur Durchsicht ist nur der Staatsanwalt befugt, soweit der Inhaber keine Sichtung durch die Durchsuchungsbeamten genehmigt (§ 110 Abs. 1, 2 StPO). Wie bei der Durchsicht von Papieren darf sich der Staatsanwalt bei seiner Durchsicht von Datenträgern eines Sachverständigen und anderer Beamte zu seiner Unterstützung bedienen. Neben privaten Datenverarbeitungsfachleuten kommen insbesondere polizeiliche Spezialisten als sachverständige Sichtungshelfer in Betracht. Dem Durchsuchungsbetroffenen ist die Anwesenheit bei der Datensichtung gestattet. Über die Einzelheiten berichtet der Aufsatz Sichtung gemäß § 110 StPO. Papiere und Daten.

Sind die Computerdaten freiwillig heraus gegeben oder wirksam beschlagnahmt worden, handelt es sich um Beweismaterial, mit dem die Ermittlungsbeamten arbeiten dürfen. Die Besonderheiten des Sichtungsverfahrens, also insbesondere die Anwesenheitspflicht eines Staatsanwalts, gelten sodann nicht mehr.

1.2. Datensicherung als Sicherstellungssurrogat

Die Sicherung von beweiserheblichen Daten ("Back-up" auf einem Datenband oder anderem Datenträger im Rahmen einer Durchsuchung) kann aus Gründen der Verhältnismäßigkeit als Sicherstellung ausreichen und die Inverwahrnahme des Originaldatenträgers entbehrlich machen.

Die Übertragung der Daten auf Datenträger der Strafverfolgungsbehörden oder beauftragter Sachverständiger stellt ein Sicherstellungssurrogat dar. Für die Sicherstellung des Surrogats gelten dieselben Grundsätze wie für Originalbeweisstücke, so dass es ohne die Genehmigung des Dateninhabers einer förmlichen Beschlagnahme bedarf. Für die Entscheidung, ob die Sicherstellung eines Surrogats ausreichend ist, sind neben den allgemeinen Verhältnismäßigkeitserwägungen auch die besonderen Anforderungen des Untersuchungsgegenstandes bedeutsam. Ist bei der Sicherstellung bereits zu erwarten, dass den Daten nicht nur eine positive Beweisbedeutung zukommt (welche Programme und welche Daten hat der Betroffene zur Verfügung?), sondern muss auch ausgeschlossen werden, dass er keine anderen Daten gesammelt und mit keinen anderen Programmen gearbeitet hat (in meinen Worten: negative Beweisbedeutung), so sollte im Zweifel die gesamte Zentraleinheit sichergestellt werden.

Bei einer Datensicherung am Durchsuchungsort kann nicht immer eine hundertprozentige Datensicherheit garantiert werden, weil durch Softwarefehler oder aufgrund von Materialmängeln an den verwendeten Datensicherungsbändern Übertragungsfehler vorkommen können. Zur Vermeidung solcher Fehler muss in den Fällen

negativer Beweisbedeutung das Interesse der Öffentlichkeit an einer funktionstüchtigen Strafverfolgung ein besonderes Gewicht bekommen und womöglich die Zentraleinheit vorübergehend sichergestellt, die Daten auf einen dienstlichen Rechner übertragen und der Computer an den Betroffenen erst herausgegeben werden, wenn ein Sachverständiger die vollständige Datenübertragung auf einen Dienstrechner bestätigt hat.

In den Fällen, in denen die Datensicherung als Sicherstellungssurrogat ausreichend erscheint, muss darauf geachtet werden, ob auch gelöschte Daten beweiserheblich sind und deshalb gleichfalls gesichert werden müssen. Die normalen Betriebssysteme von Computern nehmen üblicherweise keine physikalische Löschung von Datendokumenten vor, sondern ändern lediglich den Dokumentnamen und lassen dadurch den vom Dokumentbelegten Speicherplatz zum Überschreiben zu. Solange dieser Speicherbereich (auf der Festplatte) nicht neu überschrieben wurde, lässt sich das gelöschte Dokument einfach wieder lesbar machen.

Bei der üblichen, rein "logischen Sicherung" werden nur die nicht gelöschten Dateien auf die Sicherungsmedien übertragen. Sollen auch die möglicherweise gelöschten Daten für eine künftige Beweiserhebung gesichert werden, bedarf es einer vollständigen, "physikalischen" Datensicherung, bei der der komplette Festplatteninhalt einschließlich der "leeren" Teile gesichert werden.

Physikalisch gelöschte Daten lassen sich hingegen mit den üblichen technischen Mitteln nicht wieder lesbar machen. Eine physikalische Löschung besteht darin, dass der Festplattenbereich des gelöschten Dokuments vollständig - und meist mehrfach - mit 0-Zeichen überschrieben wird.

1.3. beschlagnahmefreie Daten

Nach den Grundsätzen für beschlagnahmefreie Gegenstände (§§ 97, 148 Abs. 1 StPO) sind insbesondere Daten im Herrschaftsbereich von Berufshelfern und solche, die sich auf den Verkehr zwischen dem Beschuldigten und seinem Verteidiger beziehen, von der Beschlagnahme ausgenommen. Insoweit besteht zwar kein generelles Sicherstellungsverbot, wohl aber ein Beschlagnahmeverbot und die Pflicht zur Belehrung darüber, dass die Herausgabe nicht erzwungen werden darf.

Die Probleme, die sich insoweit im Zusammenhang mit digitalisierten Daten ergeben, lassen sich mit dem bestehenden gesetzlichen Instrumentarium nur unzureichend lösen. Nach der gegenwärtigen Rechtslage ist zufolgern, dass für beschlagnahmefreie Daten zumindest ein Verwertungsverbot in der Hauptverhandlung und während der ihr vorausgehenden Untersuchungen besteht. Dies bedeutet, dass aus beschlagnahmefreien Daten keine Vorhalte und keine Erkenntnisgrundlagen für andere Beweiserhebungen geschöpft werden dürfen.

Sowohl bei sichergestellten Originaldatenträgern wie auch bei Sicherstellungssurrogaten ist eine Aussonderung beschlagnahmefreier Daten grundsätzlich ausgeschlossen, weil sie zur Verfälschung des Beweisinhalts wegen der übrigen, beschlagnahmefähigen Daten führen kann. Wegen der besonderen technischen Beschaffenheit der Speichermedien muss deshalb in diesen Fällen der Datenträgerinhalt insgesamt als beschlag-

nahmefähig behandelt werden, weil eine nur teilweise Sicherstellung den Nachweis der Identität und Originalität der Daten in Frage stellen kann. Technisch ist dieses Problem den Tonbändern mit Mitschnitten von Telefonüberwachungen vergleichbar: In jenen Fällen werden die Tonbänder ebenfalls aufbewahrt, aber nur Abschriften von verwertbaren Gesprächen und nicht von Telefonaten mit Verteidigern gefertigt. Die Verwahrung des kompletten Ton- oder Datenbandes dient allein dem Nachweis der Vollständigkeit. Wegen des geistigen Inhalts beschlagnahmefreier Daten bleibt dessen ungeachtet ein prozessuales Verwertungsverbot bestehen. Wegen tagebuchähnlicher Aufzeichnungen besteht schon nach der derzeitigen Rechtsprechung nur im Einzelfall ein Beweisverwertungsverbot, nicht aber bereits ein zwingendes Beweiserhebungsverbot. Tagebuch-ähnliche Aufzeichnungen unterliegen somit auch in digitalisierten Form grundsätzlich der Beschlagnahme. Über ihre Verwertung im Einzelfall muss im Rahmen der gerichtlichen Hauptverhandlung entschieden werden [30].

1.4. Einsichtnahme der Verfahrensbeteiligten

Als Beweisstücke sind sichergestellte Datenträger oder ihre Surrogate im weiteren Sinne Aktenbestandteile, die dem Gericht mit der Anklageschrift gemäß § 199 Abs. 2 StPO vorzulegen sind. Für diese Beweisstücke besteht für den Verteidiger oder Geschädigtenvertreter hingegen kein "Akteneinsichtsrecht", sondern nur ein "Besichtigungsrecht" in der Amtsstelle gemäß § 147 Abs. 1, Abs. 4 StPO. Eine Aushändigung der Originalstücke oder Surrogate an Rechtsanwälte, Beschuldigte oder sonstige Verfahrensbeteiligte darf nicht erfolgen (§ 147 Abs. 4 StPO). Bei seiner Besichtigung darf sich der Verteidiger Aufzeichnungen machen und Sachverständige beiziehen. Entsprechend der Besichtigung von Tonbandaufnahmen wird ihm auch zu gestatten sein, sich die sichergestellten Daten "vorspielen" und sich eine Kopie fertigen zu lassen. Mit Rücksicht auf dieses erweiterte Besichtigungsrecht sind die Staatsanwaltschaft und nach Anklageerhebung das Gericht zur Fertigung von Datenträgerkopien befugt, die an den Verteidiger oder Rechtsanwalt (§ 406e StPO) ausgehändigt werden können. Der Umfang der Kopien ist dabei genau zu bezeichnen, weil während des Ermittlungsverfahrens der Untersuchungszweck Vorrang vor Akteneinsicht und Beweismittelbesichtigung genießt (§ 147 Abs. 2 StPO) und gegenüber einem Geschädigtenvertreter auch die schutzwürdigen Belange des Beschuldigten oder anderer Personen zuwahren sind (§ 406e Abs. 2 StPO, § 30 AO, § 35 SGB I, §§ 78a ff. SGB X).

2. digitalisierte Verfahrensdaten

Unabhängig von der Frage, welche Computerdaten als Beweismittel beigezogen werden können, ist auch die Frage zu klären, wie mit den Computerdaten zu verfahren ist, die von den ermittelnden Polizeibeamten, dem Staatsanwalt und schließlich auch von

[30] insbesondere für den Fall, dass bei der Durchsuchung kein Staatsanwalt anwesend ist, empfehle ich in Zweifelsfällen das Verfahren nach § 110 Abs. 2, Abs. 3 StPO auch dann zu wählen, wenn die rechtliche Zulässigkeit der Beschlagnahme unklar ist und erst noch vom StA geprüft werden muss

dem Richter selber erfasst, sortiert oder elektronisch kommentiert worden sind.

Es handelt sich hierbei regelmäßig um eigene Arbeitsaufzeichnungen des Sachbearbeiters, die grundsätzlich keiner Akteneinsicht durch Dritte zugänglich sind. Datensammlungen, die von den Ermittlungsbehörden erstellt werden und deren Einzeldaten in den Ermittlungsvorgängen dokumentiert sind (Vertragstexte, Kontoauskünfte und -verdichtungen, Zeugenaussagen usw.), spiegeln nur den Akteninhalt wider und sind als Datensammlungen genauso wie Konzepte, Entwürfe und Ideenskizzen des Sachbearbeiters individuelle Arbeitsunterlagen. Sie sind als technische Hilfsmittel keine Aktenbestandteile, solange sie nicht als Ausdrucke, Programmdokumentationen in Papierform oder auf einem digitalen Datenträger zu den Akten gelangen.

"Akten" sind im Anschluss an die §§ 163, 173 und 199 StPO Schriftstücke, Urkunden und andere schriftliche Aufzeichnungen unter Einschluss von Lageplänen und anderen schriftförmigen Augenscheinsgegenständen (Fahndungsphotos, Tatortdokumentationen usw.). Wie bei einer Tonbandaufnahme von Vernehmungsprotokollen werden die aufgenommenen digitalisierten Daten in einem Aktenvermerk oder in ein Protokoll zu den Akten genommen. In gleicher Weise stellt die digitalisierte Datensammlung der Polizei nur ein Hilfsmittel dar, das allenfalls ergänzend als Augenscheinsgegenstand und damit als Beweisstück Bestandteil der Ermittlungsvorgänge wird.

Soweit Polizeibehörden schon im Wege des ersten Zugriffs ohne Anleitung durch die Staatsanwaltschaftdigitalisierte Verfahrensdaten erstellen und an die Staatsanwaltschaft weitergeben, handelt es sich um polizeiliche "Verhandlungen", die nach § 163 Abs. 2 S. 1 StPO Aktenbestandteile sind und nach § 199 Abs. 2 S. 2 StPO dem für die Hauptverhandlung zuständigen Gericht vorgelegt werden müssen. Sie sind ganz streng als Aktenbestandteile zu bewerten. Auch wenn diese Daten vom ersten Zugriff nur ergänzend in digitalisierter Form an die Staatsanwaltschaft weitergegeben werden, handelt es sich um Beweisstücke, die auch dem Gericht und den übrigen berechtigten Verfahrensbeteiligten zur Besichtigung gegeben werden müssen.

Stellt die Polizei digitalisierte Verfahrensdaten im Auftrag der Staatsanwaltschaft aus den Beweismitteln im übrigen zusammen (§ 161 StPO), so handelt es sich um technische Hilfsmittel, die der staatsanwaltlichen Aufgabenerfüllung und der Vorbereitung der Sachentscheidung über den Verfahrensabschluss dienen. Solche Daten werden nicht zwangsläufig Aktenbestandteil, sondern sind wie die eigenen vorbereitenden Aufzeichnungen des Staatsanwalts zu behandeln. Über die Dokumentation der Verfahrensdaten und ihrer Weitergabe entscheidet in diesem Fall allein die Staatsanwaltschaft.

Auch die Staatsanwaltschaft ist gehalten, die Ergebnisse ihrer Ermittlungen vollständig in Form von Vermerken und Protokollen zu dokumentieren. Soweit sie ihrer abschließenden Entscheidung die Sammlung eigener oder durch Hilfspersonen erstellter digitalisierter Verfahrensdaten zugrunde legt, sind die Arbeitsergebnisse, also die verwendeten Daten und das Ergebnis der elektronischen Datenauswertung, vollständig als Vermerk oder Protokoll in den Akten zu dokumentieren.

Bietet die Staatsanwaltschaft daneben die digitalisierten Verfahrensdaten dem Gericht

zur Verwendung an oder nimmt sie digitalisierte Verfahrensdaten auf Datenträgern bei der Vorlegung der Anklageschrift zu den Akten (§ 199 Abs. 2 S. 2 StPO), so schafft sie damit Augenscheinsgegenstände, die wie andere Beweisstücke dem Besichtigungsrecht des Verteidigers oder des Geschädigtenvertreters unterliegen.

Die für die Erfassung und Auswertung des Akteninhalts verwendeten Standardprogramme dürfen bereits deshalb nicht für Verteidiger und Rechtsanwälte kopiert werden, weil ihre Verwendung für den Anwender, hier also die Justizbehörden, lizenziert sind. Darüber hinaus handelt es sich um allgemein zugängliche Arbeitsmittel, die, wie andere Büroausstattungen auch, nicht zum Aktenbestandteil werden. Etwas anderes kann nur dann gelten, wenn für die Datenerhebung und -auswertung ein nicht marktgängiges Spezialprogramm verwendet wurde. Für diese Fällen kann keine allgemeingültige Aussagegemacht werden; im Einzelfall müssen die Lizenzbedingungen des Softwareverkäufers eingehalten werden.

3. Datenverarbeitung in Umfangsverfahren

Sichergestellte digitale Daten und digitale Sammlungen von Verfahrensdaten unterliegen als Kopien auf Datenträgern nur einem Besichtigungsrecht durch den Verteidiger und Geschädigtenvertreter, die somit auch berechtigt sind, sich bei der Besichtigung eines Sachverständigen zu bedienen und sich eine Kopie des Datenträgers anfertigen zu lassen.

Digitalisierte Datensammlungen, die den Akteninhalt widerspiegeln, sind grundsätzlich geeignet, die Hauptverhandlung zu erleichtern und auf wesentliche Untersuchungsfragen zu reduzieren. Soweit Verteidiger und Geschädigtenvertreter bereit sind, mit dem digitalen Datenmaterial zu arbeiten, bestehen keine grundsätzlichen Bedenken, Verfahrensdaten und sichergestellte Daten als Kopien auszuhändigen. In derselben Weise wie die schriftförmigen Beweismittel im übrigen erlangen digitalisierte Verfahrensdatenerst durch ihre Auswertung einen eigenen Aussagewert.

Mit der Anklageerhebung dokumentiert die Staatsanwaltschaft, dass sie eine vollständige, wertende und abwägende Auswertung der Verfahrensdaten durchgeführt hat. Hat sie sich dabei der Datenverarbeitung bedient, muss sie, um das Ergebnis ihrer Prüfung nachvollziehbar zu machen, das Auswertungsprinzip und bei komplexen Auswertungsvorgängen auch die verwendeten Auswertungsroutinen (welche Daten werden mit welchen Kriterien und mit welchen Berechnungsprozeduren zueinander in Verhältnis gesetzt, kumuliert oderausgeschieden?) vollständig dokumentieren.

Über den Umfang, die Darstellungstiefe und den formellen Aufbau solcher für das Ermittlungs- und Strafverfahren bestimmter Programmbeschreibungen gibt es bislang keine Bestimmungen oder Kriterien. Als Mindeststandard ist zu verlangen, dass einem normal gebildeten Verfahrensbeteiligten der Arbeitsvorgang nachvollziehbar dargelegt wird.

In komplizierten Auswertungsfällen (z.B. Spezialistenprogramme zur Zahlungsfähigkeit) muss ggf. der Hersteller oder Anwender des Programms als Sach-verständiger oder sachverständiger Zeuge über die Programmeigenschaften angehört werden. Im

Normalfall dürfte die allgemein gehaltene Dokumentation der Auswertungsmethode reichen, die um Einzelfallbeispiele angereichert wird. In diesen normalen und einfachen Fällen kommt dem verwendeten Programm keine eigenständige Beweisbedeutung für die Beweisaufnahme zu. Erst bei komplizierten Datenauswertungsprozessen (z.B. mit komplexen Berechnungs- und Selektionsvorgängen) bedarf es im Einzelfall der weiteren Einvernahme eines Sachverständigen, der seine wertende Beurteilung bei der Datenauswahl darlegen muss.

Beschlagnahmebeschluss, Bestimmtheit (1997)

Das BVerfG [31] hat ausgeführt:

> "Ordnet ein Richter - etwa gleichzeitig mit dem Erlass eines Durchsuchungsbefehls - die Beschlagnahme von Gegenständen an, bevor diese in amtlichen Gewahrsam genommen worden sind, so muss er die Gegenstände so genau bezeichnen, dass keine Zweifel darüber entstehen, ob sie von der Beschlagnahmeanordnung erfasst sind." [32]

Während in einem Durchsuchungsbeschluss natürlich die als Beweismittel gesuchten Gegenstände ihrer Art, ihres Inhalts und ihrer Qualität nach definiert werden müssen, um die Durchsuchung unter dem Gesichtspunkt der Verhältnismäßigkeit sinnvoll zu beschränken, so handelt es sich dabei zunächst nur um eine allgemeine Beschreibung der für beweiserheblich angesehenen Beweisstücke. Bei der Beschlagnahmeanordnung handelt es sich hingegen um einen vollstreckbaren Titel, der das einzelne Beweisstück unverwechselbar individualisieren soll.

Über den Grad der Genauigkeit der Beschreibung besteht noch keine Klarheit. Nach meiner Meinung muss es bei schriftlichen Beweisstücken ausreichen, die Gebinde, in denen sie sich befinden, individuell zu beschreiben (äußere Beschreibung und Angabe von Aktenaufschriften, nicht aber eine detaillierte Angabe des Akteninhalts).

Die hier geschilderten Anforderungen führen regelmäßig dazu, dass kombinierte Durchsuchungs- und Beschlagnahmebeschlüsse wegen der Beschlagnahmeanordnung unwirksam sind, so dass der Ermittlungsbeamte aus eigener Entscheidungskompetenz die Beschlagnahme bei Gefahr in Verzug anordnen muss.

Verwertungsverbot (1997)

Das Landgericht Wiesbaden hat entschieden (LG Wiesbaden StrafV 88, 292 f., Leitsatz):

> "Sind die prozessualen Verstöße bei einer Durchsuchung so schwerwiegend, dass nach Abwägung aller Umstände das Interesse des Staates an der Tataufklärung gegenüber dem Interesse des betroffenen Bürgers am Schutz seiner Persönlichkeitssphäre zurücktreten muss, sind die bei einer solchen Durchsuchung gefundenen Unterlagen unverwertbar."

Die Entscheidung ist berechtigt und lange Zeit ein Einzelfall geblieben. 2002 hat das BVerfG schließlich bestimmt, dass ein Verwertungsverbot an Zufallsfunden besteht, wenn die ihrer Beschlagnahme zugrunde liegende Durchsuchungsanordnung rechtswidrig war. Eine solche "systematische Suche nach Zufallsfunden" ist von der Literatur und Rechtsprechung schon lange zuvor als unzulässig angesehen worden.

---

31 BverfG NStZ 92, 91, 92

32 so auch OLG Düsseldorf wistra 97, 77 f.)

Durchsuchungsbeschluss.

materielle Wirkungslosigkeit prozessual unwirksamer Beschlüsse

Präzisierung von Durchsuchungsbeschlüssen (1997)

Zum Thema ist auf zwei Beschlüsse der 2. Kammer des 2. Senats des BVerfG hinzuweisen:

Mit seinem Beschluss vom 03.09.1991 [33] hat das Gericht festgestellt, dass "ein Durchsuchungsbeschluss, der den Tatverdacht nur schlagwortartig erwähnt, darüber hinaus aber keinerlei tatsächliche Angaben über die aufzuklärenden Straftaten enthält, den denkbaren Inhalt der zu durchsuchenden Beweismittel nicht erkennen lässt und die neben der Wohnung zu durchsuchenden "anderen Räume" nicht bezeichnet," nicht den grundrechtlichen Anforderungen der Art. 13 Abs. 1 (Unverletzlichkeit der Wohnung) und Art 2 Abs. 1 GG (freie Entfaltung der Persönlichkeit) sowie dem Rechtsstaatsprinzip entspricht. In der Beschlussbegründung wird hervorgehoben, dass "eine Durchsuchung schon ihrer Natur nach regelmäßig schwerwiegend in die grundrechtlich geschützte Lebenssphäre des Betroffenen" eingreift, so dass der Richter mit dem Durchsuchungsbeschluss die Zwangsmaßnahme von vornherein angemessen begrenzen und "durch eine geeignete Formulierung ..." sicherstellen müsse, "dass der Eingriff in die Grundrechte messbar und kontrollierbar bleibt" [34]. Dies erfordert, dass der Beschluss nicht einfach mit dem "Verdacht des Mordes" begründet wird, sondern darüber hinaus auch tatsächliche Angaben über die konkrete Tat enthält. Ich schließe daraus, dass die prozessuale Tat, wegen der die Untersuchung geführt wird, in ihren Grundzügen entsprechend dem aktuellen Ermittlungsstand umgrenzt werden muss (allerdings unterhalb der Schwellen, die nach der Rechtsprechung zu § 200 StPO für die Umgrenzung der prozessualen Tat in der Anklageschrift und zu § 264 StPO für die Feststellung der prozessualen Tat im Urteil entwickelt worden sind).

Die formelhafte Einbeziehung von "Nebengelassen" in den Durchsuchungsort ist nach diesem Beschluss nicht zu beanstanden, wenn sie sich in unmittelbarer räumlicher Nähe zur Wohnung befinden. Weit entfernte "andere Räume" sind hingegen genau zu bezeichnen.

In einem weiteren Beschluss hat das BVerfG die hier skizzierten Grundzüge wiederholt und ergänzend ausgeführt, dass die im Durchsuchungsbeschluss vorzunehmende Begrenzung des Untersuchungsgegenstandes und -ortes den Betroffenen in den Stand versetzen soll, "die Durchsuchung seinerseits zu kontrollieren und etwaigen Ausuferungen im Rahmen seiner gesetzlichen Möglichkeiten von vornherein entgegenzutreten" [35].

Mit seinem Beschluss vom 05.05.2000 - 2 BvR 2212/99 [36] hat sich das Bundesverfassungsgericht den inhaltlichen Anforderungen an Durchsuchungsbeschlüsse gewidmet. Unter den Randnummern 6 bis 8 der offiziellen Veröffentlichung im Internet hat es ausgeführt:

---

[33] BVerfG NStZ 92, 91

[34] BVerfG ebd., S. 92

[35] BVerfG NJW 94, 3281, 3282

[36] BVerfG StV 2000, 465

"Ein Durchsuchungsbeschluss, der keinerlei tatsächliche Angaben über den Inhalt des Tatvorwurfs enthält und der zudem weder die Art noch den denkbaren Inhalt der Beweismittel, denen die Durchsuchung gilt, erkennen lässt, wird diesen Anforderungen jedenfalls dann nicht gerecht, wenn solche Kennzeichnungen nach dem Ergebnis der Ermittlungen ohne Weiteres möglich und den Zwecken der Strafverfolgung nicht abträglich sind. Die nur schlagwortartige Bezeichnung der mutmaßlichen Straftat und die Anführung des Wortlauts des § 102 StPO genügen in einem solchen Fall nicht (...).

b) Diese rechtsstaatlichen Mindestanforderungen erfüllt der Durchsuchungsbeschluss des Amtsgerichts nicht. Er enthält keinerlei tatsächliche Angaben zum Inhalt des Tatvorwurfs, obwohl dies ohne weiteres möglich gewesen wäre, sondern beschränkt sich auf den Hinweis "wegen Steuerhinterziehung". Nicht einmal die Art der angeblich hinterzogenen Steuern oder ein konkreter Straftatbestand werden genannt. Aus den beispielhaft angeführten Beweismitteln - "Aufzeichnungen und Rechnungen" - lässt sich auch kein Rückschluss auf den Inhalt des Tatvorwurfs ziehen. Zum Tatzeitraum fehlen ebenfalls jegliche Angaben. Damit hat das Amtsgericht die Begrenzung des Grundrechtseingriffs vollständig den die Durchsuchung durchführenden Beamten überlassen. "

Am 29.01.2002 hat das Bundesverfassungsgericht - 2 BVR 1245/01 - einschränkend ergänzt:

1. Die Verdachtsumschreibung reicht aus, um den Zweck der Durchsuchungsanordnung zu erfüllen, den Zugriff auf Beweisgegenstände bei Vollziehung der Durchsuchung zu begrenzen.

Insbesondere bei Beginn des Ermittlungsverfahrens kann noch keine genaue Einzelaktbeschreibung gefordert werden; ausreichend ist vielmehr eine gewisse Konkretisierung in tatsächlicher und rechtlicher Hinsicht. Erforderlich ist nur, dass die Tatschilderung über eine floskelhafte Beschreibung des Vorwurfs, etwa als "Abrechungsbetrug", hinausgeht.

2. Die Angabe der Indiztatsachen, auf die der Verdacht der Straftat gestützt wird, ist in einem Durchsuchungsbeschluss zwar möglich, aber von Verfassungs wegen nicht immer geboten.

Keine Unterbrechung der Verfolgungsverjährung

Aus der Rechtsprechung des Bundesverfassungsgerichts hat der Bundesgerichtshof im Beschluss vom 05.04.2000 - 5 StR 226/99 - [37] gefolgert:

"... die Durchsuchungs- und Beschlagnahmeanordnungen ... nennen weder die dem Beschuldigten zur Last liegenden Taten, noch bezeichnen sie die beweiserheblichen Unterlagen hinreichend konkret, sondern sprechen nur von den Unterlagen, die zur Aufklärung des - nicht näher bezeichneten - Sachverhalts dienlich sind. Die Anordnungen sind inhaltlich zu unbestimmt und konnten daher die Verfolgungsverjährung nicht wirksam unterbrechen.

[37] BGH wistra 2000, 219 ff.; S. 11 f. der Druckversion im Internet

Zwar sind insoweit die Anforderungen an die Bestimmtheit der Tat nicht hoch, da ihre Einzelheiten durch die Untersuchung erst ermittelt werden sollen. Ein Anfangsverdacht genügt (...); die Taten brauchen in ihren Einzelheiten nicht festzustehen (...). Sie müssen lediglich so individualisiert sein, dass sie von denkbaren ähnlichen oder gleichartigen Vorkommnissen zu unterscheiden sind. ...

... Die zum Zwecke der Auslegung der sachlichen Reichweite der Verjährungsunterbrechung grundsätzlich mögliche Heranziehung des Inhalts der Ermittlungsakten und des Durchsuchungsantrages (...) kann jedoch dann keine Verjährungsunterbrechung mehr bewirken, wenn die jeweilige Durchsuchungsanordnung selbst den verfassungsrechtlichen Mindestvoraussetzungen nicht standhält. Danach müssen schwerwiegende Eingriffe in die Lebenssphäre der Betroffenen messbar und kontrollierbar sein. Diesen Anforderungen wird aber nach der Rechtsprechung des Bundesverfassungsgerichts ein Durchsuchungsbefehl, der keinerlei tatsächliche Anhaltspunkte über den Inhalt des Tatvorwurfs enthält, jedenfalls dann nicht gerecht, wenn solche Angaben nach dem Ergebnis der Ermittlungen ohne weiteres möglich und den Zwecken der Strafverfolgung nicht abträglich sind (...). ... Zumindest die Bezeichnung des Straftatbestandes und der Steuerarten wäre aber im vorliegenden Fall neben der Nennung des Hinterziehungszeitraumes geboten gewesen. Dieser Mangel ist so schwerwiegend, dass die Durchsuchungsanordnungen keine verjährungsunterbrechende Wirkung entfalten konnten. ..."

Durchsuchungsbeschluss ist 6 Monate wirksam (1997)

Rechtsprechung und Literatur haben in der Vergangenheit übereinstimmend die Auffassung vertreten, dass ein einmal ergangener Durchsuchungsbeschluss solange wirksam und vollstreckbar bleibt, wie noch keine Verfolgungsverjährung eingetreten ist oder sich der Ermittlungsstand noch nicht wesentlich gegenüber den Erkenntnissen verändert hat, die der richterlichen Durchsuchungsentscheidung zugrunde lagen.

Das BVerfG hat nunmehr bestimmt, dass ein Durchsuchungsbeschluss spätestens nach Ablauf eines halben Jahres seine "rechtfertigende Kraft", also seine Wirksamkeit verliert [38]. Zur Begründung hebt das Gericht hervor, dass der Richter eine Durchsuchung nur anordnen darf, "wenn er sich aufgrund eigenverantwortlicher Prüfung der Ermittlungen überzeugt hat, dass die Maßnahme verhältnismäßig ist" [39]. Mit zunehmendem Zeitablauf könnte sich nicht nur die Beurteilungsgrundlage geändert haben, sondern würde "die konkrete richterliche Beschränkung des Grundrechtseingriffs zu einer Blankettermächtigung geworden" sein [40].Von dem Vollzug der Durchsuchungsanordnung könne zwar vorläufig abgesehen werden. Dies dürfe aber nicht dazu führen, "dass der Staatsanwalt sich eine Durchsuchungsanordnung gewissermaßen auf Vorrat besorgt oder diese doch vorrätig hält" [41]. Deshalb ist "spätestens nach Ablauf eines halben Jahres ... davon auszugehen, dass die richterliche Prüfung nicht mehr die rechtlichen Grundlagen einer beabsichtigten

[38] BVerfG wistra 97, 223 ff.

[39] ebd., S. 225

[40] ebd.

[41] ebd.

Durchsuchung gewährleistet und die richterliche Anordnung nicht mehr den Rahmen, die Grenzen und den Zweck der Durchsuchung im Sinne eines effektiven Grundrechtsschutzes zu sichern vermag" [42].

Durchsuchungsbeschluss. Rechtsschutz nach Abschluss der Maßnahme (1997)

Nach früherer h. M. ist die gerichtliche Überprüfbarkeit von Durchsuchungsbeschlüssen dann "prozessual überholt", also ein darauf gerichtetes Rechtsmittel unzulässig gewesen, wenn die Durchsuchungsmaßnahme abgeschlossen ist und sich deshalb der Streit um die Durchsuchungsanordnung als solche erledigt habe. Diese Auffassung hat das BVerfG jetzt unter Aufgabe seiner bisherigen Rechtsprechung abgelehnt [43].

Das Gericht verlangt eine wirkliche Kontrolle von grundrechtseingreifenden Maßnahmen und spricht deshalb nach den Grundsätzen der Rechtsweggarantie aus Art. 19 Abs. 4 GG den Betroffenen das Recht zu, "in Fällen tiefgreifender, tatsächlich jedoch nicht mehr fortwirkender Grundrechtseingriffe auch dann die Berechtigung des Eingriffs gerichtlich klären zu lassen, wenn die direkte Belastung durch den angegriffenen Hoheitsakt sich nach dem typischen Verfahrensablauf auf eine Zeitspanne beschränkt, in welcher der Betroffene die gerichtliche Entscheidung in der von der Prozessordnung gegebenen Instanz kaum erlangen kann" [44].

Das BVerfG reagiert mit dieser Entscheidung auf die Besonderheiten der Durchsuchungsanordnung im Ermittlungsverfahren, die einerseits von einem erheblichen Eingriff in Grund-rechte geprägt ist und andererseits - ihrer Natur nach - ohne rechtliches Gehör ergeht (§ 33 Abs. 4 StPO), so dass der Betroffene allein auf die tatsächliche Durchführung der Maßnahme mit rechtsstaatlichen Mitteln reagieren kann. Mit der richterlichen (oder staatsanwaltlichen oder polizeilichen) Eingriffsentscheidung wird er zugleich mit ihrer Durchführung konfrontiert, er kann sie nicht verhindern, kaum steuern (bei Widerstandshandlungen kann der Betroffene als Störer behandelt werden [§ 164 StPO] und etwaige Rechtsmittel haben keine aufschiebende Wirkung) und ist nach bisheriger Praxis sogar von der nachträglichen richterlichen Überprüfung ausgeschlossen gewesen.

Für diese Entscheidung habe ich sehr viel Verständnis, auch wenn sie die gerichtliche Praxis nachhaltig erschweren kann.

Die größten Probleme wird der Standardfall in Wirtschaftsstrafsachen hervorrufen, wenn Staatsanwaltschaft und Polizei aufgrund eines berechtigten gerichtlichen Durchsuchungsbeschlusses eine Durchsuchung durchführen und schließlich abschließen, dabei Beweismittel finden und mangels freiwilliger Herausgabe rechtmäßig beschlagnahmen. Der Betroffene kann sodann sowohl gegen den Durchsuchungsbeschluss Beschwerde erheben wie auch gegen die Beschlagnahme um eine richterliche Bestätigung ersuchen. Daraufhin wird die Staatsanwaltschaft die Vorgänge dem Ermittlungsrichter vorlegen, der einerseits über die Nichtabhilfe aufgrund der Beschwerde gegen seinen Durchsuchungsbeschluss befinden und andererseits durch Beschluss die polizeiliche oder staatsanwaltliche Beschlagnahme bestätigen wird. Die richterli-

---

42 ebd., S. 226

43 BVerfG wistra 97, 219 ff.

44 BVerfG ebd., 219, Leitsatz 2.a

che Bestätigung der Beschlagnahme wird dem Betroffenen zugestellt und die Vorgänge auf die Nichtabhilfe des Ermittlungsrichters dem Landgericht zur Beschwerdeentscheidung vorgelegt. Während das Landgericht über die Beschwerde gegen die Durchsuchungsanordnung entscheidet, wird der Betroffene womöglich gegen die richterliche Bestätigung der Beschlagnahme Beschwerde erheben, so dass die Vorgänge nach Rückkehr vom Landgericht erneut dem Ermittlungsrichter zur Abhilfeentscheidung und schließlich nochmals dem Landgericht zur Beschwerdeentscheidung über die Beschlagnahme vorgelegt werden müssen.

Dieser Musterfall zeigt plakativ die zu erwartenden Probleme und Verzögerungen. Ich meine, dass die Praxis einheitliche Entscheidungen treffen und in einem Rechtszug die Durchsuchungs- und die Beschlagnahmeanordnungen überprüfen sollte. Dies verlangt von den Beschwerdegerichten, dass sie mit ihrer Entscheidung über die Durchsuchung von Amts wegen auch die Beschlagnahmen überprüfen würden, auch wenn sie noch nicht durch gesonderte Rechtsmittel angefochten wurden. Der Rechtsweg zum Oberlandesgericht würde dadurch nicht eröffnet werden, weil das Beschwerdegericht als zweite und letzte Instanz auch die Beschlagnahme auf das Rechtsmittel gegen die zugrundeliegende Durchsuchungsanordnung überprüft.

Anmerkung: Die mangelhafte Sensibilität mancher Strafverfolger und Gerichte zeigt sich in einer ganzen Reihe von obergerichtlichen Entscheidungen:

Gerichte und Staatsanwaltschaften, die meinen, man könne Steuerhinterziehungen über länger als 25 Jahre verfolgen, müssen sich nicht wundern, wenn der BGH daraufhin zu der Auffassung kommt, dass die Rechtskonstruktion der fortgesetzten Handlung wegfallen müsse.

Staatsanwälte und Polizeibeamte, die in einem Ermittlungsverfahren nichts veranlassen, müssen sich nicht wundern, wenn das BVerfG meint, eine plötzliche Vollstreckung eines zwei Jahren alten Durchsuchungsbeschlusses müsse dem Verhältnisgrundsatz widersprechen.

Und Staatsanwälte und Gerichte, die auf gar keiner, aufgrund einer ganz "dünnen" Tatsachengrundlage oder einer wenn nicht unüberlegten, so doch undifferenzierten Tatbestandsprüfung grundrechtsrelevante Entscheidungen treffen und entsprechende Maßnahmen durchführen, dürfen sich auch nicht wundern, wenn das BVerfG die Notwendigkeit einer nachträglichen Überprüfung im gerichtlichen Instanzenzug hervorhebt.

So ist es geschehen.

Geschlossenes Rechtsschutzsystem

Andrea Laser [45] hat zusammenfassend festgestellt:

> Es "hat sich nun in der Rechtsprechung eine einheitliche Linie ausgehend vom BVerfG über die Fachgerichte entwickelt. Rechtsschutz ist durch die Beschwerde gem. §§ 304 ff. StPO oder über den Antrag nach § 98 II 2 StPO zu erlangen. Die Fachgerichte sind der Aufforderung des BVerfG, das geltende Rechtsmittelsystem zu vereinheitlichen, in zahlreichen Entscheidungen nachgekommen.
>
> Soweit vereinzelte Unterfallgruppen noch nicht ausdrücklich entschieden sind ..., lässt jedoch die bisherige Entwicklung darauf schließen, dass auch hier zufriedenstellende Ergebnisse gefunden werden. Die Obergerichte haben in ihren Entscheidungen immer wieder die Unpraktikabilität von § 23 EGGVG hervorgehoben und auf dessen Subsidiarität hingewiesen. Die Strafprozessordnung stellt selbst ausreichende Rechtsschutzmöglichkeiten zur Verfügung.
>
> Auf Grund dessen besteht für den Gesetzgeber keine Veranlassung, neue gesetzliche Regelungen zu schaffen. Dem Betroffenen stehen in ausreichendem Maß Möglichkeiten zur Verfügung, seine Rechte geltend zu machen, ohne dass dabei Rechtsschutzlücken auftreten."

[45] Das Rechtsschutzsystem gegen strafprozessuale Zwangsmaßnahmen, NStZ 01, 120 ff., 124

Gefahr im Verzug, Durchsuchungsanordnung

Urteil des BVerfG vom 20.02.01 - 2 BvR 1444/00

Leitsätze des Gerichts:

1. a) Der Begriff "Gefahr im Verzug" in Art. 13 Abs. 2 GG ist eng auszulegen; die richterliche Anordnung einer Durchsuchung ist die Regel, die nichtrichterliche die Ausnahme.

   b) "Gefahr im Verzug" muss mit Tatsachen begründet werden, die auf den Einzelfall bezogen sind. Reine Spekulationen, hypothetische Erwägungen oder lediglich auf kriminalistische Alltagserfahrung gestützte, fall-unabhängige Vermutungen reichen nicht aus.

2. Gerichte und Strafverfolgungsbehörden haben im Rahmen des Möglichen tatsächliche und rechtliche Vorkehrungen zu treffen, damit die in der Verfassung vorgesehene Regelzuständigkeit des Richters auch in der Masse der Alltagsfälle gewahrt bleibt.

3. a) Auslegung und Anwendung des Begriffs "Gefahr im Verzug" unterliegen einer unbeschränkten gerichtlichen Kontrolle. Die Gerichte sind allerdings gehalten, der besonderen Entscheidungssituation der nichtrichterlichen Organe mit ihren situationsbedingten Grenzen von Erkenntnismöglichkeiten Rechnung zu tragen.

   b) Eine wirksame gerichtliche Nachprüfung der Annahme von "Gefahr im Verzug" setzt voraus, dass sowohl das Ergebnis als auch die Grundlagen der Entscheidung in unmittelbarem zeitlichen Zusammenhang mit der Durchsu-

chungsmaßnahme in den Ermittlungsakten dargelegt werden.

Anordnung der Durchsuchung beim Verdächtigen bei Gefahr im Verzug

Anmerkung zum Urteil des Bundesverfassungsgerichts vom 20.02.2001 - 2 BvR 1440/00

Die Entscheidung ist nicht überraschend, die Praxisprobleme bei der Anordnung von Durchsuchungen bei Gefahr im Verzug sind nicht neu und eigentlich bin ich nur davon überrascht, dass eine Entscheidung des Bundesverfassungsgerichts ergehen musste.

a) Gefahr im Verzug (GiV) bedeutet, dass eine richterliche Entscheidung entweder deshalb nicht erwirkt werden kann, weil ein zuständiger Richter nicht erreichbar ist, oder bereits in der Zeit, die für eine Unterrichtung des Richters erforderlich ist, ein Verlust von Beweismitteln zu befürchten ist.

In den Worten des BVerfG (Rn. 40):

> "Die Strafverfolgungsbehörden müssen regelmäßig versuchen, eine Anordnung des instanziell und funktionell zuständigen Richters zu erlangen, bevor sie eine Durchsuchung beginnen. Nur in Ausnahmesituationen, wenn schon die zeitliche Verzögerung wegen eines solchen Versuchs den Erfolg der Durchsuchung gefährden würde, dürfen sie selbst die Anordnung wegen Gefahr im Verzug treffen, ohne sich zuvor um eine richterliche Entscheidung bemüht zu haben. ... Dem korrespondiert die verfassungsrechtliche Verpflichtung der Gerichte, die Erreichbarkeit eines Ermittlungsrichters, auch durch die Einrichtung eines Eil- oder Notdienstes, zu sichern."

b) Auch unter den geringen gesetzlichen Anforderungen für eine Durchsuchung bei dem Verdächtigen (§ 102 StPO) müssen konkrete Tatsachen nach kriminalistischer Erfahrung die Erwartung rechtfertigen, dass am Durchsuchungsort Beweismittel gefunden werden.

In den Worten des BVerfG (Rn. 38):

> "Im Konkreten sind reine Spekulationen, hypothetische Erwägungen oder lediglich auf kriminalistische Alltagserfahrung gestützte, fallunabhängige Vermutungen als Grundlage einer Annahme von Gefahr im Verzug nicht hinreichend. Gefahr im Verzug muss mit Tatsachen begründet werden, die auf den Einzelfall bezogen sind. Die bloße Möglichkeit eines Beweismittelverlusts genügt nicht."

c) Wenn eine GiV-Entscheidung getroffen wird, dann müssen die wesentlichen Gründe für die Entscheidung und die Entscheidung als solche nachträglich, aber zeitnah, zu den Akten dokumentiert werden. Dies umfasst sowohl die Voraussetzungen der GiV wie auch die Gründe für die Eingriffsentscheidung selber. Nur so lässt sich, z.B. in einer Jahre später stattfindenden Hauptverhandlung, nachvollziehen, welche Entscheidungsgrundlagen bestanden und wie der anordnende Beamte zu seiner Würdigung der Sachlage gelangt ist.

In den Worten des BVerfG (Rn. 54):

> "Eine wirksame gerichtliche Nachprüfung einer nichtrichterlichen Durchsuchungsan-

ordnung wegen Gefahr im Verzug setzt voraus, dass der handelnde Beamte vor oder jedenfalls unmittelbar nach der Durchsuchung seine für den Eingriff bedeutsamen Erkenntnisse und Annahmen in den Ermittlungsakten dokumentiert. Insbesondere muss er, unter Bezeichnung des Tatverdachts und der gesuchten Beweismittel, die Umstände darlegen, auf die er die Gefahr des Beweismittelverlusts stützt. ... Zudem führt die Pflicht zur Dokumentation vor oder jedenfalls unmittelbar nach dem Eingriff dazu, dass sich der anordnende Beamte in besonderem Maße der Rechtmäßigkeit seines Handelns vergewissert und dass er überdies im Falle der Nachprüfung dieses Handelns auf dokumentierte Tatsachen wird verweisen können, die sein Handeln erklären."

Eine Dokumentation vor der Durchführung der Durchsuchung halte ich entgegen den Ausführungen des BVerfG-Urteils in aller Regel für ausgeschlossen. Entweder es besteht Zeitnot und Handlungsbedarf, dann muss die Eingriffsmaßnahme auch sofort vorbereitet und durchgeführt werden, oder sie bestehen nicht, so dass auch keine GiV besteht.

Die Dokumentationspflicht geht nach den Worten des BVerfG (Rn. 55) in eine Begründungspflicht für die Strafverfolgungsbehörden über:

"Auf der Grundlage dieser Dokumentation haben die Strafverfolgungsbehörden ihre Durchsuchungsanordnung in einem späteren gerichtlichen Verfahren zu begründen [46]. Ihre Ausführungen müssen sich auf die gesetzlichen Voraussetzungen der Durchsuchung (§§ 102 ff. StPO) erstrecken. Außerdem müssen sie darlegen, warum eine richterliche Anordnung zu spät gekommen wäre, und gegebenenfalls, warum von dem Versuch abgesehen wurde, eine richterliche Entscheidung zu erlangen."

d) Zutreffend und wichtig finde ich, was das BVerfG zu den Anforderungen an die Gerichte ausgeführt hat, die die GiV-Entscheidungen zu überprüfen haben (Rn. 51, 52):

"Die Kontrolle einer Durchsuchungsanordnung der Strafverfolgungsbehörden wegen Gefahr im Verzug muss die faktischen Bedingungen polizeilichen und staatsanwaltschaftlichen Handelns in der Situation, um die es geht, zur Kenntnis nehmen und verarbeiten. Der Richter darf nicht seine - ohne zeitlichen Druck und unter Berücksichtigung der weiteren Entwicklung gewonnene - nachträgliche Einschätzung der Lage an die Stelle der Einschätzung der handelnden Beamten setzen. Vielmehr muss das konkrete Handlungsfeld der Beamten, das der Richter gegebenenfalls aufzuklären hat, Ausgangspunkt seiner Prüfung sein. Er muss darauf Bedacht nehmen, unter welchen Bedingungen die Beamten über eine Durchsuchung mit oder ohne richterliche Anordnung entschieden haben und welcher zeitliche Rahmen ihnen gesteckt war. Er hat zu berücksichtigen, wie groß der Beurteilungs- und Handlungsdruck war oder ob ausreichend Zeit für Rücksprachen mit Kollegen und Vorgesetzten sowie zwischen Polizei und Staatsanwaltschaft bestand. Er muss ferner die situationsbedingten Grenzen von Erkenntnismöglichkeiten in Rechnung stellen, deren mögliche Unvollständigkeit und vorläufige Natur.

[46] vgl. BVerfGE 6, 32 <44 f.>; 49, 24 <66 f.>

Auf dieser Grundlage hat der Richter die von den Strafverfolgungsbehörden getroffene Einschätzung der konkreten Situation nachzuvollziehen. Beruht diese Einschätzung auf den einschlägigen Tatsachen und ist sie nach der Sachlage, wie sie sich den handelnden Amtsträgern darstellte, nahe liegend oder jedenfalls plausibel, so darf der Richter sie bei seiner Entscheidung als zutreffend zu Grunde legen, wenn nicht konkrete Anhaltspunkte dafür ersichtlich sind, dass die getroffene Einschätzung mit der eines sachkundigen und pflichtgemäß handelnden Strafverfolgungsbeamten nicht in Einklang zu bringen ist."

Insoweit besteht auch eine Aufklärungspflicht durch das Gericht (Rn. 63).

Sachverständige im Ermittlungsverfahren

Den Einsatz von Sachverständigen im gerichtlichen Strafverfahren regelt § 73 StPO:

§ 73 [Auswahl der Sachverständigen]

(1) Die Auswahl der zuzuziehenden Sachverständigen und die Bestimmung ihrer Anzahl erfolgt durch den Richter. Er soll mit diesen eine Absprache treffen, innerhalb welcher Frist die Gutachten erstattet werden können.

(2) Sind für gewisse Arten von Gutachten Sachverständige öffentlich bestellt, so sollen andere Personen nur dann gewählt werden, wenn besondere Umstände es fordern.

Die Rechtsprechung verlangt von der Staatsanwaltschaft und der Polizei, dass sie die in § 73 Abs. 2 StPO vorgesehenen Auswahlkriterien ebenfalls berücksichtigen müssen, wenn sie in eigener Ermittlungskompetenz Sachverständige einsetzen (§§ 161, 163 StPO).
Danach gilt grundsätzlich folgende Auswahlreihenfolge:

1) beamtete Sachverständige (Fachämter, Hochschullehrer)

2) öffentlich bestellte, vereidigte Sachverständige (Industrie- und Handelskammer)

3) sonstige unparteiische Sachverständige

4) bei Verfahrensbeteiligten angestellte Sachverständige

Wegen der unter Nr. 4) genannten angestellten Sachverständigen sind besondere Vorkehrungen zu treffen. Ihre Auswahl kommt nur dann in Betracht, wenn sie Aus-

kunft zu hochgradig spezialisierten Fachfragen geben sollen und kein vergleichbar qualifizierter Sachverständiger aus den anderen drei Gruppen zur Verfügung steht - und sich auch nicht in angemessener Zeit einarbeiten könnte. Dies ist z.B. der Fall bei hochwertigen und gleichzeitig komplexen Fertigungsmaschinen, bei der Beurteilung chemischer Fertigungstechniken oder zur Wiedererkennung handwerklicher oder individuell angepasster Produkte.

Bei ihrem Einsatz ist darauf zu achten, dass der angestellte Sachverständige keine Kenntnisse von den Geschäftsgeheimnissen des Durchsuchungsbetroffenen erlangt. Dies zwingt in aller Regel dazu, sie z.B. nicht kontinuierlich an einer Durchsuchung teilnehmen zu lassen, sondern sie nur punktuell beizuziehen, wenn ihre Fachkompetenz zwingend benötigt wird.

Zweifel an der vom Gesetz verlangten Unparteiligkeit von sachverständigen Fachleuten können auch auftreten, wenn sie Angestellte eines gewerblichen Interessenverbandes sind.

Ich will dies am Beispiel der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. (GVU) erläutern.

Die Struktur der GVU beruht auf 4 Säulen:

Ermittlungsabteilung: Bundesweit befanden sich 1998 sieben dezentral tätige Ermittler im Einsatz.

Die Rechtsabteilung "überprüft" die "aufgrund der Aktivitäten erlangten Informationen" auf ihre strafrechtliche Bedeutung, tritt "mit inhaltlich und formell optimalem Beweismaterial an die Strafverfolgungsbehörden heran und stellt (die) ggf. notwendigen Strafanträge" (Hervorhebung im Text).

Die Hauptaufgabe der Technischen Abteilung "ist die Erstellung forensischer Gutachten für die Gerichte".

Controlling: Stabs- und Verwaltungsabteilung.

Die GVU beschränkt sich faktisch auf die "Bekämpfung von Urheberrechtsverletzungen mit den Mitteln des Strafrechts" (Hervorhebung im Text) und berühmt sich besonders der "Erfolge der Arbeit der GVU" anlässlich ihrer Mitwirkung "an über 7.000 (siebentausend) Strafverfahren" (Hervorhebung im Text). Auf ihrer Homepage beschreibt sie zusammenfassend ihre Arbeit wie folgt:

> "Alle von den Ermittlern gesammelten Informationen werden auf ihre strafrechtliche Relevanz überprüft.
>
> Beweismittel und Berichte der Ermittler werden zusammengefasst und den Strafverfolgungsbehörden zur Verfügung gestellt.
>
> Das gesamte Strafverfahren wird bis zum erfolgreichen Abschluss mit vielschichtigen Informationen begleitet.
>
> Parallel dazu wird für jede Mitgliedsfirma auf Wunsch das strafrechtliche Beweismaterial zur Durchführung zivilrechtlicher Maßnahmen aufbereitet."

Es entspricht praktischen Erfahrungen, dass die Ermittler der GVU auch zu polizeilichen Ermittlungen als Durchsuchungshelfer beigezogen werden und von der Polizei die dabei sichergestellten Daten zur Auswertung erhalten. Die GVU erhält dadurch strafprozessual erhobene Beweismittel, die sie auf urheberrechtsrelevante Bestandteile untersucht. Insoweit wird sie noch als Sach-

verständige der Kategorie 3) tätig. Wenn die GVU dann aber auch namens ihrer Mitgliedsfirmen Strafanträge stellt oder sogar außerhalb der Kontrolle der Vorschriften über die Akteneinsicht das von der Polizei aufgrund hoheitlicher Maßnahmen gewonnene "Beweismaterial zur Durchführung zivilrechtlicher Maßnahmen aufbereitet", dann handelt sie insgesamt parteiisch.

Ich meine, die Aufgaben als Durchsuchungshelfer und Sachverständige einerseits und Interessenvertreter ihrer Mitglieder müssen strikt getrennt werden.

Schützenhilfe für diese Meinung bekomme ich auch aus der Zivilrechtsprechung:

M. Michael König [47] bespricht das Urteil des Kammergerichts Berlin (KG) vom 11.08.00 - 5 U 3069/00 -, das auch in Verfahren des einstweiligen Rechtsschutzes den Einsatz parteieigener Sachverständiger verbietet und unparteiische Sachverständige verlangt.

In jenem Fall hatte MS Hinweise darauf erhalten, dass ein Unternehmen, das Schulungen für MS-Office-Programme veranstaltet und eine Lizenz für mehrere Office-Pakete hatte (aber nur einen Original-Datenträger; das ist üblich so), eine Kopie vom Original-Datenträger hergestellt haben und davon die Installation auf mehreren PCs vorgenommen haben soll.

Allein die Tatsache, dass eine Kopie der Original-CD angelegt wird, rechtfertigt nach Meinung des KGs nicht die Annahme, dass auch gegen die Lizenzbedingungen verstoßen wird. Diese haben nämlich die Installation mehrerer Office-Pakete mit demselben Datenträger vorgesehen (was die MS-Anwälte, wie es scheint, in ihrem Antrag auf Einstweilige Verfügung nicht dargelegten). Das KG folgert daraus, dass bereits kein Verfügungsgrund vorgelegen hat (also kein Titel hätte erlassen werden dürfen, so dass auch kein Gerichtsvollzieher zur Vollstreckung des Titels hätte herangezogen werden können).

Ich sehe mich deshalb auch wegen eines anderen Problems vom KG bestätigt:

Datensicherung - auch von Basis-Datenträgern - ist im Interesse eines professionellen, mithin "kunstgerechten" Umgangs mit Programmen erforderlich und deshalb auch zulässig. Dies gilt umso mehr, wenn ein Unternehmen nur einen Original-Datenträger besitzt, davon aber eine Mehrzahl von Installationen herstellen darf. Das Original gehört verschlossen; die Installationen sind mittels einer Kopie zu machen. Wenn die Kopie dabei physikalisch geschädigt wird, was in der Praxis nicht auszuschließen ist, kann vom Original ohne übermäßigen Aufwand eine neue Kopie hergestellt werden.

---

[47] Halt geboten. Einstweilige Verfügung Microsofts war zu weit gegangen, c't 12/02, S. 206

Bankauskünfte und Bankunterlagen
Sach- und Personenbeweise, Zeugenpflichten

Kreditinstitute und Banken weigern sich häufig, aufgrund eines Auskunftsersuchens der Staatsanwaltschaft schriftliche (zeugenschaftliche) Auskünfte über das Bestehen von Kontoverbindungen, über Kontoinhaber und Zeichnungsberechtigte, über Kreditlinien, Kontobewegungen und -salden zu erteilen. Darüber hinaus wird die Erstellung von Kontoverdichtungen (auch "Kontostaffeln" [48]) und ganz besonders die Herausgabe von Belegen, von deren Ablichtungen und letztlich auch von ganzen Aktenstücken (Kreditakten, Protokolle des Kreditausschusses usw.) verweigert. In diesen Fällen wird auf ein gegenüber den Kunden bestehendes Bankgeheimnis hingewiesen und bekundet, die Auskünfte und Herausgaben nur aufgrund eines "gerichtlichen Beschlusses" vornehmen zu können. Im Ergebnis wird von den Banken und Kreditinstituten ein Branchen-Sonderrecht behauptet, das auf einen generellen Richtervorbehalt gegenüber staatsanwaltlichen Ermittlungshandlungen hinausläuft.

Die Rechtsprechung und Literatur haben in der Vergangenheit mehrere Richtungswechsel vollzogen. Im Ergebnis ist festzustellen, dass die Staatsanwaltschaft im Fall der Weigerung eigenständig das Zwangsmittel des Ordnungsgeldes wegen zeugenschaftlicher Auskünfte anordnen kann und wegen dieser Auskünfte und wegen der Verweigerung der Herausgabe sachlicher Beweismittel beantragen kann, ohne dass es zunächst einer richterlichen Wiederholung der Ersuchen bedarf.

Zusammenfassung der Ergebnisse:

1. Der Gesetzgeber zur Strafprozessordnung geht davon aus, dass der normale Bürger die Strafverfolgungsbehörden bei ihrer Arbeit unterstützt und bereitwillig Auskünfte gibt oder Beweismittel zur Verfügung stellt.

   Diese Aussage klingt banal und steht nirgendwo im Gesetz. Gleichwohl entspricht sie den dokumentierten Motiven des Gesetzgebers und die herrschende Meinung ist sich darüber einig. Das dem zugrunde liegende gesetzliche und verfassungsrechtliche Leitbild sieht vor, dass die Öffentlichkeit ein besonders schützenswertes Interesse an einer funktionstüchtigen, effektiven und Gleichheit verwirklichenden Strafrechtspflege hat.

2. Abwehr- und Verweigerungsrechte sieht das Prozessrecht für persönliche Konfliktlagen vor. Dies sind zunächst die Zeugnis- und Auskunftsverweigerungsrechte der Angehörigen (§ 52 StPO [49]) und der Berufshelfer (§ 53 StPO). Hieraus werden in § 97 Abs. 1 StPO Beschlagnahmeverbote abgeleitet, die ihrerseits von den Detailregelungen der Folgeabsätze beschränkt werden. Im Interesse des besonderen Schutzes der Vertraulichkeitsbeziehung zwischen Verteidiger und Beschuldigtem hat die Rechtsprechung ein erweitertes Beschlagnahmeverbot für Verteidigungs korrespondenz in der Hand des Be-

[48] Bittmann, Das Beiziehen von Kontounterlagen im staatsanwaltlichen Ermittlungsverfahren, wistra 90, 326

[49] Die Zitatquellen wurden überwiegend aus einem Aufsatz aus dem Jahr 1997 übernommen.

schuldigten postuliert (Argument aus § 148 StPO).

3. Das Kreditwesen / die Banken sind keine Berufshelfer im Sinne des § 53 StPO.

   Kurz gesagt: Im Strafverfahrensrecht gibt es kein geschütztes Bankgeheimnis.

4. § 161a StPO ermächtigt die Staatsanwaltschaft, Zeugen und Sachverständige sanktionsbewehrt (Ordnungsgeld) zu laden und zu vernehmen.

   In Rechtsprechung und Literatur wird anerkannt, dass anstelle einer mündlichen Aussage in geeigneten Fällen auch schriftliche Aussagen gefordert werden dürfen, deren Verweigerung ebenfalls die Sanktionen des § 161a StPO auslösen können.

5. Das staatsanwaltliche Auskunftsersuchen beschränkt sich auf personenbeweisliche Beweismittel, also auf solche Auskünfte, die durch die Vernehmung von Zeugen und Sachverständigen erhoben werden können.

   Im Zusammenhang mit Bankauskünften sind dies unzweifelhaft Angaben über das Bestehen von Kontoverbindungen, Depots, Kreditlinien, Scheckproteste, Kündigungen, Zeichnungsbefugnisse und einzelne Kontobewegungen.

6. Über den Umfang der Auskunftspflicht bei Kontobewegungen besteht Streit.

   Einzelne Banken akzeptieren Auskunftsersuchen, wenn ein bestimmter Auskunftszeitraum nicht überschritten wird.

   Bei der Verweigerung von Auskünften über Kontobewegungen über längere Zeiträume wird darauf verwiesen,

   dass insoweit die Auskünfte nicht durch die Vernehmung einzelner Zeugen erhoben werden könnten,

   dass Zeugen keiner Editionspflicht für Wahrnehmungen unterlägen, die außerhalb ihres eigenen Wahrnehmungsbereiches lägen,

   und dass diese Auskünfte dem Sachbeweis unterlägen (Zusammenstellen von Kontobelegen).

7. Gemäß § 94 Abs. 1 StPO ist grundsätzlich jedermann zur Herausgabe von (sachlichen) Beweismitteln verpflichtet.

   Diese Verpflichtung wird von den Beschlagnahmeverboten in § 97 StPO und dem Verhältnismäßigkeitsgrundsatz begrenzt, der hingegen im Interesse einer funktionstüchtigen Strafrechtspflege nur in seltenen Ausnahmefällen zu einem Beweiserhebungsverbot führen kann.

8. Das Gesetz kennzeichnet grundsätzlich zwei Wege, wie im Falle der Verweigerung die Herausgabe von Beweismitteln erzwungen werden kann.

   Gemäß § 94 Abs. 2 StPO können Beweismittel beschlagnahmt werden. Hierzu sind gemäß § 98 StPO der Richter und unter der weiteren Voraussetzung, dass Gefahr im Verzug besteht, der Staatsanwalt oder seine Hilfsbeamten (§ 152 GVG) befugt.

9. § 95 Abs. 1 StPO bestimmt ferner, dass Beweismittel auf Verlangen von ihrem Gewahrsamsinhaber herauszugeben sind. Verweigert er dies, so können vom Richter gemäß § 95 Abs. 2 in Verbindung mit § 70 StPO Ungehorsamsfolgen angeordnet werden: Ordnungsgeld, Ordnungs- und Erzwingungshaft.

Über die Frage, wer die Herausgabe mit Sanktionsfolgen verlangen darf, hat Streit bestanden. Die Mehrzahl der Stimmen in der Literatur sprechen sich dafür aus, dass das Herausgabeverlangen wirksam nur von einem Richter ausgesprochen werden kann, weil im Regelfall nur ihm die Beschlagnahmebefugnis aus den §§ 94 Abs. 2, 98 Abs. 1 StPO zustehe.

10. Die Gegenmeinung ist der Auffassung, dass auch erfolglose staatsanwaltliche und polizeiliche Auskunftsersuchen die Sanktionsfolgen des § 95 Abs. 2 StPO auslösen können.

    Nachdem zunächst nur das LG Lübeck [50] diese Auffassung vertreten hat, sind inzwischen auch das LG Gera [51] und das LG Halle [52] auf diese Position eingeschwenkt. Bittmann [53] würdigt diese Entwicklung positiv und m.E. zutreffend.

11. Unstrittig ist auf jedem Fall, dass die Sanktionen des § 95 Abs. 2 StPO nur vom Richter angeordnet werden können.

    Strittig ist hingegen, ob die Anordnung von Sanktionen ein richterliches Herausgabeersuchen voraussetzt oder ob ein solches der Ermittlungsbehörden ausreicht.

    Im Anschluss an die unter Nr. 10 genannten Entscheidungen halte ich (jetzt) ein staatsanwaltliches oder polizeiliches Herausgabeverlangen für ausreichend.

Einzelheiten:

1. Kein strafprozessuales Bankgeheimnis

In Literatur und Rechtsprechung wird einheitlich ein privatrechtliches Bankgeheimnis anerkannt, das zu der Verpflichtung der Banken führt, die Vermögensverhältnisse ihrer Kunden gegenüber Dritten geheim zu halten. Diese Geheimhaltungspflicht ergibt sich auch ohne besondere Vereinbarung nach Treu und Glauben aus der Vertragsbeziehung zwischen der Bank und ihrem Kunden. Sie findet ihre Grenze in öffentlichrechtlichen Auskunftspflichten (z.B. gegenüber dem Bundesaufsichtsamt für das Kreditwesen, gegenüber den Finanzämtern und selbstverständlich auch gegenüber Gerichten und Staatsanwaltschaften).

---

[50] NJW 2000, 3148 f.; Beschluss des LG Lübeck vom 03.02.00 - 6 Qs 3/00 -

Leitsatz:
Die Staatsanwaltschaft kann in eigener Zuständigkeit Kontounterlagen vom Geldinstitut gem. § 95 I StPO herausverlangen. Eine richterliche Anordnung ist nicht erforderlich.

[51] NStZ 2001, 276; Beschluss des LG Gera vom 30.09.99 - 2 Qs 412/99 -;

Leitsatz:
Für das Herausgabeverlangen nach § 95 I StPO ist neben dem Richter auch die StA zuständig, und zwar auch dann, wenn Gefahr im Verzug nicht besteht.

[52] NStZ 01, 276 f.; Beschluss des LG Halle vom 06.10.99 - 22 Qs 28/99 -;

Leitsätze: 1. Für das Herausgabeverlangen nach § 95 I StPO ist neben dem Richter auch die StA zuständig, und zwar auch dann, wenn Gefahr im Verzug nicht besteht. 2. Beschlagnahmemöglichkeit (§ 94 II StPO) und Herausgabeverlangen (§ 95 StPO) stehen grundsätzlich gleichrangig nebeneinander. Ein Herausgabeverlangen kommt aber nur dann in Betracht, wenn eine Beschlagnahme zur Sicherstellung der benötigten Beweismittel faktisch ungeeignet ist.

[53] Bittmann, Das staatsanwaltliche Auskunftsverlangen gemäß § 95 StPO, NStZ 01, 231 ff.

Für das Besteuerungsverfahren bestehen besondere Regelungen. In § 93 Abs. 1 bis Abs. 4 AO wird die Auskunftspflicht Dritter ausdrücklich bestimmt und formell geregelt; sie gilt selbstverständlich auch für die Banken. Die Auskunftsverweigerungsrechte sind in den §§ 101 und 102 AO den Vorschriften der §§ 52, 53 StPO nachgebildet worden und erweitern nicht den Kreis der Berufsgeheimnisträger. Schon nach dem sogenannten Bankenerlass [54] des Bundesministeriums für Finanzen sollen aber Kreditinstitute nach § 93 Abs. 1 S. 3 AO nur dann um Auskunft ersucht werden, wenn die Sachverhaltsaufklärung durch den Steuerpflichtigen nicht zum Erfolg geführt hat oder keinen Erfolg verspricht. Dies gilt auch für die Steuerfahndung, solange gegen den Betroffenen noch kein steuerliches Straf- oder Bußgeldverfahren eingeleitet worden ist. Im Fall des Todes müssen die Banken gemäß § 33 ErbschaftsStG die Vermögensgegenstände ihres Kunden ausdrücklich dem zuständigen Finanzamt mitteilen.

Soweit hiernach ein privatrechtlicher oder steuerrechtlicher Geheimnisschutz anerkannt ist, steht den Mitarbeitern der Banken ein persönliches Zeugnisverweigerungsrecht gemäß § 383 Abs. 1 Nr. 6 ZPO im Zivilverfahren zu.

Ein strafprozessual geschütztes Bankgeheimnis gibt es hingegen nicht. Banken und Kreditinstitute sind keine nach § 53 StPO zur Verweigerung des Zeugnisses berechtigten Berufsgeheimnisträger [55], so dass außerdem die in ihrem Gewahrsam befindlichen Beweisgegenstände keinem Beschlagnahmeverbot nach § 97 StPO unterliegen [56]. Somit gilt, was das Bundesverfassungsgericht im Zusammenhang mit gesellschaftsrechtlichen Geheimhaltungsvorschriften ausgeführt hat [57]:

> "Die Pflicht des Zeugen zur Aussage geht aufgrund des öffentlichen Interesses an der Tatsachenermittlung solchen privaten Geheimhaltungsinteressen vor, soweit nicht das Prozessrecht selbst diese als schützenswert anerkennt."

Für die strafprozessuale Praxis wirkt somit das privat- und steuerrechtliche Bankgeheimnis ausschließlich bei der Abwägung der Verhältnismäßigkeit des einzelnen hoheitlichen Eingriffs mit. Es kann somit keine grundsätzliche Sperrwirkung und keinen generellen Richtervorbehalt schaffen.

---

54 BFM vom 31.08.1979, NJW 79, 2190; der Bankenerlass hat später Eingang in den § 30a Abgabenordnung (Schutz von Bankkunden) gefunden; zuletzt neu gefasst am 01.10.02

55 eine entsprechende Regelung wie in § 383 Abs. 1 Nr. 6 ZPO wird in § 53 pp. StPO nicht vorgesehen

56 KG NStZ 89, 192: Die Sparkasse darf die Herausgabe nicht unter Berufung auf das "Bankgeheimnis" oder ein etwa dem Kunden zustehendes Zeugnisverweigerungsrecht ablehnen (Leitsatz)

57 BVerfG NJW 88, 899

2. Schriftliche Auskünfte des Zeugen (§ 161a StPO)

Mit der Strafprozessordnung ist deutlich zwischen persönlichen Beweismitteln - also im Wesentlichen Zeugen und Sachverständige (§§ 48 ff., 72 ff., 161a StPO) - und sachlichen Beweismitteln zu unterscheiden - Beweisgegenstände (§ 94 Abs. 1 StPO, dazu unten, Nr. 4.).

Die Eingangsfrage ist, ob die Staatsanwaltschaft oder Polizei schriftliche Auskünfte von Banken oder anderen nicht-behördlichen (dort gilt § 96 StPO) Institutionen erzwingen können. Für die Staatsanwaltschaft ist das zu bejahen.

Nach § 161a Abs. 1 S. 1 StPO sind Zeugen verpflichtet, auf Ladung vor der Staatsanwaltschaft zu erscheinen und zur Sache auszusagen. Mit Ausnahme der Anordnung der Haft, die gemäß § 161a Abs. 2 S. 2 erster Halbsatz StPO dem Richtervorbehalt unterliegt, können die übrigen Ungehorsamsfolgen bei unberechtigtem Ausbleiben oder unberechtigter Weigerung des Zeugen gemäß § 161a Abs. 2 S. 1 StPO von der Staatsanwaltschaft angeordnet werden; dies sind die Auferlegung der durch das Ausbleiben entstandenen Kosten (§§ 51 Abs. 1 S. 1, 70 Abs. 1 S. 1 StPO) und die Festsetzung eines Ordnungsgeldes (§§ 51 Abs. 1 S. 2, 70 Abs. 1 S. 2 StPO). Die Anordnung der Ersatzordnungshaft (§§ 51 Abs. 1 S. 2, 70 Abs. 1 S. 2 StPO) und der Erzwingungshaft (§ 70 Abs. 2 StPO) obliegen allein dem Richter, die Anordnung der zwangsweisen Vorführung hingegen auch der Staatsanwaltschaft (§ 161a Abs. 2 S. 1 i.V.m. § 51 Abs. 1 S. 3).

Es stellt sich die Frage, ob es ein gerechtfertigtes grundsätzliches Auskunftsverweigerungsrecht gegen schriftliche Auskunftsersuchen der Staatsanwaltschaft gibt. Sie ist zu verneinen. Die nachfolgenden Ausführungen werden sich mit dem Umfang der Auskunfts- und Herausgabepflichten auf schriftliche Ersuchen befassen.

In der Literatur und Rechtsprechung wird übereinstimmend anerkannt, dass die Staatsanwaltschaft in geeigneten Fällen nicht nur behördliche Auskünfte einholen darf (§ 161 StPO [58]), sondern ebenso gut Zeugen [59] zur schriftlichen Auskunft auffordern kann. Die RiStBV [60] bestimmen deshalb in Nr. 67 Abs. 1:

In geeigneten Fällen kann es ausreichen, dass ein Zeuge sich über bestimmte Fragen zunächst nur schriftlich äußert, vorausgesetzt, dass er glaubwürdig erscheint und eine vollständige Auskunft von ihm erwartet werden kann. In dieser Weise zu verfahren, empfiehlt sich besonders dann, wenn der Zeuge für seine Aussage Akten, Geschäftsbücher oder andere umfangreiche Schriftstücke braucht.

Eine gesetzliche Ausgestaltung der Auskunftserteilung wie in § 93 AO fehlt für das

---

[58] es gilt hiernach der Grundsatz der freien Gestaltung des Ermittlungsverfahrens, wonach alle zulässigen Maßnahmen zu ergreifen sind, die geeignet und erforderlich sind, zur Aufklärung der Straftat beizutragen; nur die Eingriffe in die Rechtssphäre anderer bedürfen der gesetzlichen Grundlage; LR-Rieß, § 160, RN 35 ff. (zitiert nach Löwe-Rosenberg, StPO, 24. Auflage, Berlin, New York 1989).

[59] nach schriftlicher Belehrung gemäß §§ 52, 53 StPO und Hinweis auf die Ungehorsamsfolgen "Kostentragungspflicht" und "Ordnungsgeld" (Belehrungspflichten aus § 163a Abs. 5 StPO); vergl. auch LR-Rieß, § 161a, RN 14.

[60] RiStBV: Richtlinien für das Straf- und Bußgeldverfahren (Verwaltungsvorschriften ohne Gesetzesrang)

staatsanwaltliche Ermittlungsverfahren. Dort wird - hier nur auszugsweise wiedergegeben - bestimmt:

> (1) Die Beteiligten und andere Personen haben der Finanzbehörde die ... erforderlichen Auskünfte zu erteilen. ...
>
> (2) In dem Auskunftsersuchen ist anzugeben, worüber Auskünfte erteilt werden sollen und ob die Auskunft für die Besteuerung des Auskunftspflichtigen oder für die Besteuerung anderer Personen angefordert wird. ...
>
> (3) Die Auskünfte sind wahrheitsgemäß nach bestem Wissen und Gewissen zu erteilen. Auskunftspflichtige, die nicht aus dem Gedächtnis Auskunft geben können, haben Bücher, Aufzeichnungen, Geschäftspapiere und andere Urkunden, die ihnen zur Verfügung stehen, einzusehen und, soweit nötig, Aufzeichnungen daraus zu entnehmen. ...
>
> (5) Der Auskunftspflichtige kann die Auskünfte schriftlich, mündlich oder fernmündlich erteilen. Die Finanzbehörde kann verlangen, dass der Auskunftspflichtige schriftlich Auskunft erteilt, wenn dies sachdienlich ist.

In der Kommentarliteratur zu § 161a StPO ist anerkannt, dass die Staatsanwaltschaft gleichermaßen eine Vernehmung an Amtsstelle und an anderen Orten (z.B. bei der ermittelnden Polizeibehörde), am Wohn- oder Geschäftssitz des Zeugen, indem der Staatsanwalt auch ohne Ankündigung den Zeugen aufsucht, oder eben - nach Nr. 67 RiStBV - im schriftlichen Wege durchführen darf [61]. Die Form der Ladung ist für die spätere Anordnung der Ungehorsamsfolgen unbeachtlich [62]: Auch wenn der Staatsanwalt den Zeugen unmittelbar aufsucht und ihn über die möglichen Folgen belehrt, rechtfertigt die unberechtigte Zeugnisverweigerung die Anordnung von Zwangsmitteln [63]. Somit eröffnet auch die unberechtigte Auskunftsverweigerung im schriftlichen Verfahren die Anwendung der Zwangsmittelvorschriften, ohne dass es einer Ladung zur Zeugenvernehmung bei der Staatsanwaltschaft bedarf, wenn die Folgen der Auskunftsverweigerung in dem schriftlichen Ersuchen bezeichnet worden sind.

Über die Reichweite der Auskunftspflichten von Banken gegenüber den Staatsanwaltschaften besteht eine langwierige Kontroverse, wobei auch die hier entwickelte Position in Frage gestellt wurde. Schon 1981 hat der "Zentrale Kreditausschuss" folgende Auffassung vertreten [64]:

> "Ein schriftliches Auskunftsverfahren sieht die StPO nicht vor, weshalb für die Kreditinstitute auch keine mit staatlichen Zwangsmitteln durchsetzbare Pflicht besteht, einem entsprechenden Auskunftsbegehren nachzukommen. Durch das dem Kunden gegenüber bestehende Bankgeheimnis sind Kreditinstitute sogar zivilrechtlich verpflichtet, die Auskunft zu verweigern. Lediglich dann, wenn ein richterlicher Durchsuchungs- oder Beschlagnahmebeschluss bzw. eine Zeugenladung vorliegt, zumindest aber in Aussicht gestellt

---

61 Kleinknecht/Meyer-Goßner, StPO, 42. Auflage, § 161a, RN 2; LR-Rieß, § 161a, RN 8

62 so für das richterliche Herausgabeverlangen nach § 95 Abs. 1 StPO: KG NStZ 89, 192

63 Kleinknecht/Meyer-Goßner, ebenda, RN 17; LR-Rieß, § 161a, RN 42

64 zitiert aus dem Schreiben vom 03.08.1981 - StPO-161 a -, gerichtet an den Bundesminister der Justiz

wird, mag sich für das Kreditinstitut in bezug auf den Kunden eine Berechtigung zur Auskunftserteilung ergeben, wenn es die genannten Maßnahmen durch die Erteilung von Auskünften über den betreffenden Geschäftsvorfall abwenden kann. Eine Verpflichtung gegenüber der Staatsanwaltschaft erwächst daraus aber nicht, so dass das Kreditinstitut es auf eine Beschlagnahme, Durchsuchung oder Zeugenladung ankommen lassen könnte."

Der Zentrale Kreditausschuss hat daraus gefolgert, dass Auskunftsersuchen allenfalls von den Staatsanwaltschaften, nicht aber auch von Polizeibehörden gestellt werden könnten; die Auskünfte selber dürften nur an die Staatsanwaltschaft erteilt und nicht auf Ersuchen der Staatsanwaltschaft an die Polizei gerichtet sein. Der Bundesminister der Justiz hat hierauf am 14.12.1981 entgegnet [65]:

"Es kann in einem solchen Fall keinen Unterschied machen, ob die Auskunft der Polizei unmittelbar oder über die Staatsanwaltschaft zugeleitet wird. Die von Ihnen aus § 161a StPO hergeleiteten rechtlichen Zweifel teile ich nicht. Ich verweise auf § 161 Satz 1 StPO, wonach die Staatsanwaltschaft Ermittlungen jeder Art (also auch die Einholung von Auskünften) entweder selbst vornehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen lassen kann. § 161a StPO begründet demgegenüber lediglich die Pflicht des Zeugen, vor der Staatsanwaltschaft zu erscheinen und zur Sache auszusagen. An der Tatsache, dass diese Regelung gegenüber der Polizei nicht gilt, ändert sich nichts dadurch, dass eine von der Staatsanwaltschaft erbetene Auskunft auf deren Wunsch unmittelbar der Polizei zugeleitet wird. Da diese auf Anordnung der Staatsanwaltschaft tätig wird und die Staatsanwaltschaft die Erteilung der Auskunft notfalls erzwingen könnte, steht der vorgeschlagenen Verfahrensweise auch nicht das sogenannte "Bankgeheimnis" entgegen."

In der Praxis haben sich aber auch in der Folgezeit gelegentlich Meinungsverschiedenheiten ergeben, die die Landeszentralbank Niedersachsen 1988 zu folgender Stellungnahme veranlasst haben [66]:

"Wenn die Banken gegenüber Auskunftsersuchen der Ermittlungsbehörden mitunter formale Einwendungen erheben, so liegt der Grund nicht etwa darin, dass sie nicht bereit wären, entsprechend den gesetzlichen Bestimmungen mit den Ermittlungsbehörden "zusammenzuarbeiten". Die Banken müssen nur darauf sehen, dass eindeutig formulierte und begründete Anordnungen, die gegenüber ihren Kunden eine hinreichende Rechtsgrundlage dafür liefern, dass die Offenbarung geschäftlicher Vorgänge zivilrechtlich gerechtfertigt ist."

Gerade in Strafverfahren verwickelte Kunden machen - z.T. unterstützt durch Rechtsanwälte - den Banken Vorwürfe wegen erteilter Auskünfte. Soweit das Bankpersonal gar Amtsträger ... ist ..., könnte sogar der strafrechtliche Vorwurf

[65] zitiert aus dem Schreiben vom 14.12.1981 - 4110 - 66 179/80 -, gerichtet an den Zentralen Kreditausschuss

[66] auszugsweise zitiert aus dem Rundschreiben vom 08.07.1988, gerichtet an die drei Generalstaatsanwaltschaften und das Landeskriminalamt in Niedersachsen

der Verletzung von Privatgeheimnissen nach § 203 StGB erhoben werden.

... Es hat sich deshalb in der Praxis durchgesetzt, dass die Staatsanwaltschaften die sie interessierenden Fragen den Banken schriftlich mit der Bitte um Auskunft und Beifügung von Fotokopien stellen. Die Zulässigkeit solcher Auskünfte ist aber unter dem Gesichtspunkt des Bankgeheimnisses nicht unproblematisch. ...

Bei den Kreditinstituten erscheinenden Ermittlungsbeamten fehlt in fast allen Fällen die Befugnis, ohne Beschlagnahme- oder Durchsuchungsbeschluss bei den Banken vorzugehen, weil durchweg davon auszugehen ist, dass die Banken ihre Geschäftsunterlagen ordnungsgemäß aufbewahren und deshalb Gefahr im Verzuge nicht angenommen werden kann. Ganz abgesehen davon liegt eine Durchsuchung in der Regel auch gar nicht im Interesse der Ermittlungsbehörden, weil sie aufwendig ist und ohne aktive Unterstützung der Bank kaum den gleichen Erfolg hat wie eine schriftliche Auskunft.

Wir möchten daher bitten, dass Sie in Ihrem Geschäftsbereich anregen, von vornherein klare und rechtlich überzeugende Ersuchen an die Banken zu richten.

Wichtig erscheinen uns auf jedem Fall folgende Punkte:

1.) Das Schreiben muss von einem Staatsanwalt (oder Richter) unterschrieben und

2.) mit Dienstsiegel versehen sein.

3.) Auf die Verpflichtung zur Aussage sollte ausdrücklich hingewiesen, die Vorschrift des § 161a StPO erwähnt werden.

4.) Sofern eine ordnungsgemäße Ladung ausgesprochen wird, könnte diese mit dem Anheimstellen verbunden werden, durch schriftliche Auskunft das Erscheinen vor der StA abzuwenden.

5.) Die Aufforderung, bestimmte Bankunterlagen herauszugeben, dürfte grundsätzlich eine richterliche Durchsuchungs- bzw. Beschlagnahmeanordnung voraussetzen."

Die Stellungnahme der Landeszentralbank Niedersachsen hat zumindest einen Streitpunkt geklärt: Schriftliche Auskunftsersuchen gemäß § 161a StPO werden anerkannt und sollen von den Banken wenigstens in dem Umfang beantwortet werden, wie sie oder ihre Mitarbeiter als Zeugen in einer formellen Vernehmung zur Auskunft verpflichtet wären. Dabei dienen die förmlichen Forderungen der Nrn. 2. bis 3. zur Identifikation als staatsanwaltliches Auskunftsersuchen, so dass sich ein Streit über ihre Berechtigung nicht lohnt - schon gar nicht mehr heute, mehr als 20 Jahre später.

Gegen die verlangte Verfahrensweise nach Nr. 1. muss hingegen eingewendet werden, dass Polizeibeamte im Ermittlungsverfahren durchaus im Auftrag der Staatsanwaltschaft tätig werden (§ 161 StPO) und dabei zur eigenständigen Zeugenvernehmung berechtigt sind (§ 163a Abs. 4, 5 StPO). Die im Rahmen des Ermittlungsauftrages [67] von der Polizei eingeholten Auskünfte sind zweifellos zulässig und verwertbar, nur nicht erzwingbar. Ein ausdrückliches Ermittlungsersuchen der Staatsanwaltschaft an die Polizei, das die für erforderlich gehaltenen Bankauskünfte nach Adressat und Umfang konkret bezeichnet und den Hinweis enthält,

[67] und darüber hinaus: § 163 StPO (erster Zugriff der Polizei)

dass die Auskunftsersuchen der Vermeidung einer staatsanwaltlichen Zeugenvernehmung dienen, müsste auch den Bedenken der Banken ausreichend Rechnung tragen.

Zeugenschaftliche Auskünfte über das Bestehen von Kontoverbindungen, über den Kontoinhaber und die Verfügungsberechtigten, über den sachbearbeitenden Bankmitarbeiter, über eingeräumte Kreditlinien und sogar über einzelne Buchungsvorgänge oder über die genaue Art und den Umfang der Buchführung der Bank (z.B. nach der Gestalt und der Art der vorhandenen Kreditakten) sind somit im Wege des schriftlichen Auskunftsersuchens durchsetzbar und erzwingbar. Der Nr. 5 des Schreibens der Landeszentralbank Niedersachsen kann hingegen nach der jüngeren Rechtsprechung nicht zugestimmt werden (dazu unten, Nr. 4. im Einzelnen).

3. Kontoverdichtungen. Vorbereitungspflicht des Zeugen?

Bei den von den Staatsanwaltschaften verlangten Kontoverdichtungen handelt es sich um schriftliche Kontokorrentaufstellungen, die die Herkunft von Kontozugängen und die Verwendung von Kontobelastungen innerhalb eines bestimmten Zeitraums und für einen bestimmten Kontoinhaber ausweisen. Im Gegensatz zu einfachen Auskünften über das Bestehen von Kontoverbindungen usw., wie sie oben dargestellt und durchsetzbar sind, handelt es sich hierbei um Zusammenfassungen von Unterlagen der Bank, die eine selbständige schöpferische Leistung darstellen. Insoweit wurden Bedenken dagegen erhoben, dass Kontoverdichtungen im Rahmen von § 161a StPO eingefordert werden können, weil nur die Zeugenaussage als solche, nicht aber Vorbereitungsleistungen des Zeugen erzwungen werden könnten.

3.1. Handlungs- und Vorbereitungspflicht des Zeugen?

Die damit angesprochene Frage, ob dem zur Aussage verpflichteten Zeugen der Zugriff auf Aufzeichnungen und Akten seines Arbeitsbereiches abverlangt und die schöpferische Erstellung von Kontoverdichtungen auch im Wege der schriftlichen Auskunft zur Vermeidung einer staatsanwaltlichen Zeugenvernehmung eingefordert werden können, ist im Gegensatz zu meiner früher geäußerten Meinung im Ergebnis zu verneinen.

Dieses Ergebnis steht nur scheinbar im Gegensatz zu den Urteilsgründen in BGHSt 1, 4 (8), worin der Bundesgerichtshof ausgeführt hat:

> "Ein vom Gericht vernommener Zeuge hat nicht nur das Recht, sondern unter Umständen sogar die Pflicht, sich früherer Aufzeichnungen als Gedächtnisstützen zu bedienen, um sein Erinnerungsbild aufzufrischen und gegebenenfalls zu berichtigen. Die Verletzung dieser Pflicht kann ihn sogar der Gefahr aussetzen, wegen fahrlässigen Falscheides gemäß § 163 StGB zur Verantwortung gezogen zu werden."

Der Bundesgerichtshof setzt damit voraus, dass der Zeuge stillschweigend erklärt: "Ich habe Aufzeichnungen und ich habe mich zur

Vorbereitung meiner Vernehmung ihres Inhalts versichert". Wenn er dazu nichts sagt, dann müsste eine Vorbereitungspflicht des Zeugen bestehen, wenn ihm wegen Schweigens ein fahrlässigen Falscheid drohen soll.

Eine solche Vorbereitungspflicht des Zeugen - sozusagen vorprozessuale Vorbereitungspflicht - wird von der Literatur und Rechtsprechung grundsätzlich abgelehnt [68]. Nach der Auffassung des OLG Köln [69], dem die Literatur und Rechtsprechung seit fast 40 Jahren folgt, kann für erfahrene Amtszeugen (Polizei- und andere Ermittlungsbeamte [70]) eine gesteigerte Vergewisserungspflicht bestehen, woraus eine Vorbereitungspflicht für diese Zeugen abgeleitet wird. Die Verpflichtung des Zeugen hingegen, nach Unterbrechung seiner Aussage zu einer weiteren zu erscheinen und hierzu vorbereitend außerhalb der Hauptverhandlung auch umfangreiche Aufzeichnungen und Akten einzusehen, wird von der Rechtsprechung stillschweigend anerkannt [71].

Die Grenzen dieser - mit anderen Worten - prozessualen Vorbereitungspflicht bezeichnet Krehl wie folgt [72]:

> (Das OLG Köln in anderer Sache) "begrenzt nämlich die Einsichtspflicht in vorhandene Aufzeichnungen auf dem Zeugen mögliche und zumutbare Nachforschungen und anerkennt damit die Verpflichtung, auch außerhalb der Hauptverhandlung gedächtnisauffrischend tätig zu werden. ...
>
> Nicht in jedem Fall nämlich ist es zulässig, den Zeugen zur Nachforschung zu veranlassen. Zum einen ist dies dann ausgeschlossen, wenn der Zeuge sich zu einer bestimmten Beweisfrage erstmalig Kenntnis verschaffen soll, er also Wahrnehmungen zu der Sache ursprünglich gar nicht gemacht hat. Er ist dann also gerade nicht verpflichtet, für das Gericht Feststellungen zu treffen. Zum anderen ist die Erkundigungspflicht von Zeugen beschränkt auf mögliche und zumutbare Ermittlungen.
>
> Schwierige, einen außergewöhnlichen Zeitaufwand in Anspruch nehmende Nachforschungen, etwa das eingehende Studium ganzer Bilanzen oder das Durchsuchen einer Unzahl von Aktenordnern, um eine bestimmte Unterlage zu finden, sind danach nicht erforderlich. Hier ist das Gericht darauf angewiesen, sich die notwendigen Erkenntnisse selbst zu verschaffen bzw. durch Sachverständige verschaffen zu lassen."

Krehls Abgrenzung zwischen vorprozessualer und prozessualer Vorbereitungspflicht ist nach systematischen und logischen Gesichtspunkten nicht zwingend: Wenn tatsächlich eine Pflicht des Zeugen zu einer Vergewisserung und zur Nachforschung in Akten und Aufzeichnungen bestände, so ist dies eine qualitative Normentscheidung und bestände die Pflicht gleichermaßen vor sei-

---

68 vergl. RGSt 8, 108 (109 f.) und Krehl, Die Erkundigungspflicht des Zeugen bei fehlender oder beeinträchtigter Erinnerung und mögliche Folgen ihrer Verletzung, NStZ 91, 416

69 OLG Köln NJW 66, 1420 (1421); Krehl lehnt die gesteigerte Vergewisserungspflicht ab: ebenda, 417

70 die Entscheidung lässt aber offen, ob sich die Vergewisserungspflicht auf Ermittlungsbeamte beschränkt; sie ließe sich unschwer auf alle Zeugen übertragen, die Wahrnehmungen im Zusammenhang mit ihrer Berufsausübung bekunden

71 Krehl, ebenda, 417, m.w.N.

72 ebenda

ner weiteren wie auch vor seiner "ersten" Vernehmung.

Der Ausgangspunkt für die rechtliche Verpflichtung zur Vorbereitung und ihrem Umfang könnte insoweit nur sein, dass der Zeuge weiß, zu welchem Gegenstand er Auskunft über seine eigenen Wahrnehmungen geben soll. Auch wenn ihm ein detaillierter Fragenkatalog an die Hand gegeben wird, so macht es keinen Unterschied, ob ihm diese Fragen vor der ersten oder erst im Verlauf dieser ersten, dann unterbrochenen Vernehmung bekannt geworden sind. Nur neue Fragen, die erst im Rahmen der "ersten" Vernehmung auftauchen, würden dann eine (quantitative) weitere Nachforschungspflicht begründen. "Weitere" Nachforschungspflichten in diesem Sinne könnten dann nur durch die Erweiterung des Beweisthemas entstehen [73].

Diese Überlegungen ändern nichts daran, dass eine allgemeine staatsbürgerliche Pflicht zwar angenommen werden kann, eine gesetzlich vorgeschriebene und sanktionsbewehrte Verpflichtung zur inhaltlichen Vorbereitung auf eine Zeugenaussage hingegen nicht besteht. Die oben zitierten Entscheidungen haben nur Erwägungen angestellt, ohne in den zugrunde liegenden Fällen wegen eines Pflichtverstoßes tatsächlich verurteilt zu haben. Selbst wenn man Krehl und der Rechtsprechung zur prozessualen Vorbereitungspflicht folgte, ließe sich daraus nicht der Schluss ziehen, dass auch eine vorprozessuale Vorbereitungspflicht bestünde.

Auch die vom Bundesgerichtshof angestellten Erwägungen helfen nicht weiter. Wenn keine vorprozessuale Vorbereitungspflicht besteht, dann kann sich der Zeuge, der seine mangelhafte Vorbereitung verschweigt, auch nicht wegen eines fahrlässigen Falscheides strafbar machen, weil ihm keine Pflichtverletzung vorzuwerfen ist. Erklärt der Zeuge wahrheitsgemäß auf eine ausdrückliche Frage, dass er sich nicht vorbereitet habe, dann hat er auch nicht falsch ausgesagt. Das Gericht und die anderen Verfahrensbeteiligten können versuchen, durch Vorhalte, Augenscheinsgegenstände oder das Verlesen von Urkunden das Erinnerungsvermögen des Zeugen aufzufrischen. Eine Verpflichtung zur Prüfung und Recherche durch den Zeugen selber - also eine Handlungspflicht - kann dadurch aber nicht entstehen.

Die vorbereitende (freiwillige) Einsichtnahme des Zeugen in seine eigenen Aufzeichnungen, Akten oder Handelsbücher ersetzt die Beweiserhebung über den Inhalt genau dieser sachlichen Beweismittel. Der Zeuge, der sich der Mühe einer Vorbereitung auf seine Vernehmung unterzieht und sich Kenntnisse über den Inhalt seiner ihm zur Verfügung stehenden Sachbeweismittel verschafft, erspart dem Gericht die Erarbeitung des Inhalts dieser Beweismittel und prozessuale Handlungen (z.B. Durchsuchung, Beschlagnahme, Beweisaufnahme). Er bietet mit seiner aufgefrischten Erinnerung ein Surrogat für die Beweisaufnahme über den Inhalt sachlicher Beweismittel an.

---

[73] durch die Wahrnehmung des Fragerechts der Parteien im Zivilprozess und der Beteiligten im Strafverfahren wird der Beweisgegenstand regelmäßig erweitert, wenn der Richter die Fragen zulässt; nur "beiläufige" Bekundungen des Zeugen außerhalb des ihm bekannten Beweisthemas unterliegen nicht der prozessualen Wahrheitspflicht, so dass auch keine Strafbarkeit besteht, wenn beiläufige Bekundungen außerhalb des Beweisthemas sachlich falsch sein sollten

3.2. Forderung nach einem Surrogat

Wenn die Staatsanwaltschaft eine Kontoverdichtung fordert, so kann sie die damit verbundene Tätigkeit der Bankmitarbeiter nicht erzwingen. Ebenso wenig wie es eine festgeschriebene und erzwingbare Vorbereitungspflicht des Zeugen gibt, besteht auch keine Editionspflicht.

Die Forderung nach einer Kontoverdichtung enthält jedoch einen Verzicht auf Zwangsmittel, die die Staatsanwaltschaft einsetzen könnte: Sie kann den Zeugen zum Erscheinen und - soweit die §§ 52 und 53 StPO nicht greifen - zur Aussage zwingen. Darüber hinaus kann sie aus eigener Befugnis (dazu unten, Nr. 4.) die Herausgabe genau der Unterlagen erzwingen, deren inhaltlichen Auswertung in die Kontoverdichtung einfließen sollen: Belege, Kontoauszüge, Microfiches und Daten über die Kontoführung.

Mit der Erstellung der Kontoverdichtung erspart die Bank ihren Mitarbeitern die mühselige Vernehmung als Zeugen zu einzelnen Buchungen und ihrer Kontierung und erspart sich (neben der Störung des Geschäftsbetriebes) die langwierige Herausgabe ihrer Geschäftsbücher und sonstigen Buchführungsunterlagen, die als sachliche Beweismittel beschlagnahmt werden könnten.

Die Forderung nach der Erstellung einer Kontoverdichtung stellt sich somit als eine Abwendungserlaubnis dar: Die Staatsanwaltschaft verzichtet auf den Einsatz von Zwang, indem sie der Bank die Edition einer Kontoverdichtung gestattet. Mit der Kontoverdichtung erhält die Staatsanwaltschaft schließlich ein Surrogat (einen Ersatz) für die sachlichen Beweismittel in der Bank und für die personenbeweisliche Vernehmung ihrer Mitarbeiter.

4. Herausgabepflichten (Kontobelege und andere Schriftstücke)

Gemäß § 95 Abs. 1 StPO ist jeder, der den Gewahrsam über einen Gegenstand von potentieller Beweisbedeutung im Sinne von § 94 StPO ausübt, verpflichtet, diesen Gegenstand auf Verlangen herauszugeben. Für den Fall der Weigerung nimmt § 95 Abs. 2 StPO auf die Ungehorsamsfolgen des § 70 Abs. 1 und Abs. 2 StPO Bezug.

Die Staatsanwaltschaft ist ein dem Gericht gleichgeordnetes Organ der Strafrechtspflege, dem namentlich die Strafverfolgung obliegt [74], und ist gemäß § 161 StPO berechtigt, alle dem Zweck des Ermittlungsverfahrens (§ 160 StPO) dienenden Ermittlungen durchzuführen oder die Beamten des Polizeidienstes mit den Ermittlungen zu betrauen. Hieraus folgt, dass die reine Aufforderung gemäß § 95 Abs. 1 StPO, Beweisstücke herauszugeben, von der Staatsanwaltschaft genauso wie von den von ihr um die Ermittlungen ersuchten Polizeibeamten erfolgen kann.

Die Befugnis Staatsanwaltschaft, gemäß § 95 Abs. 1 StPO von der Bank als Zeugin die Belege und Akten als Beweismittel herauszuverlangen, ist zunächst ganz überwiegend bejaht und sorgfältig begründet worden [75]. Dabei ist unstreitig gewesen, dass die Zwangsmittel des § 70 Abs. 1 und Abs. 2 StPO nur vom Gericht angeordnet werden dürfen (§ 70 Abs. 3 StPO). Insbesondere das Landgericht Düsseldorf [76] und Braczyk

---

74 BGHSt 24, 170 (171)

75 Bittmann, Das Beiziehen von Kontounterlagen im staatsanwaltlichen Ermittlungsverfahren, wistra 90, 325 ff.; Klinger, die Zuständigkeit der Staatsanwaltschaft für Maßnahmen nach § 95 StPO, wistra 91, 17 ff.

76 LG Düsseldorf wistra 93, 199 f.

[77] haben später mit knappen Worten gefolgert, dass in Fällen ohne Gefahr im Verzug eine Zwangsmittelanordnung nicht bereits aufgrund eines staatsanwaltlichen Herausgabeersuchen erfolgen könne, sondern es zunächst eines gerichtlichen Herausgabeverlangens und sogar einer Beschlagnahmeanordnung bedürfe.

Für das Fehlen staatsanwaltlicher Eingriffsbefugnisse sollen folgende Erwägungen leitend sein: Nach § 94 Abs. 2 StPO bedarf es im Falle der nicht freiwilligen Herausgabe von Beweismitteln einer Beschlagnahme. Zu dieser Zwangsentscheidung sind gemäß § 98 Abs. 1 Satz 1 StPO grundsätzlich das Gericht und nur im Ausnahmefall - bei Gefahr im Verzug - die Staatsanwaltschaft oder ihre Hilfsbeamten befugt (§ 152 GVG). § 94 Abs. 2 StPO verweise auf das Beschlagnahmeerfordernis, so dass nur das Strafverfolgungsorgan, das auch zur Beschlagnahme befugt sei, die Ungehorsamfolgen androhen könne und im Normalfall ohne richterliche Beschlagnahmeanordnung auch keine Zwangsmittel angeordnet werden könnte. Die Gegenmeinung würde das Beschlagnahmeerfordernis des § 94 Abs. 2 StPO unterlaufen und dazu führen, "dass für die weniger einschneidende Maßnahme der Beschlagnahme der Richtervorbehalt gelten würde, während die Staatsanwaltschaft den Betroffenen zu der zwangsmittelbewehrten, damit grundrechtsrelevanten Herausgabe von Gegenständen allein verpflichten könne" [78].

Das LG Düsseldorf entnimmt dem § 94 Abs. 2 StPO, dass nach einer Herausgabeweigerung einzig eine Beschlagnahme erfolgen könne, und begründet seinen Schluss mit der Gesetzessystematik. Wenn der Gesetzgeber aber einzig die Beschlagnahme hätte eröffnen wollen, so hätte er nicht gleichzeitig in § 95 Abs. 2 StPO auf die Ungehorsamsfolgen Bezug nehmen können [79]. Darüber hinaus scheint das LG Düsseldorf den Begriff des Gesetzesvorbehalts mit dem des Richtervorbehalts gleichzusetzen. Gemäß Art. 19 Abs. 1 S. 1 GG darf in Grundrechte nur aufgrund eines Gesetzes und nach Art. 19 Abs. 2 GG nur so weit eingegriffen werden, dass der Wesensgehalt des Grundrechtes erhalten bleibt (Gesetzesvorbehalt). Im Gegensatz dazu greift der grundgesetzliche Richtervorbehalt nur in den Grenzen des Art. 104 GG durch, also bei der Freiheitsentziehung über einen Tag hinaus. "Einfachgesetzliche" Richtervorbehalte müssen ausdrücklich bestimmt werden und sind von der StPO in allen Fällen vorgesehen, wo das Gesetz weit in Grundrechte eingreift, also neben freiheitsentziehenden Maßnahmen auch bei der Durchsuchung und der zwangsweisen Beschlagnahme.

Eine wirksame Beschlagnahme wird aber in aller Regel deshalb nicht möglich sein, weil der Beschlagnahmegegenstand nicht hinreichend genau bezeichnet werden kann. Die Beschlagnahme verlangt - anders als die Angabe der gesuchten Gegenstände in einem Durchsuchungsbeschluss - eine individuelle Beschreibung. Nach den §§ 102 und 103 StPO reicht es aus, dass nach kriminalistischer Erfahrung der Verdacht (beim Verdächtigen) oder aufgrund der Beweiserhebung im übrigen die konkrete Erwartung besteht (beim Unbeteiligten), dass sich im Gewahrsam des Durchsuchungsbetroffenen

---

[77] Braczyk, Zur Zuständigkeit der Staatsanwaltschaft für das Herausgabeverlangen nach § 95 StPO, wistra 93, 57 f.

[78] LG Düsseldorf, a.a.O., S. 200

[79] Klinger, a.a.O., S. 18

Beweisgegenstände befinden. Eine Beschlagnahmeanordnung verlangt hingegen nach einer gegenständlichen Präzisierung [80].

Das LG Stuttgart [81] hat schließlich darauf hingewiesen, dass sich aus dem Text der §§ 94, 95 StPO kein Hinweis darauf ergebe, dass einem Herausgabeersuchen eine Beschlagnahme vorausgehen müsse, so dass es zu dem Schluss kommt, es bedürfe nur eines gerichtlichen Herausgabeverlangens ohne gesonderte Beschlagnahmeanordnung, weil "richterliches Herausgabeverlangen und richterliche Beschlagnahme ... alternativ und gleichberechtigt nebeneinander" ständen [82].

Im Gegensatz zu diesen Meinungen in der Rechtsprechung und Literatur [83] bin ich der Auffassung, dass die Herausgabeweigerung des Gewahrsamsinhabers wegen eines staatsanwaltliches Herausgabeersuchen als Voraussetzung für eine Zwangsmittelanordnung ausreicht. Entgegen der Behauptung des LG Düsseldorf verweist § 95 Abs. 1 StPO nicht insgesamt auf § 94 StPO, sondern nur auf die in § 94 Abs. 1 StPO definierten Beweistücke als Gegenstände von potentieller Beweisbedeutung. Der Schluss, dass damit auch das Beschlagnahmeerfordernis nach § 94 Abs. 2 StPO zur Voraussetzung der Zwangsmittelanordnung nach § 95 Abs. 2 i.V.m. § 70 StPO einbezogen werde, lässt sich weder aus dem Wortlaut, noch aus dem Sinnzusammenhang ziehen. Aus der gesetzlichen Funktion der Staatsanwaltschaft als gleichberechtigtes Organ der Strafrechtspflege und ihrer Aufgabe, die sachlich gebotenen Ermittlungen aus eigener Entscheidungs- und Ermittlungskompetenz zu führen, ist deshalb m.E. die Staatsanwaltschaft auch zum "strafbewehrten" Herausgabeersuchen befugt.

Ausschlaggebend sind die Regel-Ausnahme-Verhältnisse, die die StPO vorsieht. Der Umfang und die Reihenfolge der Ermittlungen werden von der Staatsanwaltschaft bestimmt, wobei die Untersuchungsmaßnahmen, die tief in den grundrechtlich geschützten Bereich des Betroffenen eindringen können, dem Richtervorbehalt unterliegen (z.B. Durchsuchung, Beschlagnahme und Untersuchungshaft). Das Herausgabeverlangen nach § 95 Abs. 1 StPO und das Auskunftsersuchen nach § 161a StPO sind davon ausgenommen und unterliegen ausdrücklich nicht dem Richtervorbehalt. Es ist entgegen dem LG Düsseldorf auch nicht nachvollziehbar, dass die Drohung mit dem Antrag, vom Gericht die gesetzlich vorgesehenen Zwangsmittel anordnen zu lassen, tiefer in die geschützte Grundrechtssphäre des Betroffenen eindringen würde als der - stillschweigende - Antrag an den Ermittlungsrichter, ohne rechtliches Gehör einen Durchsuchungsbeschluss zu erlassen. In beiden Fällen obliegt es dem Gericht, die Voraussetzungen für die Zwangsmaßnahme zu prüfen und nur bei

---

80 strenge Anforderungen beim LG Stuttgart, StrafV 86, 471 f.; vergl. auch LG Oldenburg wistra 87, 38;
zur Unzulässigkeit der pauschalen Beschlagnahmeanordnung im Durchsuchungsbeschluss: OLG Düsseldorf StrafV 82, 513; BVerfG NStZ 92, 91 f.;
vergl. auch BVerfG NJW 91, 690 f.; BVerfG NJW 94, 3281 f. (Mindestangaben in einem Durchsuchungsbeschluss: Angaben über den Inhalt des Tatvorwurfs)

81 LG Stuttgart NStZ 92, 249 f.

82 LG Stuttgart, a.a.O., S. 250

83 diese noch ergänzt um LR-Schäfer, § 95 StPO, RN 8 und 9; KK-Nack, § 95 StPO, RN 3

einer gesetzesgemäßen Entscheidungslage die Eingriffsentscheidung zu treffen [84].

Diese Meinung teilen jetzt das LG Lübeck [85], das LG Gera [86] und das LG Halle [87]. Bittmann [88] würdigt diese Entwicklung positiv und m.E. zutreffend.

5. Praktische Folgerungen

Auf Auskunfts- und Herausgabeersuchen der Staatsanwaltschaften wird von den Banken häufig "der übliche Beschluss des Gerichts" gefordert. Ein reiner Beschlagnahmebeschluss gemäß § 94 Abs. 2 in Verbindung mit § 98 StPO scheidet dabei grundsätzlich aus, weil die Beschlagnahmegegenstände nur in allgemeiner Form, nicht aber in ausreichend konkreter Weise beschrieben werden können (vergleichbar einem Titel zur Zwangsvollstreckung). Danach müsste zur Vorbereitung einer förmlichen Beschlagnahme ein Durchsuchungsbeschluss gegen die Bank als unbeteiligte Dritte gemäß § 103 StPO erwirkt werden. In der Praxis dürfte dies der häufigste Fall sein, ohne dass es zu regelmäßigen Durchsuchungen bei den Geschäftsbanken gekommen ist.

Weniger bekannt dürfte der Weg sein, der sich aus § 95 StPO ableiten lässt: Ein durch Beschluss bestimmtes Herausgabeverlangen des Ermittlungsrichters, in dem dieser die Herausgabepflicht feststellt und ggf. angemessene Ersatz-Beweismittel kennzeichnet (Surrogate: Kopien bestimmter Arten von Beweismittel, Zusammenstellungen vereinzelter Beweismittel z.B. in Form einer Kontoverdichtung). Wählt der Staatsanwalt dieses Vorgehen, muss er sich an die Bank mit einem eigenen Auskunftsersuchen gemäß § 161a StPO und gleichzeitig mit einem richterlichen Herausgabebeschluss gemäß § 95 Abs. 1 StPO wenden.

Beispiele hierzu zeigen die beiden anliegenden Muster:

Herausgabebeschluss gemäß § 95 StPO
Auskunftsersuchen gemäß § 161a StPO

---

84 Klinger, a.a.O., S. 18; ausführlich begründet bei Bittmann, a.a.O., S. 330

85 NJW 2000, 3148 f.; Beschluss des LG Lübeck vom 03.02.00 - 6 Qs 3/00 -

Leitsatz:
Die Staatsanwaltschaft kann in eigener Zuständigkeit Kontounterlagen vom Geldinstitut gem. § 95 I StPO herausverlangen. Eine richterliche Anordnung ist nicht erforderlich.

86 NStZ 2001, 276; Beschluss des LG Gera vom 30.09.99 - 2 Qs 412/99 -;

Leitsatz:
Für das Herausgabeverlangen nach § 95 I StPO ist neben dem Richter auch die StA zuständig, und zwar auch dann, wenn Gefahr im Verzug nicht besteht.

87 NStZ 01, 276 f.; Beschluss des LG Halle vom 06.10.99 - 22 Qs 28/99 -;
Leitsätze:
1. Für das Herausgabeverlangen nach § 95 I StPO ist neben dem Richter auch die StA zuständig, und zwar auch dann, wenn Gefahr im Verzug nicht besteht.
2. Beschlagnahmemöglichkeit (§ 94 II StPO) und Herausgabeverlangen (§ 95 StPO) stehen grundsätzlich gleichrangig nebeneinander. Ein Herausgabeverlangen kommt aber nur dann in Betracht, wenn eine Beschlagnahme zur Sicherstellung der benötigten Beweismittel faktisch ungeeignet ist.

88 Bittmann, Das staatsanwaltliche Auskunftsverlangen gemäß § 95 StPO, NStZ 01, 231 ff.

Dennoch sind solche gerichtlichen Beschlüsse nicht erforderlich, weil staatsanwaltliche Auskunfts- und Herausgabeaufforderungen für sich allein die Anordnung von Zwangsmitteln auslösen können.

a) Das schriftliche Auskunftsersuchen (§ 161a StPO) berechtigt die Staatsanwaltschaft im Weigerungsfall zur Feststellung der Kostenpflicht und zur Festsetzung eines Ordnungsgeldes. Die Anordnungen der Ordnungshaft oder der Erzwingungshaft unterliegen zwar dem Richtervorbehalt, verlangen aber nicht, dass das Auskunftsersuchen vom Richter noch einmal wiederholt werden müsste, um "strafbewehrt" zu sein.

b) Auch das Herausgabeersuchen der Staatsanwaltschaft wegen sachlicher Beweismittel gemäß § 95 Abs. 1 StPO ist "strafbewehrt". Mangels einer dem § 161a StPO entsprechenden Regelung kann die Staatsanwaltschaft zwar keine Zwangsmittel selber anordnen. Dennoch löst die Weigerung unmittelbar die Zulässigkeit der gesetzlich vorgesehenen Zwangsmittel aus (§ 95 Abs. 2 i.V.m. § 70 StPO).

Muster: **Herausgabebeschluss gemäß § 95 StPO:**

Beschluss

In dem Ermittlungsverfahren

gegen ___,

geboren am ___,

wohnhaft ___,

wegen des Verdachts der Untreue (§ 266 StGB)

wird gemäß § 95 Abs. 1 in Verbindung mit §§ 94 Abs. 1, Abs. 2, 98 Abs. 1 Strafprozessordnung als richterliches Herausgabeverlangen angeordnet:

Die ... Bank, [Straße, BLZ, Stadt]

ist zur Herausgabe aller Schriftstücke verpflichtet, die die Eröffnung und Schließung, die Zeichnungsbefugnisse und alle Zu- und -abgänge von Geld und Wertpapieren in dem Zeitraum vom ___ bis ___

des Kontos Nr. ___

und des Depots Nr. ___

des [Beschuldigten]

betreffen.

Diese Verpflichtung umfasst:

a) Konten- und Unterschriftsblätter,

b) Buchungslisten über Zu- und Abgänge, Saldenaufstellungen, Bestandsverzeichnisse,

c) Buchungsbelege für Zahlungsein- und -ausgänge,

d) den Schriftverkehr im Zusammenhang mit der Kontoführung.

Die Herausgabe der Schriftstücke zu b) und c) darf dadurch abgewendet werden, dass die Herausgabepflichtige eine vollständige

Aufstellung aller und Kontobuchungen und Depotveränderungen für die Zeit vom ___ bis zum ___ erstellt und an die Strafverfolgungsbehörden aushändigt. Wegen der Schriftstücke zu c) gilt dies mit der Einschränkung, dass den Strafverfolgungsbehörden alle Buchungsbelege als Ablichtung auszuhändigen sind, die sich auf einen Betrag von mindestens 10.000,- DM beziehen.

Die Herausgabepflichtige ist berechtigt, ihre herausgegangenen Geschäftsbriefe und internen Vermerke als Ablichtung den Strafverfolgungsbehörden auszuhändigen.

Die Staatsanwaltschaft ____ und die von ihr zu beauftragenden Hilfsbeamten werden gemäß § 36 Abs. 2 S. 1 Strafprozessordnung mit der Zustellung und Vollstreckung dieses Herausgabeverlangens beauftragt.

Für den Fall der Verweigerung der Herausgabe werden zugleich die Ungehorsamsfolgen des § 95 Abs. 2 Strafprozessordnung angedroht (Ordnungsgeld, Ordnungshaft, Erzwingungshaft; § 70 Abs. 1, Abs. 2 Strafprozessordnung).

Gründe:

Der [Beschuldigte] ist verdächtigt, Untreuehandlungen zum Nachteil einer von ihm als Vorstand vertretenen [Firma] begangen zu haben.

Nach den bisherigen Ermittlungen hat der Beschuldigte bei der Herausgabepflichtigen die oben angegebenen Konten eingerichtet. Die Wertpapiere im Depot sollen per ___ einen Verkaufswert von ___ DM gehabt haben.

Der strafrechtliche Untersuchungsgegenstand erfordert die Sicherstellung der oben genannten Schriftstücke als Beweismittel (§ 94 Abs. 1 Strafprozessordnung), zu deren Herausgabe die [Bank] verpflichtet ist (§ 95 Abs. 1 Strafprozessordnung).

In Anwendung des Verhältnismäßigkeitsgrundsatzes sind die oben im einzelnen dargelegten Abwendungsbefugnisse angeordnet worden.

Muster: **Auskunftsersuchen gemäß § 161a StPO**

Verfügung

1. Schreiben fertigen, Durchschrift zu den Akten nehmen, Beschluss des AG ___ ___ Gs ___/__ beifügen (zweifach) und absenden an

... Bank, ___;

< höfl., begl.:

In dem Ermittlungsverfahren gegen M. R. wegen des Verdachts der Untreue nehme ich Bezug auf den anliegenden Beschluss des Amtsgerichts ___ vom ___ und auf § 161a StPO, soweit ich um zeugenbeweisliche Auskünfte ersuche.

Ich bitte mir mitzuteilen,

a) von wann bis wann die im Beschluss genannten Konten bei Ihnen geführt wurden,

b) ob, welche und von wann bis wann weitere Konten für den Beschuldigten ___ bei Ihnen geführt wurden,

c) wer neben ___ zeichnungsbefugt war oder ist.

Darüber hinaus bitte um die Übersendung der im Beschluss bezeichneten Schriftstücke. Auf die Abwendungsbefugnisse zu den zu lit. b) bis d) benannten Schriftstücke weise ich hin.

Abschließend bitte ich zur Vermeidung erfolgloser Ermittlungshandlungen darum, den Beschuldigten und seine Angehörigen nicht davon zu unterrichten, dass die Staatsanwaltschaft wegen dieser Aufforderung zur Auskunftserteilung und Herausgabe von Unterlagen an Sie herangetreten ist. Ich gehe davon aus, dass diese Gefahr nicht mehr bestehen wird, wenn nach vollständiger Erledigung meines Ersuchens ein Monat vergangen ist. Anderenfalls werde ich Sie gesondert unterrichten. >

2. Schreiben fertigen, Durchschrift zu den Akten nehmen, Beschluss des AG ___ vom ___ beifügen (zweifach) und absenden an

... Bank, ____;

< gleichlautend wie Nr. 1. >

3. Schreiben fertigen, Durchschrift zu den Akten nehmen, Beschluss des AG ____ vom ___ beifügen (zweifach) und absenden an

... Bank, ____;

< gleichlautend wie Nr. 1. >

...

... Wv. des Retentheftes am ___ .

6. Anhang

6.1 keine richterliche Überprüfung der Zweckmäßigkeit

LG Hannover, Beschluss vom 10.10.01 - 33 Qs 193/01 -

Auszug:

"Im Rahmen des gegen den Beschuldigten wegen des Verdachts des Betruges geführten Ermittlungsverfahrens sind zur weiteren Aufklärung des Sachverhaltes und zur Feststellung der Personalien des Beschuldigten sämtliche das von dem Beschuldigten gegenüber der Geschädigten angegebene Bankkonto mit der Nr. (Kontonummer) bei der (Bank) betreffende Unterlagen gemäß § 94 Abs. 1 StPO als Beweismittel von Bedeutung. Den auf Beschlagnahme gemäß §§ 98 Abs. 1, 94 StPO gerichteten Antrag der Staatsanwaltschaft vom 18.08.2001 hätte das Amtsgericht nicht unter Hinweis auf die gemäß §§ 161, 161a StPO bestehende Auskunftspflicht der (Bank) zurückweisen dürfen, weil der Ermittlungsrichter gemäß § 162 Abs. 3 StPO allein die gesetzliche Zulässigkeit der beantragten Untersuchungshandlung ... zu prüfen hat."

6.2. Durchsuchung von Bankschließfächern ist keine Wohnungsdurchsuchung

BVerfG, 3. Kammer des 2. Senats, Beschluss vom 16.10.02 - 2 BvR 1306/02

Leitsätze:

1. Bei dem Bankschließfach einer Person handelt es sich nicht um Räume, die dem Aufenthalt oder Wirken von Menschen dienen, mithin nicht um "Wohnungen" i.S. von Art. 13 Abs. 1 GG.

Soweit Art. 13 GG betroffen ist, berührt die Durchsuchung von Bankschließfächern ausschließlich das Hausrecht der betroffenen Bank.

2. Durchsuchung und Beschlagnahme stellen regelmäßig einen schwerwiegenden Eingriff in die grundrechtlich geschützte Lebenssphäre des Betroffenen dar. Deshalb ist es Aufgabe des Richters, von vornherein für eine angemessene Begrenzung der Zwangsmaßnahme Sorge zu tragen.

Der Richter hat durch hinreichende tatsächliche Angaben über den Tatvorwurf und konkrete Kennzeichnung der zu beschlagnahmenden Beweismittel sicherzustellen, dass der Betroffene die Reichweite des Eingriffs ermessen und kontrollieren kann.

Durchsuchung beim Berufshelfer

Rechtsanwalt Birkenstock schreibt hierzu:

"**Durchsuchung der Praxis des Beraters**

Grundsätzlich Voraussetzungen wie bei Durchsuchung beim Unverdächtigen

Gelegentlich versucht Steufa den Berater zu verdächtigen um einfacher an dessen eigene Unterlagen (Handakten) kommen zu können

In der Rechtsprechung war lange unklar, was denn nun beschlagnahmt werden kann und was nicht. Hierzu kann das folgende zusammengefasst werden:

Nach herrschender Meinung sind alle diejenigen Unterlagen die im Vertrauensverhältnis zwischen Mandant und Berater entstanden sind geschützt (Handakte im engeren Sinn)

Das Durchblättern der Handakte mit dem Ziel festzustellen ob diese ausschließlich solche Unterlagen enthält wird allgemein als zulässig angesehen. Um Streit zu vermeiden: Handakte versiegeln lassen, mitgeben und Richter entscheiden lassen ob Beschlagnahmefähig oder Beschlagnahmefrei

Unterlagen die nicht unter die Definition "Vertrauensverhältnis" fallen, wie z.B. Buchführungsunterlagen, Korrespondenz des Mandanten mit Dritten, Unterlagen die beim Berater lediglich aufbewahrt werden, Datenträger mit solchen Daten etc. können auch beim Berater beschlagnahmt werden

Die Durchsicht des Computers wird als zulässig angesehen. Maßnahmen finden ihre Grenze im Verhältnismäßigkeitsgrundsatz"

Im Großen und Ganzen hat der Autor recht:

1) Eine Durchsuchung allein zur Suche und Sicherstellung beschlagnahmefreier Gegenstände (§ 97 Abs. 1 StPO) ist unzulässig.

2) Beschlagnahmefrei sind vor allem schriftliche Mitteilungen in den Händen von zeugnisverweigerungsberechtigten Angehörigen (§ 52 StPO) oder Mitteilungen, Aufzeichnungen und ärztliche Untersuchungsbefunde in den Händen von Berufshelfern (§ 53 StPO; Ärzte, Steuerberater, Rechtsanwälte u.a.).

3) Aus dem Grundsatz des freien Verkehrs zwischen Verteidiger und Beschuldigtem (§ 148 StPO) hat die Rechtsprechung eine Erweiterung der Beschlagnahmefreiheit abgeleitet: Auch der Schriftverkehr, der die Verteidigung des Beschuldigten im aktuellen Verfahren betrifft und der sich in der Hand des Beschuldigten befindet, ist beschlagnahmefrei. Der Grund hierfür ist, dass im Interesse der "Waffengleichheit" die Strafverfolgungsbehörden keine Kenntnisse von der Verteidigungsstrategie bekommen sollen.

4) Die Beschlagnahmeverbote gelten nicht, wenn der Berufshelfer selber Beschuldigter, Anstifter oder Begünstiger einer Straftat seines Mandanten oder einer selbständigen Tat ist (§ 97 Abs. 2 StPO). Die Tatwerkzeuge und die Beute dürfen selbstverständlich auch beim Berufshelfer beschlagnahmt werden (§ 97 Abs. 2 S. 3 StPO).

5) Beschlagnahmeverbote bestehen auch dann nicht, wenn der Berufshelfer über diese Beweismittel außerhalb des Kernbereichs seiner berufshelferischen Tätigkeit verfügt. Dies gilt ganz besonders für Buchhaltungsunterlagen in der Hand des Steuerberaters. Über die Handelsbücher, Abschlussübersichten und Jahresabschlüsse verfügt der Steuerberater nur, wenn er abseits von seiner steuerberatenden Tätigkeit auch die originären Buchführungsaufgaben des Kaufmanns übernimmt. Diese kaufmännischen Unterlagen seines Mandanten sind beschlagnahmefähig.

   Eine Frage des Einzelfalls ist es, ob eine rein steuerliche Bilanz außerhalb eines steuerstrafrechtlichen Ermittlungsverfahrens beschlagnahmt werden darf. Für den Konfliktfall schlage ich vor, zunächst gemäß § 110 Abs. 2, Abs. 3 StPO zu verfahren.

6) Computerdaten sind Papiere im Sinne von § 110 StPO. Dazu nimmt der gesonderte Aufsatz in den Themen des EDV-Workshops Stellung: Sichtung gemäß § 110 StPO.

7) Notwendige Ergänzung:

   Dem Wortlaut nach gibt es keine Vorschrift in der Strafprozessordnung, die es den Ermittlungsbeamten erlaubt, den Telefonverkehr oder die Benutzung der EDV / DFÜ während einer Durchsuchung zu untersagen. Aus § 164 StPO ist jedoch der Grundsatz zu entnehmen, dass die Durchsuchungsbeamten alle Maßnahmen zu treffen haben, die den Erfolg der strafprozessualen Maßnahme sichern.

   Gerade in der Anfangsphase einer Durchsuchung, ich nenne sie Orientierungsphase, während der die räumliche und personelle Situation erfasst, Warnungen an Mittäter und Beweismittelvernichtungen verhindert werden müssen, sind Außenkontakte - orientiert am Einzelfall und besonders daran, ob beim Verdächtigen oder beim Unbeteiligten

durchsucht wird - zu unterbinden und andere Beschränkungen zulässig. Je nach den örtlichen und sachlichen Gegebenheiten müssen diese Beschränkungen mit fortschreitender Zeit gelockert werden.

Wegen der Kontaktaufnahme zum Rechtsanwalt oder zum Verteidiger gilt:

Wenn der Durchsuchungsleiter meint, es könne eine Verdunkelung erfolgen, so wählt er selber die vom Betroffenen genannte Telefonnummer an, vergewissert sich, dass tatsächlich eine Verbindung zum Rechtsvertreter besteht und gibt den Hörer weiter.

Sinngemäß gilt dies für alle weiteren Anordnungen im Zusammenhang mit der Art und Weise der Durchsuchung.

Beschlagnahme zu verjährten Taten (1997)

Unter einer versteckten Problemstellung hat das LG Köln (LG Köln wistra 97, 237 f.; mit Anmerkung von Stahl, ebd., S. 238) die Beschlagnahme solcher Beweismittel für unzulässig angesehen, die sich (allein) auf verjährte Taten beziehen. In der Sache hat das LG Köln entschieden, dass die Steuerfahndung nach § 404 AO keine Befugnis zur Beschlagnahme solcher Beweismittel hat, die sich auf strafprozessual verjährte Taten beziehen, auch wenn die Steuerfahndung im übrigen beauftragt ist, die weitergehenden, steuerlich unverjährten Handlungen des Beschuldigten aufzuklären.

Diese Entscheidung gibt Anlass zu drei Anmerkungen:

1) Das Gericht scheint einen Gedankenfehler zu begehen, weil der Beschuldigte wegen der strafrechtlich verjährten und steuerlich noch nicht verjährten Tatbestände den Mitwirkungs- und Auskunftspflichten nach den §§ 90, 93 AO unterliegt. Soweit also die Steuerfahndung im Rahmen ihrer steuerstrafrechtlichen Durchsuchungen Beweisstücke vorfindet, die zwar über strafrechtlich verjährte, hingegen aber über steuerlich noch nicht verjährte Umstände Auskunft geben, so wäre der Betroffene nach § 97 AO zu ihrer Vorlage verpflichtet. Eine Berechtigung zur Mitnahme ergibt sich somit schon aus der Abgabenordnung und kann nicht durch strafprozessuale Beschränkungen suspendiert werden.

2) Die Entscheidung greift jedenfalls dann nicht, wenn "betagte" Beweisstücke Auskunft über solche Sachverhalte geben, die in strafrechtlich nicht verjährter Zeit relevant bleiben.

3) Das LG Köln meint, dass solche Beweisstücke nicht beschlagnahmt werden dürften, die verjährte Straftaten begründen (dabei aber nicht in unverjährte Zeit fortwirken). Bei der Strafzumessung sind nach § 46 Abs. 2 StGB hingegen gerade auch die Umstände des Vorlebens des Beschuldigten zu ermitteln, so dass ich diese Beschränkung für schlicht falsch halte.

Teil 2: Telekommunikation

Provider und Netze. Technische Funktionen

Dem Wort "Provider" (englisch für "Ernährer" oder "Versorger") begegnen wir permanent im Zusammenhang mit Telekommunikations- (TK-) und Internet-Dienstleistungen. Dabei haben sich inzwischen einige Begriffe gebildet, die verschiedene Dienstleistungen von Providern unterscheiden. [89]

Im umgangssprachlichem Sinne ist der Provider das Unternehmen, das dem Kunden unmittelbar den Zugang zu einem Telekommunikationsnetz, zum Internet oder zu anderen Teilnetzen verschafft.

Genauer gesagt handelt es sich dabei um einen Zugangsprovider (Access-Provider, englisch für "Zugriff", auch Network-Provider) oder ISP (Internet Service Provider).

Beschränken wir uns auf die Internet-Dienste:

Während der einfache Zugangsprovider nur einen eigenen Internet-Server betreibt und seinen Kunden zur Verfügung stellt, wird von einem ISP (teilweise auch "Link-Provider") etwas mehr verlangt: Er betreibt ein Teilnetz als Bestandteil des Internets. Bekannte ISP sind z.B. das Deutsche Forschungsnetz (DFN) und der Onlinedienst T-Online.

Bei einem Internet-Server handelt es sich im einfachsten Fall um einen Rechner, der einerseits mit anderen Rechnern im Netz und andererseits über Modem-, ISDN-, DSL- oder Standleitungen mit seinen Kunden verbunden ist. [90]

Zwischen den Teilnetzen wird die Verbindung durch "Vermittlungsrechner", sogenannte Gateways und Router hergestellt (die Bereitstellung solcher Knotenrechner ist die Kerntätigkeit des "Network-Providers"). Diese müssen abgehende Daten adressieren und gegebenenfalls in eine Protokollsprache umwandeln, die von anderen Vermittlungsrechnern verstanden wird. Sie senden ihre Daten nicht zielgerichtet, sondern

---

[89] Die erste Fassung dieses Aufsatzes erschien im Januar 2001 im EDV-Workshop

[90] Anmerkungen:

Modem: Kunstwort aus den Worten Modulation / Demodulation: Ein Gerät, das in der Lage ist, digitale in akustische Signale umzuwandeln, die über das analoge Telefonnetz gesendet werden.

ISDN: Digitales TK-Netz, Abkürzung von "Integrated Services Digital Network". Trotz erheblicher Leistungsverbesserungen bei der analogen Signalübermittlung ist die digitale deutlich schneller und lässt eine Vielzahl zusätzlicher TK-Dienste zu.

DSL: Breitbandiges TK-Netz, das Daten bis zu zwölfmal schneller als per ISDN überträgt; Abkürzung von "Digital Subscriber Line". Im Deutschland ist DSL am bekanntesten als T-DSL, weil es von der Telekom beworben wird. Diese versucht ihre Kunden dazu zu bringen, für Internet-Verbindungen nur noch DSL und nicht ISDN zu verwenden, weil sie Überlastungen des Telefonnetzes befürchtet. Die analoge Telefonie, ISDN und DSL verwenden dieselben Telefonkabel, aber unterschiedliche Trägerfrequenzen.

Standleitungen bestehen unabhängig von den übrigen TK-Netzen. Selbst mit normaler Kabeltechnik können äußerst hohe Übertragungsgeschwindigkeiten erreicht werden, die durch Glasfaserleitungen (Lichtleiter) noch übertroffen werden.

ungerichtet in das jeweils andere Netz, das die Weiterleitung selber organisieren muss.

Während ein Gateway in der Lage sein muss, Verbindungen auf allen physikalischen und protokollarischen Schichten herzustellen (auf allen 7 Schichten des ISO-OSI-Modells), muss ein Router nur die protokollarischen oberen 3 Schichten auf der Basis des IP (internet protocol, siehe unten) bedienen. Router werden deshalb auch als Level-3-Gateways bezeichnet.

Switche funktionieren genau umgekehrt. Sie nehmen Daten aus ihrem eigenen oder einem fremden Netz auf und senden sie zielgerichtet an die im Dateikopf benannte Adresse weiter.

Auch Switches müssen gegebenenfalls die empfangenen Daten entsprechend verschiedener Protokollanforderungen übersetzen. Das zur Zeit wohl bekannteste und wichtigste Protokoll ist das TCP/IP (Transmission Control Protocol / Internet Protocol).

Das TCP besorgt die Segmentierung und Identifizierung der versendeten und empfangenen Daten und das IP die eigentliche Adressierung (Routing).

Zusammen dienen die beiden Protokolle TCP/IP nicht nur zur Datenübertragung zwischen den weltweit verbreiteten Rechnern im Internet, sondern zunehmend auch bei der Vernetzung firmeninterner oder häuslicher Computer. Diese Kleinnetze bilden sogenannte LANs (Local Area Networks, auch Ethernet genannt, wobei dieser Begriff eher die technische Leistungsfähigkeit und Architektur des Netzes anspricht; im Gegensatz hierzu: WAN = Wide Area Network). [91]

LANs benötigen ihrerseits Router zur Verbindung zu anderen Netzen. In der Praxis kann es sich dabei um ISDN-Karten, also um Einsteckkarten für einen PC, oder um eigenständige, z.B. an eine Telefondose angeschlossene Geräte handeln.

Zwei einzelne Computer können durch Netzwerkkarten - also Routern - und einem einzelnen umgepolten Kabel verbunden werden (Cross-Link-Kabel). Sollen mehr als zwei Rechner vernetzt werden, so können sie entweder hintereinander (in Reihe) geschaltet (sog. Bus-Topologie, gleichberechtigte Peer-to-Peer-Netzwerke) oder sternförmig durch einen Hub verbunden werden (aktiver Verteiler der Datensignale; Client-Server-Architektur, der Server stellt Dienste zur Verfügung, die der Client generell oder unter bestimmten Bedingungen [z.B. Zugangskennung] nutzen darf).

Es erscheint mir sinnvoll, die Aufgaben und Verantwortlichkeiten der verschiedenen Provider anhand der Regelungen des § 5 Teledienstegesetz (alte Fassung) vorzunehmen, die insoweit wortgleich mit §§ 6 ff. Mediendienstestaatsvertrag sind.

Die Unterscheidung zwischen Telediensten und Mediendiensten einerseits sowie die korrekte juristische Zuordnung soll insoweit ausgeklammert bleiben.

Thobias H. Strömer [92] bietet folgende Faustformel an:

---

[91] Marco Gercke, Rechtswidrige Inhalte im Internet (Book on Demand [Diss.], Köln 2000, S. 5), weist neben LAN und WAN noch auf das **MAN** hin (Metropolitan Area Network), das in einem räumlich beschränkten Bereich verschiedene Computer miteinander verbindet. Seine Dissertation enthält weitere technische Beschreibungen, die er als Grundlage für seine rechtlichen Schlussfolgerungen nimmt

[92] Online-Recht, Heidelberg 1999 (dpunkt Verlag, siehe auch Leseempfehlung), S. 12 f.

"Das Teledienstegesetz gilt für Anbieter von Telebanking, Teleshopping, Datenbanken und Suchmaschinen, aber auch für die meisten Content-Provider und vor allem für Homepage-Anbieter und Website-Betreiber. Hierzu zählen neben den privaten Angeboten im World Wide Web vor allem auch Unternehmenspräsentationen. ...

Der Mediendienstestaatsvertrag richtet sich dem gegenüber an diejenigen Content-Provider, die sich mit redaktionell gestalteten Inhalten an die Öffentlichkeit wenden. Die Online-Ausgaben von Printmagazinen wie Spiegel, Freundin und FAZ sind deshalb typische Mediendienste, die Website eines Softwarehauses dagegen ein Teledienst."

Strömer weist aber auch auf die bestehende rechtliche Unsicherheit hin: "Das Landgericht Düsseldorf hat ... apodiktisch die Behauptung aufgestellt, eine Website sei grundsätzlich ein Mediendienst ..."

Dirk M. Barton, Multimedia-Strafrecht, Neuwied und Kriftel 1999 (Luchterhand), S. 270, nimmt hingegen alle privaten Webseiten und Beiträge im Internet von den Regelungen des TDG und des MDStV aus, weil diese nur für kommerzielle Anbieter gälten.

Um die Verwirrung komplett zu machen: Im Zusammenhang mit markenrechtlichen Streitigkeiten sind private Homepages hingegen als gewerbliche Veranstaltungen angesehen worden.

Besser, nachvollziehbar und praktisch umsetzbar erscheint mir hingegen der Ansatz von Marco Gercke (Rechtswidrige Inhalte im Internet, Book on Demand (Diss.), Köln 2000, S. 26 ff.) zu sein. Er unterscheidet danach, wer die Initiative für einen Datenübermittlungsvorgang ausübt. push (stoßen, drücken) bezeichnet danach den Vorgang, dass eine Datenübermittlung auf Initiative des Anbieters, und pull (ziehen, zerren) den auf Initiative des Nutzers erfolgt.

Diesem Ansatz folgend weist Gercke den Telediensten die pull-Initiative der Nutzer und den Mediendiensten die push-Initiative des Anbieters zu.

Die Anbieter von Homepages unterliegen danach dem TDG.

Ich ordne die verschiedenen Provider-Aufgaben den drei gesetzlich definierten Typen zu (siehe linke Spalte):

Zugangsprovider,

Host-Provider und

Inhaltsprovider.

Im Gegensatz zum Zugangsprovider ist der Content-Provider ein Lieferant von Inhalten.

Während der Netzservice nur bedeutet, dass eine Übertragungs-Infrastruktur verwendet werden darf, stellt der Content-Service den Zweck zur Verfügung: Informationen in Form von Auskünften, Programmen, Bildern u.v.a.m.

Inhalts-Provider (Content-Provider) sind für ihre Veröffentlichungen gemäß § 8 Abs. 1 TDG n. F. unmittelbar zivil- und strafrechtlich verantwortlich. Dies gilt gleichermaßen für eigene wie auch für "zu eigen gemachte" Inhalte.

Umgekehrt sind Zugangs-Provider gemäß § 11 S. 1 TDG für fremde Inhalte grundsätzlich nicht verantwortlich.

Eine Zwischenstellung nimmt der Host-Provider nach § 8 Abs. 2, 11 S.11 TDG n.F. ein, der fremde Inhalte technisch zur Nutzung bereit hält.

Verantwortlichkeit verschiedener Provider nach § 5 Teledienstegesetz (TDG):

(1) Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.
[Inhalts- oder Content-Provider]

(2) Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich undzumutbar ist, deren Nutzung zu verhindern.
[Host-Provider]

(3) Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich.
[Zugangs- oder Service-Provider] (*)

(4) Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.

Eine automatische und kurzzeitige Vorhaltung fremder Inhalte auf Grund Nutzerabfrage gilt als Zugangsvermittlung.

[Proxy-Services]

(*) Gelegentlich werden auch Host-Provider als Service-Provider bezeichnet. Angesichts der Vielzahl von Internet-Diensten hat dieser Begriff keine vernünftige Trennschärfe und sollte ganz vermieden werden.

Eine neue Fassung des Gesetzes über die Nutzung von Telediensten (Teledienstegesetz - TDG) gilt seit dem 21.12.01 und eine neue Fassung des Staatsvertrags über Mediendienste (MDStV) seit Juli 2002. Die Vorschriften des § 5 a.F. wurden in den §§ 8 bis 11 TDG n.F. detailliert und der MDStV verwendet dieselben Formulierungen. Die hier geschilderten Grundsätze gelten fort.

Eine tiefere Auseinandersetzung mit der inhaltlichen Verantwortlichkeit erfolgt in dem Aufsatz Online-Strafrecht III. Ordnungswidrigkeiten im besonderen Multimediarecht.

Web-Provider - auch Presense-Provider und Webhosting- oder Hosting-Provider - stellen ihren Abonnenten Speicherplatz und technische Funktionen im Internet zur Verfügung.

Soll ein Informationsangebot im Internet abrufbar sein, so bedarf es zweierlei technischer Voraussetzungen: Das Informationsangebot muss physikalisch auf einem am Netz angeschlossenen Rechner permanent gespeichert und dieser Speicherstandort muss über die Netz-Infrastruktur ständig erreichbar sein.

Webhosting (Host = Gastgeber) bedeutet, dass ein Host-Provider seinen Abonnenten Speicherplatz im Internet anbietet.

Von quantitativ besonderer Bedeutung ist insoweit die Firma KPNQwest, die im Auftrag der Firma Strato bis Juli 2002 für mehr als 1,5 Millionen Domains der TLD (Top Level Domain) ".de" (für "Deutschland") den Web-Speicherplatz bereit stellte. Im März 2001 stürzte deren Server ab. Sie geriet - nach ihrer ausländischen Muttergesellschaft - im Sommer 2002 in Insolvenz, worauf Strato die deutsche Infrastruktur erwarb.

Andere Hostingangebote sind für die Abonnenten kostenlos und werden durch Werbung oder Sponsoren finanziert. Qualitativ unterscheiden sie sich im wesentlichen durch die Menge an Speicherplatz und dadurch, welche technischen Freiheiten die Abonnenten genießen dürfen.

Strato und Puretec (1&1) sind wohl die bekanntesten Domainnamen-Registrare in Deutschland und werden gelegentlich auch abschätzig "Domain-Discounter" bezeichnet. Sie haben - ebenso wie die anderen Mitglieder der DeNIC eG - einen direkten Zugang zur Datenbank der DeNIC (ungewöhnlich, aber wohl richtig: Registrator), in der schließlich die Inhaber-Daten (Registrierer) der deutschen de-Domains eingetragen werden. Auch die weitere Verwaltung der Inhaber-Daten überlässt die DeNIC im wesentlichen den Registraren.

Ein Host-Provider ist auch die DeNIC, die die de-Domains verwaltet. Sie sorgt dafür, dass allen de-Domainnamen eindeutige numerische IP-Adressen und dass Domains keine doppelten IP-Adressen zugeordnet sind. Als Datenbankbetreiber würde sie vereinzelt auch - wie die Anbieter von Suchmaschinen - als Information-Provider bezeichnet werden.

Zur Wahrnehmung ihrer Aufgaben unterhält sie eine für jedermann erreichbare Datenbank, die auch die Zugangsprovider mit den numerischen IP-Adressen versorgt, zu denen sie Domain-Adressierungen senden müssen.

Dem DNS-Server (Domain Name Service) der DeNIC sind örtliche Rechner nachgeordnet, die ihre Standorte zumeist an Hochschulen haben.

Die Domainnamen stellen - wie das Dateisystem - eine Art Aufsatz über dem numerischen System der IP-Adressen dar. Wenn ich in meinen Browser eine Domain-Adresse eingebe, muss diese natürlich in eine numerische IP-Adresse umgewandelt werden. Hierfür sind sogenannte DNS zuständig (Domain Name Server; selten auch bezeichnet als DMS [Domain Main Server]), die Datenbanken unterhalten, in denen die Domain-Adressen mit den ihnen zugeordneten IP-Adressen gespeichert sind.

Die DNS sind - ähnlich, wie wir es bei der Dateiverwaltung auf Speichermedien kennen gelernt haben - hierarchisch strukturiert. Mit der TLD (Top Level Domain) "de" rufen wir die Verwaltung für alle de-Domains auf, die von der DeNIC geleistet wird. Diesem nationalen DNS sind eine Reihe von lokalen DNS untergeordnet, die örtliche Zonen verwalten. [93]

Heise-Meldung vom 06.08.02:
DeNIC baut Nameserver-Netz aus

Auszug aus der Meldung:
"... Der zentrale ("primary") Nameserver für alle de-Domains wird vom DeNIC in Frankfurt betrieben. Kopien der Informationen werden auf mehreren "Secondary"-Nameservern vorgehalten. Zusammen mit den bereits vorhandenen Secondaries in Frankfurt, Karlsruhe, Dortmund, Wien, Amsterdam und Stockholm sind nach der Erweiterung zwölf Rechner im Einsatz. ..."

[93] Auf die Dokumentation von Links zu Meldungen und anderen Quellen im Internet wird in dieser Textfassung verzichtet. Wegen dieser Verknüpfungen siehe die Version im EDV-Workshop.

Das Kürzel "NIC" bedeutet "Network Information Center". Die numerischen IP-Adressen werden von 3 regionalen Internet-Registries verwaltet. Für Europa ist das das RIPE mit Sitz in den Niederlanden (Réseaux IP Européen). Die Schaltungen zwischen den in Deutschland verfügbaren Netzen besorgen 3 Austauschknoten (Exchange): De-CIX (Deutscher Commercial Internet Exchange), MAE Frankfurt (Metropolitan Area Exchange) und INXS München (Internet Exchange Point Munich).

Weitere Einzelheiten können bei der DeNIC (faq [frequently asket questions]) nachgelesen werden.

Zu den Host-Providern gehören auch die Anbieter verschiedener klassischer Internet-Dienste:

Mail-Server:

Auch beim eMail-Verkehr wird eine Mischung aus Netz-Infrastruktur und Zwischenspeicherung zur Verfügung gestellt.

Der Versender einer elektronischen Nachricht sendet diese an seinen Mail-Server als Zugangsprovider. Dieser leitet die Nachricht weiter an den Mail-Empfangsserver des Empfängers. Mit Gercke (s.o.) handelt es sich um eine pull-Initiative nach dem TDG.

Der Mail-Empfangsserver ist ein echter Host-Provider, weil er die Nachricht so lange in einer Mailbox zwischenspeichert, bis der Empfänger sie von ihm herunterlädt oder der Server die Nachricht löschen darf.

Gegebenenfalls bleibt die Nachricht bei ihm zur späteren Nutzung gespeichert, auch wenn der Empfänger die eMail herunterlädt.

Umgekehrt wird auch der Zugangsprovider des Versenders zum Host-Provider, wenn die Nachricht keinen Mail-Empfangsserver erreichen kann. Die Nachricht wird dann nämlich (in aller Regel) an den Absender zurückgesandt, wobei sie bei dessen Mail-Empfangsserver gespeichert wird, bis er sie wieder (mit entsprechenden Fehlervermerken) herunterlädt.

Siehe auch "Die Überwachung der Telekommunuikation" (anschließender Aufsatz).

Newsgroups / Usenet:

eMails und Newsgroups verwenden dieselbe technische Infrastruktur: Das Usenet.

Newsgroups sind - im Gegensatz zu eMails, die an einen oder mehrere namentlich benannte Empfänger versandt werden - öffentlich zugängliche Nachrichtenbereiche im eMail-Netz.

Man kann sich das Usenet als offene eMail-Zwischenspeicher vorstellen, mithin Host-Provider, die die Nachrichten für jedermann zur Verfügung stellen und jedermann eine eigene Äußerung der bereits gespeicherten Nachricht hinzufügen kann.

Je nach Art der Newsgroup kann es sich beim Betreiber um verschiedene Arten eines Providers handeln:

Werden die Newsgroups moderiert, also redaktionell betreut, inhaltlich kommentiert und einzelne Beiträge ausgeschlossen, so handelt es sich um die Dienste eines Inhalts-Provider. Sie sind als Mediendienste nach dem MDStV anzusehen ("push", s.o.).

Findet keine Moderation statt, so handelt der Betreiber bei der Veröffentlichung fremder "News" als Host-Provider. Auch in diesem Fall liegt bei ihm eine gewisse Nähe zum Inhalts-Provider vor, weil die Entscheidungen darüber, zu welchen Themen Newsgroups eingerichtet oder geschlossen werden, letztendlich dem Betreiber obliegen. Grundsätzlich müssen diese Newsgroups als Teledienste angesehen werden ("pull", s.o.).

Zugangsprovider müssen die Newsgroups im Usenet ihrerseits abonnieren, um sie ihren Kunden zur Nutzung zur Verfügung zu stellen. Dementsprechend sind auch sie Host-Provider. Auch hier liegt bei der Auswahl der Newsgroups eine gewisse Nähe zum Inhalts-Provider vor.

Siehe auch ergänzend das Urteil des AG Charlottenburg vom 25.01.02 - 230 C 150/01- (Quelle: jurpc.de):

> Ein in einer Internet-Newsgroup veröffentlichter Text mit herabwürdigendem Inhalt für eine andere Person verletzt deren Persönlichkeitsrecht und ist auch nicht als zulässige Meinungsäußerung anzusehen, wenn die Ebene der sachlichen Diskussion verlassen wird. Die Messlatte für die Streitkultur an einem privaten Stammtisch darf nicht dieselbe sein wie die für ein - quasi in der Öffentlichkeit stehendes - für jedermann zugängliches Diskussionsforum im Internet.

Internet Relay Chat (IRC)

Beim Chatten im IRC handelt es sich um eine schriftliche Online-Kommunikation in Echtzeit.

Der Chat-Dienst stellt hierzu inhaltlich benannte Foren zur Verfügung. Soweit er die Foren moderiert, handelt er sowohl bei der thematischen Auswahl der Foren wie auch bei der Moderation als Inhaltsprovider.

Was die Beiträge der "Chatter" in unmoderierten oder moderierten Foren anbelangt, handelt der Chat-Dienst als Host-Provider.

Gercke weist beide Formen den Mediendiensten zu ("push", s.o.).

Gästebücher

sind "Mini-Newsgroups", die Homepagebetreiber ("Nettizens") von ihrer Homepage aus zugänglich machen. Die Besucher der Homepage sollen hier ihre Kritik oder - eigentlich - ihren Lob für die gelungene Internetpräsentation hinterlassen.

Gästebücher sind Webhosting-Dienste. Im Detail gibt es aber große Unterschiede:

Bietet ein Web-Provider die Einrichtung von Gästebüchern seinen Kunden als zusätzlichen Dienst an, so wird hierfür der physikalische Speicherplatz genutzt, den der Kunde gemietet hat. Der Provider handelt insoweit als Host-Provider und sein Kunde als Moderator zusammen mit den Autoren der Gästebucheintragungen als Inhaltsprovider.

Selbständige Gästebuch-Services speichern hingegen die Nachrichten auf ihren eigenen Host-Rechnern. Sie sind Host-Provider ohne kontrollierenden Einfluss auf die Gästebücher ihrer Kunden.

Ungeachtet der rechtlichen Fragen, ob private, nichtkommerzielle Homepage-betreiber überhaupt als Tele- oder Multimediadienste angesehen werden können und wie in diesem Zusammenhang die Veröffentlichungen der Autoren in Newsgroups, Chat-Räumen oder Gästebücher zu beurteilen sind, lässt sich folgende technische Zuordnung machen:

Der Kunde hat keinen Einfluss darauf, was die Besucher seines Gästebuches inhaltlich hinterlassen. Insoweit handelt auch er als Host-Provider. Nimmt er die Beiträge inhaltlich zur Kenntnis (manche Gästebuch-Dienste übermitteln die Einträge auch automatisch per eMail), so kann er die Beiträge verändern, löschen oder kommentieren. Nimmt er diese Möglichkeiten wahr, handelt er als Inhaltsprovider.

Die hier vertretene Position deckt sich mit der jüngsten Rechtsprechung im Zusammenhang mit der Verantwortlichkeit von Auktionen im Internet. Siehe hierzu z.B. das Urteil des LG Potsdam vom 10.10.2002 - 51 O 12/02 - (Quelle: jurpc.de):

> 1. Soweit die Internet-Auktionsplattform eBay auch privat angebotene jugendgefährdende CD-ROMs, DVDs oder Computerspiele beinhaltet, ist eine Verantwortlichkeit von eBay hierfür gemäß § 11 Satz 1 TDG (n.F.) nicht begründet, da es sich um fremde Inhalte handelt, die sich eBay nicht zu eigen macht, da eBay hierfür nicht verantwortlich zeichnet, keine Bewertung oder Kommentierung der Verkaufsgegenstände abgibt, sondern lediglich den Kontakt zwischen Anbieter und Käufer vermittelt.
>
> 2. Eine Kenntnis von den jugendgefährdenden Inhalten gemäß § 11 Satz 1 Nr. 1 TDG (n.F.) ist nicht anzunehmen, da hierfür das positive Wissen um die Strafbarkeit der einzelnen eingestellten Angebote erforderlich ist, was bei dem nicht moderierten, nicht redaktionell aufbereiteten und unkommentierten Forum für Auktionsangebote von eBay nicht der Fall ist.

Online-Dienste

stellen die breiteste Kombination von Provider-Aufgaben dar. Als Zugangsprovider bieten sie zunächst ihren Abonnenten den Zugang zu ihrem eigenen Netz (ISP). Daneben bieten sie eigene Inhalte (Inhalts-Provider) und ihren Kunden Speicherplatz für deren Homepages (Host-Provider). Insoweit bieten sie den Zugang zu fremden Inhalten gemäß § 11 S. 1 TDG an.

Außerdem verschaffen sie den Zugang zum Internet (Network-Provider), zu eMail-, Newsgroup- und IRC-Diensten (im wesentlichen als Zugangs-Provider) und fungieren als Mail-Empfangsserver (Host-Provider).

Proxy-Server

sind "Stellvertreterdienste" eines Zugangsproviders oder ISP und werden von den Abfragen der Abonnenten von Zugangs-Providern aktiviert. Sie speichern die Dateien aus fremden Netzen, um diese ihren weiteren Kunden schneller zur Verfügung zu stellen. Es handelt sich dabei um eine ganz vernünftige Sache, die auch von den Browsern aller PCs gemacht wird: Viele Dateien müssten eigentlich mehrfach aus fremden oder auch aus dem eigenen Netz geladen werden. Diese Downloads werden aber

physikalisch zwischengespeichert (Cache), um den Netztransfer zu verringern.

Aus dem Proxy-Server bekommen die Kunden die schon von Vorgängern abgefragten Dateien, wodurch sich ihr Downloadvorgang beschleunigt und die Datenübertragungen zwischen den Netzen verringert.

Auf diese technische Besonderheit spricht § 9 Abs. 2, 11 S. 1 TDG an: Proxy-Server sind Host-Provider, werden aber als (unverantwortliche) Zugangsprovider behandelt, solange sie die Zwischenspeicherung auf Kundenabfrage nur kurzzeitig und vorübergehend vornehmen.

Die Zwischenspeicherung darf nach der Begründung zum Informations- und Kommunikationsdienstegesetz (IuKDG, wovon ein Teil das TDG ist) 24 Stunden nicht überschreiten. Danach wird der Proxy-Provider wie ein Host-Provider behandelt und muss für fremde Inhalte einstehen, wenn er von verbotenen Inhalten Kenntnis hat und ihm die Verhinderung des Zugangs zu diesen verbotenen fremden Inhalten technisch zuzumuten ist.

Alle technischen Spielarten habe ich mit diesem Beitrag nicht untersuchen und darstellen können. Hier ein paar Nachträge:

APS (Applikation Service Provider) bieten Software über das Internet an (z. B. Buchführungssoftware, Office-Anwendungen und andere gelegentlich oder probeweise benötigte Programme)

AD-Server speichern, verwalten und versenden z.B. Werbebanner. Darüber hinaus müssen sie die Häufigkeit und Dauer der Verwendung der Werbebeiträge verwalten und abrechnen. Es handelt sich dabei um eine Kombination aller drei wesentlichen Providing-Typen.

Spider suchen die Websites des Internets ab und geben ihre Suchergebnisse zur Speicherung in Suchmaschinen ab. Hier gilt dasselbe.

Eine interessante Entwicklung stellen drahtlose Netze (**WLAN**, Wireless Local Area Networks) dar, über die Armin Medosch am 22.05.02 in Telepolis berichtet hat:

Freie drahtlose Bürgernetze. Das Comeback der Internet-Utopien mit den Wireless Local Area Networks

Provider und Netze. Tabellarische Übersicht

Provider	Tätigkeit	Vorschrift	Verantwortlichkeit
Zugangs-P.	vermitteln den Zugang zur Nutzung fremder Inhalte	§ 9 Abs. 1 TDG, § 5 Abs. 3 S. 1 MDStV	grundsätzlich keine Verantwortung für fremde Inhalte
Access-P.	engl. "Zugriff"		
Network-P.	Router zur Netzverbindung		
ISP, Link-P.	Internet Service Provider, Betreiber von Teilnetzen		
Host-P.	"Gastgeber", halten fremde Inhalte zur Nutzung bereit	§ 11 TDG, § 5 Abs. 2 MDStV	Verantwortlichkeit für fremde Inhalte dann, wenn der Provider (oder Anbieter) Kenntnis von ihnen hat und wenn es ihm technisch möglich und zumutbar ist, die Nutzung zu verhindern
Web-P., Presense-P., Webhosting-P., Hosting-P.	stellen ihren Kunden physikalischen Speicherplatz in einem Netz zur Verfügung		
Information-P.	Datenbank- und Suchmaschinen-Anbieter		
Inhalts-P.	stellen eigene Inhalte zur Nutzung bereit	§ 8 Abs. 1 TDG, § 5 Abs. 1 MDStV	volle Verantwortlichkeit
Content-P.			
Applikation Service Provider (APS)	bieten Software über das Internet an		
Proxy-Server	Host-P., die wegen der automatisch von ihren Kunden veranlassten kurzzeitigen Zwischenspeicherung als Zugangs-P. behandelt werden	§§ 9 Abs. 2, 10 S. 1 TDG, § 5 Abs. 3 S. 2 MDStV	keine Verantwortlichkeit, solange die Zwischenspeicherung 24 Stunden nicht überschreitet; darüber hinaus Verantwortlichkeit als Host.-P.

TDG i.d.F. des Art. 1 Nr. 4 Gesetzes vom 14.12.2001 mit Wirkung vom 21.12.2001

Die Überwachung der Telekommunikation

Soweit "Daten" physikalisch verkörperlicht wurden, sind sie als Sachbeweismittel beschlagnahmefähig (§§ 94, 95, 98 StPO). Dies gilt für die auf Datenträgern gespeicherten Daten (Festplatten, Disketten, CD-Rs usw.).

Die damit in Verbindung stehenden Probleme werden in dem Beitrag Sichtung gemäß § 110 StPO erörtert.

Über die Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO gibt die Projektbeschreibung des Max-Planck-Instituts für ausländisches und internationales Strafrecht - Freiburg Auskunft.

Von § 3 Nr. 16 TKG wird die Telekommunikation (TK) definiert als "technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen".

Wegen der im Zusammenhang mit der TK erhobenen, protokollierten und gespeicherten Daten muss nach den technischen Gegebenheiten und verschiedenen Ermächtigungs- und Eingriffsvorschriften differenziert werden [94].

Welche Daten dürfen TK-Unternehmen speichern und aufbewahren?

Bestands- und Vertragsdaten
§ 89 II Nr. 1 lit. a TKG; § 4 I TDSV

... sind die personenbezogenen Daten eines an der TK Beteiligten, die erhoben werden, um ein Vertragsverhältnis über TK-Dienste einschließlich ihrer inhaltlichen Ausgestaltung zu begründen oder zu ändern, und dürfen zu diesem Zweck gespeichert werden.

Verbindungsdaten
§ 89 II Nr. 1 lit. b TKG;
neu: § 100g III StPO

... sind die personenbezogenen Daten, die bei der Bereitstellung und bei der Erbringung von TK-Diensten erhoben werden. Sie dürfen gespeichert werden, soweit dies

zur Herstellung und Aufrechterhaltung von TK-Verbindungen (TKG)

und für die Bereitstellung von TK-Dienstleistungen (TDSV) erforderlich ist.

Transportdaten
§ 89 IV, V TKG

... sind Steuersignale und Nachrichteninhalte, die gemäß § 89 III TKG grundsätzlich nicht erhoben, verarbeitet und genutzt werden dürfen. Ausnahmen:

Die Transportdaten sind der Gegen-stand oder aus verarbeitungstechnischen Gründen Bestandteil des TK-Dienstes (§ 89 IV TKG) oder

[94] Einen guten Überblick bieten Bernd Holznagel u.a., Grundzüge des Telekommunikationsrechts, Münster, Hamburg, London 2000 (LIT Verlag), S. 191; das Buch ist jetzt neu bei Beck erschienen.

ihre Erhebung und Verarbeitung ist zur Durchführung von Umschaltungen oder zur Erkennung und Eingrenzung von Netzstörungen erforderlich (§ 89 V TKG).

Abrechnungsdaten
§ 89 II Nr. 1 lit. c TKG; § 6 I TDSV; § 19 MDStV

... sind wie die Vertragsdaten personenbezogene Daten, die für die ordnungsgemäße Ermittlung und zum Nachweis der Entgelte für TK-Leistungen, Tele- oder Mediendienste bis zu 9 Monate gespeichert werden dürfen (Verbindungsdaten).

Störungsbehebungsdaten
§ 89 II Nr. 1 lit. d TKG;
§ 7 I Nr. 1 TDSV

... sind personenbezogene Daten, die für die Erkennung und Beseitigung von Störungen an TK-Anlagen gespeichert werden dürfen.

Missbrauchsvermeidungsdaten
§ 89 II Nr. 1 lit. e TKG

... sind personenbezogene Daten, die für die Aufklärung und Unterbindung von Leistungserschleichungen oder anderer rechtswidriger Inanspruchnahmen des TK-Netzes, seiner Einrichtungen und der geschäftsmäßigen TK-Dienste gespeichert werden dürfen, sofern tatsächliche Anhaltspunkte für Missbräuche vorliegen.

Nach der Neufassung des § 9 II TDSV Ende 2000 dürfen diese Daten höchstens 6 Monate lang gespeichert werden (vorher: 1 Monat) [95]

Nach dem Teledienstedatenschutzgesetz soll dem Nutzer - wenn möglich - eine anonyme oder eine Nutzung unter Pseudonym ermöglicht werden. Die Provider sind grundsätzlich dazu verpflichtet, alle Daten sofort zu vernichten, die nicht für vertragliche Zwecke, insbesondere zur Abrechnung benötigt werden.

T-Online z.B. behält die " 'Nutzungsdaten' der Kunden nach eigenen Angaben 80 Tage lang ... - auch die der Nutzer einer T-DSL-Flatrate" [96].

[95] Die Frist von 6 Monaten ist eine Höchstdauer

[96] Holger Bleich, Joerg Heidrich, Ach wie gut, dass niemand weiß ... Wie anonym sind Internet-Nutzer wirklich?, c't 19/02, S. 124, 125

Welche Daten können die Ermittlungsbehörden aufgrund welcher Eingriffsnormen abfragen oder herausfordern?

Überblick:

Im Anschluss an Wolfgang Bär (Skript Strafrecht und Internet) lassen sich drei sinnvolle Gruppen von Telekommunikationsdaten bilden:

Bestandsdaten:
dauerhaft gespeicherte Kunden- und Vertragsdaten des Nutzers,
fest vergebene IP-Nummern und
eMail-Adressen.

Verbindungsdaten (§ 100g III StPO):
"nähere Umstände" der TK,
Absender und Empfänger,
Zeitpunkt und Dauer der Verbindung sowie
dynamisch vergebene IP-Nummern.

Inhaltsdaten:
Inhalte der TK (komplette Überwachung)
Standort bei der Mobil-Telefonie [97]

Kundendaten
(Teil der Bestandsdaten) Wegen der Rufnummern, Rufnummernkontingente, Namen und Anschriften (Kundendateien) bietet § 90 I TKG ein einfaches, automatisiertes Abrufverfahren bei der Regulierungsbehörde für Telekommunikation und Post an. Den Zugang zu diesen Daten müssen die TK-Anbieter der RegTP gewähren, so dass diese die Abfrageergebnisse unmittelbar abrufen und an den Auskunftsberechtigten weiterleiten kann. Die Website der RegTP hält u.a. die wesentlichen Gesetzestexte, Verordnungen und Verwaltungsvorschriften bereit. Auch die ausgegebenen Nummernkreise sind hier dokumentiert.

Wegen der Rufnummern, Rufnummernkontingente, Namen und Anschriften (Kundendateien) bietet § 90 I TKG ein einfaches, automatisiertes Abrufverfahren bei der Regulierungsbehörde für Telekommunikation und Post an. Den Zugang zu diesen Daten müssen die TK-Anbieter der RegTP gewähren, so dass diese die Abfrageergebnisse unmittelbar abrufen und an den Auskunftsberechtigten weiterleiten kann. Die Website der RegTP hält u.a. die wesentlichen Gesetzestexte, Verordnungen und Verwaltungsvorschriften bereit. Auch die ausgegebenen Nummernkreise sind hier dokumentiert.

Zur Abfrage berechtigt sind neben den Strafverfolgungsbehörden auch die Polizei zur Gefahrenabwehr, der Zoll, die Verfassungsschutzämter, der Militärische Abschirmdienst und der Bundesnachrichtendienst (§ 90 III TKG). Die Abfragen können mit einem standardisierten Formular oder auch direkt per Datenfernübertragung angefordert werden. Zuvor müssen sich die berechtigten Einrichtungen bei der RegTP angemeldet haben.

In der Vergangenheit ist ein reibungsloser automatischer Abruf von Kundendaten nicht immer möglich gewesen, so dass die Anfragen auch unmittelbar an die TK-Unternehmen gerichtet werden mussten.

§ 90 Abs. 3 TKG bestimmt, dass die Auskünfte über Kundendaten "unentgeltlich" erteilt werden. Dies gilt m.E. aber nur für das in den Absätzen 2 und 4 näher beschriebene "automatische Abrufverfahren" über die

[97] BGH [Ermittlungsrichter], Beschluss v. 21.02.01 - 2 BGs 42/2001

RegTP. Für die Direktanfragen der Ermittlungsbehörden gelten nach meinem Verständnis sinngemäß die Absätze 5 und 7, wonach eine Entschädigung nach dem ZSEG erfolgt.

Hierüber hat Streit bestanden und dieser dauert wohl auch noch an. Die Telekom zum Beispiel weigert sich nach meiner Erfahrung, allein auf § 90 TKG gründende Auskünfte zu erteilen und verlangt einen ausdrücklichen Hinweis auf § 89 TKG, um eine Entschädigung zu erlangen.

Diese Vorschrift betrifft aber - über die Kundendaten hinaus - die Auskunft über Vertragsdaten.

Die Pflicht zur Erhebung und Speicherung von Kundendaten gilt laut OVG Nordrhein-Westfalen auch für Prepaid-Kunden (Beschluss vom 17.05.02 - 13 A 5293/00 - JurPC Web-Dok. 218/2002):

Auch Anbieter von Prepaid-Produkten (z.B. Kartentelefon) sind zur Führung von Kundendateien mit Rufnummer, Name und Anschrift des Nummerinhabers sowie zur Prüfung der Identität des Nummerninhabers anhand bestimmter Dokumente verpflichtet.

Die Aufsichtsbehörde kann die Einhaltung dieser gesetzlichen Verpflichtungen durch Leitlinien sicherstellen und deren Verbindlichkeit gegenüber dem einzelnen Anbieter durch feststellenden Verwaltungsakt begründen.

Die Verpflichtung zur Führung von Kundendateien für sicherheitsbehördliche Auskunftsersuchen ist nicht auf die nach § 89 Abs. 2 TKG erlaubtermaßen erhebbaren Daten beschränkt.

Kontakt (Norddeutschland):

Deutsche Telekom AG, Zentralbereich Konzernsicherheit Telekommunikationsüberwachung:

ReSA, KS25
30145 Hannover Auskunftsersuchen:

ReSA, KS25, Auskunft
30145 Hannover

Debitel Kommunikationstechnik GmbH & Co. KG
Schelmenwasenstr. 37, 70567 Stuttgart

Zustelladressen für Überwachungsanordnungen (Mobiltelefonie, mit besonderen Dank an Herbert Dauben):

Dienstanbieter Name und Anschrift Tel. / Fax

D1 Deutsche Telekom AG Tel.: 0190 871210
53105 Bonn, Friedrich-Ebert-Allee 140 Fax: 0190 871166

D2 Vodafone D2 Tel.: 0172 7654934
40547 Düsseldorf, Am Seestern Fax: 0211 5332007

Eplus Eplus Service GmbH & Co. KG Tel.: 0177 4481122
14473 Potsdam, Edison-Allee 1 Fax: 0211 4484750

vodafone o2 O2 (Germany) GmbH & Co. OHG Tel.: 0190 871707
80992 München, Georg Brauchle Ring 23-25 Fax: 0190 871708

Vertragsdaten (Teil der Bestandsdaten)

Die personenbezogenen Daten, die für die Begründung, inhaltliche Ausgestaltung oder Veränderung eines Vertragsverhältnisses erhoben wurden, können von den bereits benannten Strafverfolgungs- und Ermittlungsbehörden gemäß § 89 VI TKG angefordert werden.

Hierzu zähle ich auch die Kontoverbindungen des Kunden, Auskünfte über die Vertragsdauer und über weitere Anschriften oder Bevollmächtigte des TK-Kunden. Für diese erweiterten Auskünfte bedarf es in aller Regel eines ausdrücklichen staatsanwaltlichen Auskunftsersuchens gemäß § 161a StPO (siehe ergänzend den Lexikonbeitrag zu Bankauskünften).

Der Aufwand der TK-Dienste wird nach dem ZSEG erstattet.

Verbindungsdaten

Bei den Verbindungsdaten musste man bis zum 31.12.2001 danach unterscheiden,

ob es sich um die Aufzeichnungen des Zugangsproviders (siehe hierzu den Beitrag über Internet-Provider) aus der Vergangenheit handelt, so dass ein Auskunftsersuchen auf § 12 FAG gestützt werden konnte,

oder ob es sich um die zukünftigen Verbindungsdaten handelt, so dass ein Aufzeichnungsverlangen nur auf § 100a StPO gestützt werden kann.

Anhand dieser Unterscheidung wird auch deutlich, worum es sich bei den Verbindungsdaten handelt: Es sind die Aufzeichnungen des Zugangsproviders über die Inanspruchnahme von technischen Leistungen seines Kunden. Soweit der Provider diese Daten nach dem TKG oder nach anderen Vorschriften erheben darf und zur Vertragsabwicklung speichern muss, sind sie physikalisch auf Datenträgern verkörpert und können insoweit auch vervielfältigt werden (Abrechnungsdaten, dynamische IP-Adressen).

Die zukünftig anfallenden Daten sollen hingegen zu den Zwecken der Strafverfolgung aufgezeichnet und womöglich sofort zur Verfügung gestellt werden (z.B. die Standorte eines Handy-Benutzers). Diese Aufzeichnungen zeigen eine deutliche Nähe zum Inhalt der TK, so dass die strengere Eingriffsnorm des § 100a StPO einschlägig ist.

Wegen der Verbindungsdaten sind auch die Aufzeichnungen von Host-Providern von Interesse. Strato z.B. protokolliert die Datenabfragen auf die Homepages seiner Kunden während der zurückliegenden 6 Wochen. Dies dient zur Abrechnung des Transfervolumens gegenüber dem Strato-Kunden. Dokumentiert werden damit aber auch die IP-Adresse und der DNS-Name des Zugangsproviders des "Besuchers".

2003 hat das Bundesverfassungsgericht entschieden, dass die Polizei auch auf die Verbindungsdaten von Journalisten zugreifen darf.

Aus der Urteilsbegründung [98]:

> "Presse- und Rundfunkfreiheit sind nicht unbegrenzt gewährleistet. Nach Art. 5 Abs. 2 GG finden sie ihre Schranken in den Vorschriften der allgemeinen Gesetze, zu denen auch die Strafprozessordnung und die sie ergänzenden Vorschriften mit ihrer prinzipiellen Verpflichtung für jeden Staatsbürger zählen, zur Wahrheitsermittlung im Strafverfahren beizutragen und die im Gesetz vorgesehenen Ermittlungsmaßnahmen zu dulden. Die in den allgemeinen Gesetzen bestimmten Schranken der Presse- und der Rundfunkfreiheit müssen

[98] Christiane Schulzki-Haddouti, Karlsruhe provoziert Gesetzesänderungen, Telepolis 13.03.2003

allerdings ihrerseits im Lichte dieser Grundrechtsverbürgungen gesehen werden. Im Rahmen der gebotenen Abwägung ist das Gewicht des Rechtsguts zu berücksichtigen, dessen Schutz das einschränkende Gesetz dient."

Leitsätze

1. Die öffentlichrechtlichen Rundfunkanstalten können sich zum Schutz der Vertraulichkeit der Informationsbeschaffung und der Redaktionsarbeit auf das Fernmeldegeheimnis aus Art. 10 GG und insoweit auch auf die Rechtsschutzgarantie des Art. 19 Abs. 4 GG berufen.
2. Richterliche Anordnungen gegenüber Telekommunikationsunternehmen, im Rahmen der Strafverfolgung Auskunft über die für Abrechnungszwecke bereits vorhandenen oder in Durchführung einer Zielwahlsuche zu ermittelnden Verbindungsdaten zu erteilen, greifen in das Fernmeldegeheimnis des von der Auskunft Betroffenen ein.
3. Derartige Eingriffe sind nur gerechtfertigt, wenn sie zur Verfolgung einer Straftat von erheblicher Bedeutung erforderlich sind, hinsichtlich der ein konkreter Tatverdacht besteht und wenn eine hinreichend sichere Tatsachenbasis für die Annahme vorliegt, dass der durch die Anordnung Betroffene mit dem Beschuldigten über Telekommunikationsanlagen in Verbindung steht.

Inhaltsdaten

stellen sinnbildlich das "Horchen an der Tür" oder das "Anklemmen an die TK-Verbindungstechnik" dar. Solche Maßnahmen sind nur unter den strengen Voraussetzungen des § 100a StPO zulässig. Diese Vorschrift galt bis zum 31.12.2001 auch für die Verbindungsdaten der Zukunft.

Der BGH vertritt im Beschluss 1 StR 177/02 vom 09.07.02 ausdrücklich, dass eine Einschränkung des § 100a StPO weder hinsichtlich der Verwertbarkeit noch hinsichtlich der Zulässigkeit einer darauf gestützten Maßnahme in Betracht kommt, wenn die Maßnahme Zeugnisverweigerungsrechte gemäß § 52 StPO berührt.

Jens Eckhardt und Holger Dambeck [99]widmen sich den aktuellen gesetzgeberischen Initiativen: Die Autoren stellen folgende Übersicht zur Verfügung:

Überwachung der Telekommunikation in Deutschland			
strafprozessuale Ermittlungen		Ermittlungen des Zollkriminalamtes	Verfassungsschutz, MAD, BND
§§ 100a, 100b, 100g StPO	§§ 100g, 100h StPO (seit 2002)	§§ 39 ff. AußenwirtschaftsG (AWG)	Gesetz zu Artikel 10 Grundgesetz (G10)
Inhalte einschließlich Verbindungsdaten	nur Verbindungsdaten	Inhalte einschließlich Verbindungsdaten	Inhalte einschließlich Verbindungsdaten

[99] Jens Eckhardt und Holger Dambeck Strengere Maßstäbe. Erschwerter Zugriff auf Verbindungsdaten ab 2002 geplant, c't 20/01, S. 54.

fehlerhafte Anordnung der TK-Überwachung

Der BGH hat mit seinem Beschluss vom 01.08.02 - 3 StR 122/02 - Stellung zum Begründungsumfang bei der Anordnung der (inhaltlichen) Überwachung der Telekommunikation gemäß § 100a StPO genommen. Er nimmt nicht nur den Ermittlungs- sondern auch den erkennenden Richter mit der Folge in die Pflicht, dass die mangelhafte Prüfung der Verwertbarkeit von Erkenntnissen aus der Telekommunikationsüberwachung als Revisionsgrund anerkannt wird (Volltext bei hrr-strafrecht.de).

1. In der Begründung des ermittlungsrichterlichen Beschlusses, durch den die Überwachung der Telekommunikation angeordnet oder bestätigt wird, ist die Verdachts- und Beweislage, die die Maßnahme rechtfertigt, darzustellen. Dabei kann im Einzelfall eine konkrete Bezugnahme auf Aktenteile genügen. (Leitsatz von BGHSt)

2. Ist die Darstellung der Verdachts- und Beweislage im ermittlungsrichterlichen Beschluss plausibel, kann sich der erkennende Richter, der die Verwertbarkeit der Überwachungsergebnisse zu beurteilen hat, in der Regel hierauf verlassen. Fehlt es jedoch an einer ausreichenden Begründung oder wird die Rechtmäßigkeit der Maßnahme konkret in Zweifel gezogen, hat der erkennende Richter die Verdachts- und Beweislage, die im Zeitpunkt der Anordnung gegeben war, anhand der Akten zu rekonstruieren und auf dieser Grundlage die Verwertbarkeit zu untersuchen (im Anschluss an BGHSt 41, 30). War die Überwachung der Telekommunikation in einem anderen Verfahren angeordnet worden, hat er hierzu die Akten dieses Verfahrens beizuziehen. dieses Verfahrens beizuziehen. (Leitsatz von BGHSt)

3. Unterlässt der erkennende Richter eine erforderliche Beiziehung von Akten und verhindert er dadurch die gebotene Prüfung der Rechtmäßigkeit der Überwachungsmaßnahme, liegt hierin ein eigenständiger Rechtsfehler, der im Einzelfall zur Aufhebung des tatrichterlichen Urteils in der Revision führen kann. (Leitsatz von BGHSt)

4. In einem rechtsstaatlichen Strafverfahren dürfen Erkenntnisse aus einer rechtswidrig angeordneten Telefonüberwachung nicht als Beweismittel verwertet werden. Dies gilt insbesondere in Fällen, in denen es an einer wesentlichen sachlichen Voraussetzung für die Maßnahme nach § 100 a StPO fehlt. So hat es die Unverwertbarkeit zur Folge, wenn der Verdacht einer Katalogtat des § 100 a Satz 1 StPO von vornherein nicht bestand (vgl. BGHSt 31, 304, 308 f.; 32, 68, 70; 41, 30, 31). Bei der Prüfung eines hinreichenden, auf bestimmte Tatsachen gestützten Tatverdachts und des Fehlens oder der Erschwernis anderer Ermittlungsmöglichkeiten räumt das Gesetz dem zur Entscheidung berufenen Ermittlungsrichter oder Staatsanwalt (§ 100 b Abs. 1 StPO) jedoch einen Beurteilungsspielraum ein. Als rechtsstaatswidrig - mit der Folge eines Verwertungsverbots - stellt sich die Anordnung der Überwachungsmaßnahme nur dann dar, wenn die Entscheidung diesen Spielraum überschreitet und daher nicht mehr vertretbar ist. Allein unter diesem Blickwinkel hat im weiteren Verfahren sowohl das erkennende wie das Rechtsmittelgericht die Rechtmäßigkeit der Maßnahme zu beurteilen (BGHSt 41, 30, 33 f.). (Bearbeiter von hrr-strafrecht.de)

Überwachung des eMail-Verkehrs

Technisch passiert folgendes:

1. Prozess	Absender	>	Zugangsprovider des Absenders (Durchleitung)	>	Netz (Durchleitung)	>	Mailbox des Empfängers (Speicherung)

2. Prozess	Mailbox des Empfängers (Speicherung)	< >	Netz (Durchleitung)	< >	Zugangsprovider des Empfängers (Durchleitung)	< >	Empfänger

Der fließende Datenverkehr darf nur unter den strengen Voraussetzungen des § 100a StPO abgehört werden. Dies betrifft vor allem die Zugangsprovider des Absenders und des Empfängers. Abhörmaßnahmen an diesen Stellen verlangen nach den besonderen Voraussetzungen des § 100a StPO.

Streitig ist die Rolle des eMail-Empfangs-Servers des Empfängers als Host-Provider. Das LG Hanau hat eine Beschlagnahme an dieser Stelle unter Anwendung des § 14 TDSV abgelehnt. Es sieht damit - in Analogie zum Schutz des Postverkehrs (§ 99 StPO), der vom Post-Briefkasten bis zum Haus-Briefkasten reicht - den gesamten Übermittlungsverkehr von eMails vom Versenden bis zum Empfangen der eMail am Computer des Empfängers als geschützt an.

Im klassischen Postverkehr wird der Inhalt der Nachricht aber bei einer Zwischenstation nicht gespeichert. Ebenso wenig wird der Inhalt einer Nachricht für mehrere Abfragen des Empfängers bereit gehalten, was heißt, dass die Nachricht über den Zeitpunkt des Empfangs beim Empfänger gespeichert wird (dies gilt m.W. auch für die klassische Telegraphie).

Nicht unberechtigt erscheint mir danach die Meinung verschiedener Literaturautoren, dass der eMail-Empfangs-Provider auch zur Herausgabe der Inhaltsdaten nach den einfachen Beschlagnahmevorschriften verpflichtet sei (§§ 94, 95, 98 StPO).

Ich bin der Meinung, dass auf jeden Fall die Inhaltsdaten unter den einfachen Voraussetzungen der §§ 94 pp. StPO beschlagnahmefähig sind, die nach dem Abruf des Empfängers auf seinem Server weiterhin gespeichert werden. Mit seinem Abruf ist der Inhaltsübermittlungsverkehr abgeschlossen und jede verbleibende physikalische Kopie wie das Carbon-Blatt im Abfalleimer oder die Kopie in der Hand des Boten als körperliches Beweismittel gemäß §§ 94, 95, 98 StPO zu behandeln und damit beschlagnahmefähig.

Völlig geklärt sind die Rechtsfragen noch nicht. Es bleibt abzuwarten, wohin sich die Rechtsprechung entwickeln wird. Ggf. können dann doch alle zwischengespeicherten (physikalisch gespeicherten) Daten in den Ermittlungsverfahren, die als Offizial- oder im besonderen öffentlichen Interesse geführt werden (Privatklageverfahren), nach § 94 Abs. 2 StPO beschlagnahmt werden.

Ergänzender Hinweis:

RA Klaus Sakowski: Beschlagnahme von eMails und Überwachung der eMail - Kommunikation

Ich teile die Auffassung von Sakowski nicht, dass die beim Durchsuchungsbetroffenen eingegangenen eMails dem besonderen Schutz der Postbeschlagnahme unterliegen. Der Schutzbereich umfasst nämlich nur die Strecke zwischen Post- und Hausbriefkasten. Dort angekommen greifen die allgemeinen Vorschriften zur Beschlagnahme nach §§ 94, 95 pp. StPO.

Technik der Überwachung des eMail-Verkehrs

Auszug aus der Heise-Meldung vom 07.08.02:
RegTP will Übergangslösung für E-Mail-Überwachung schnell durchsetzen

"... Im Moment setzen die Provider bei Vorlage von Überwachungsanordnungen in der Regel sogenannte Shadow-Boxen ein, in denen sie Kopien des E-Mail-Verkehrs anlegen, die dann per FTP an die Ermittler weitergeleitet oder in POP-Boxen zur Selbstabholung bereitgehalten werden. Letzteres gefällt den Behörden überhaupt nicht. Ab 2003 will die RegTP daher nun zwei Regellösungen einführen, die möglicherweise auch gar nicht mehr zeitlich befristet würden: die Übermittlung der Kopie der zu überwachenden E-Mail mittels FTP und eine Übermittlung mittels SMTP.

... Ein Vertreter des Bundesbeauftragten für den Datenschutz erklärte die Verschlüsselung der Daten für unabdingbar. Dabei könnte die auch für Voice-Anbieter ab dem kommenden Jahr obligatorische Kryptobox von Secunet zum Einsatz kommen, zwei vergleichbare Kryptoboxen werden von der RegTP derzeit noch geprüft. Für die Übertragung per SMTP will die RegTP einen etwas leichter zu installierenden Transport Layer Security (TLS)-Tunnel vorschlagen. ..."

Man kann die Frage nach der Überwachung der Internet-Kommunikation auch ganz anders sehen.

Zum Beispiel meint "Roger Pilon vom radikalliberalen Cato Institute" (Heise-Meldung vom 07.06.02, FBI soll verstärkt Internet überwachen), dass es die "erste Pflicht einer Staatsregierung (sei), ihre Bürger vor Bedrohungen zu schützen. Die Überwachung der Internet-Kommunikation durch das FBI sei nicht viel mehr als ein Kontrollgang, den ein Polizist täglich durch sein Revier führt."

Laut BGH 2 ARs 373/02 – Beschluss vom 11.12.02 - gilt:

"Hat ein Anbieter von Telekommunikationsdiensten an einem anderen bekannten Ort als am Verwaltungssitz der Gesellschaft eine Abteilung errichtet, die den Abruf von Telekommunikationsdaten technisch umsetzt, so folgt daraus gemäß § 162 Abs. 1 StPO, dass nicht das Amtsgericht am Verwaltungssitz für die Anordnung der Übermittlung von Verbindungsdaten zuständig ist, sondern dasjenige Amtsgericht, in dessen Bezirk die Auskünfte zu erteilen sind."

Vermögensstraftaten unter Einsatz von Telekommunikationstechnik

Seit 2001 werden immer häufiger Verfahren bekannt, die Betrugsformen unter dem Einsatz von Telekommunikationseinrichtungen (Rückrufaufforderungen mittels Handys, Telefonen und Faxgeräten; Manipulation von technischen Anlagen und Dialer) und der Verwendung von Rufnummern für Mehrwertdienste betreffen. [100]

Die einzelnen Fallgruppen und Formen wurden bisher unstrukturiert im Lexikon des EDV-Workshops dargestellt und werden hier zusammengefasst. Der Darstellung, welche Tricks und Techniken bekannt geworden sind, gilt das besondere Interesse dieses Artikels. Neben den Fallgruppen werden auch die Grundsätze strafbaren Verhaltens, der Tarifstruktur der Mehrwertdienste, der Rechnungslegung und des Inkassos vorgestellt.

Mehrwertdienste sind Telekommunikationsdienstleistungen, bei denen neben der reinen Bereitstellung von Netzdienstleistungen (Lieferung der technischen Infrastruktur, Carrier-Dienste) Inhalte "eingekauft" werden. Dies können vor Allem neben den normalen premium rate - Angeboten (0190- und 0900-Nummern der Telefonie) auch Kurzwahl- und Auslands-Nummern sein. In diesen Fällen wird das dem Anrufer in Rechnung gestellte Entgelt (in Form verschiedener Aufteilungsschlüssel) zwischen dem Telekommunikationsnetzbetreiber (Carrier; das Unternehmen, das die reine Netzverbindung schaltet und seinen Kunden gegenüber abrechnet) und dem Mehrwertdienstanbieter geteilt (Anschlussinhaber der Mehrwertdienstnummer). Nur wegen des an den Mehrwertdienstanbieter abgeführten Teils kommt ein Vermögensschaden i.S.d. § 263 StGB in Betracht.

Überall dort, wo in diesen Fällen dem zahlenden Anrufer Leistungen versprochen, aber von dem Zahlung Erhaltenen nicht geleistet werden, muss genauer geprüft werden, ob dahinter eine betrügerische Absicht des angerufenen Anschlussinhabers steckt.

1. **Fallgruppen**

Voraussetzung dafür, dass überhaupt ein betrügerisches Verhalten in Betracht kommt, ist der Einsatz von Mehrwertdienstenummern (premium rate - Nummern der Rufnummerbereiche 0190, 0180, 0900 und Kurzwahlen), bei denen neben dem Entgelt für die schlichte Netznutzung ein weiteres Entgelt für die per Netz geleisteten Dienste erhoben wird. Solche Techniken, die "nur" schädigende Funktionen haben (z.B. die programmgesteuerte Anwahl einer Auslandsnummer über den B-Kanal einer ISDN-Anlage ohne Kenntnis des Computernutzers), werden nicht unter dem Gesichtspunkt eines Vermögensdelikts, wohl aber als Datenveränderung i.S.v. § 303a StGB zu prüfen sein.

Die Fallgruppen werden zunächst beschrieben, ohne dass eine eingehende strafrecht-

[100] Dieser Aufsatz erschien erstmals im Oktober 2003 im EDV-Workshop. Seine Originalfassung enthält eine umfangreiche Dokumentation und Erläuterung von Meldungen einschließlich gerichtlichen Entscheidungen, auf deren Wiedergabe in dieser Fassung verzichtet wird.

liche Prüfung erfolgt (diese muss anhand des praktischen Einzelfalls geleistet werden) und ohne dass auf die Mehrwertdienstenummern und das Inkasso eingegangen wird (siehe dazu Nr. 2. und 3.).

1.1. **Rückrufaufforderung (Festnetz, Fax, Handy, SMS)**

Bei den meisten Formen der Fallgruppen geht es darum, den Kunden dazu zu animieren, sorglos eine teure Servicenummer zurück zu rufen. Verwendet werden dazu u.a. ISDN-Festnetzanschlüsse, die die anrufenden Telefonnummern speichern, Anzeigen, die zu einem Fax-Abruf auffordern, Handys, die "Anrufe in Abwesenheit" anzeigen, und nicht zuletzt SMS-Mitteilungen, die zum Rückruf auffordern.

Allein die Sorglosigkeit der Rückrufer wird von unserer Rechtsordnung nicht geschützt. Dies gilt besonders dann, wenn der werbende TK-Dienstleister (siehe auch oben: "Provider und Netze" nebst tabellarischem Anhang) die Bedingungen, zu denen er seine Leistungen anbietet, klar und offen ankündigt und die angekündigte Leistung auch erbringt. In diesen Fällen liegen selbstverständlich keine Straftaten vor.

Zu den vergleichbaren Handlungsformen im Zusammenhang mit rechnungsähnlich aufgemachten Vertragsangeboten hat der BGH mit seinem Urteil vom 26.04.01 – 4 StR 439/00 - Stellung genommen (Quelle: hrr-strafrecht.de; siehe auch im Lexikon: betrügerische Angebotsschreiben (Offertenbetrug)).

In dem Leitsatz wird ausgeführt:

> Wer Angebotsschreiben planmäßig durch Verwendung typischer Rechnungsmerkmale (insbesondere durch die hervorgehobene Angabe einer Zahlungsfrist) so abfasst, dass der Eindruck einer Zahlungspflicht entsteht, dem gegenüber die - kleingedruckten - Hinweise auf den Angebotscharakter völlig in den Hintergrund treten, begeht eine (versuchte) Täuschung im Sinne des § 263 Abs. 1 StGB.

Diese Rechtsprechung kann m.E. unmittelbar für die hier vorgestellten Handlungsformen übernommen werden. Danach kann ein Betrug auch dann vorliegen, wenn der Täter zur tatbestandlichen Täuschung die Eignung der - inhaltlich richtigen - Erklärung, einen Irrtum hervorzurufen, planmäßig einsetzt und damit unter dem Anschein "äußerlich verkehrsgerechten Verhaltens" gezielt die Schädigung des Adressaten verfolgt, wenn also die Irrtumserregung nicht die bloße Folge, sondern der Zweck der Handlung ist. Insoweit genügt allerdings nicht bedingter Vorsatz; vielmehr ergibt sich schon aus dem Erfordernis planmäßigen Verhaltens, dass die Annahme der Täuschung in diesen Fällen auf Seiten des Täters ein Handeln mit direktem Vorsatz voraussetzt (in Anlehnung an die Urteilsbesprechung bei hrr-strafrecht.de).

Somit könnte z.B. betrügerisches Handeln bei den SMS-Aktionen vorliegen, die auch mich erreicht haben:

> Diese SMS wurde Dir geschickt, weil es jemanden gibt der dich kennt und mag. Um herauszufinden wer, ruf 0190-829-6822
>
> Erst auf der nächsten Display-Seite wurde angezeigt:
>
> haltezeit 2 Min.Euro 1,86/Min.

Ganz sicher betrügerisch sind solche Aktionen, die es nur auf den Rückruf anlegen, ohne dafür eine Gegenleistung anzubieten. Beispiele dafür sind die Fälle, in denen nur Warteschleifen oder - in einem ganz dreisten Fall - nur das Freizeichen vom Tonband bei laufender Verbindung übermittelt wird. Wegen der Warteschleifen sind auch gestufte Varianten denkbar, in denen der Anrufer ohne Notwendigkeit in einer Warteschlange gehalten oder von geschultem Personal bewusst hingehalten wird. Bei der Abgrenzung zwischen straflosem und betrügerischem Handeln wird es im Einzelfall auf die verwendeten technischen Vorkehrungen und z.B. auf die Anweisungen ankommen, die dem Telefonpersonal gemacht wurden.

1.1.1. **eingesetzte Technik**

Sicherlich wird es auch den Täter geben, der mit eigener Hand ihm bekannte oder beliebige Rufnummern in der Hoffnung anwählt, er könne den Angerufenen zum Rückruf anreizen.

Der Gedanke an einen solchen "eigenhändigen" Täter drängt sich bereits deshalb auf, weil die Polizei und die Staatsanwaltschaften zunächst nur die Strafanzeigen einzelner aufgebrachter Telefonkunden wahrnehmen, die auf ihrer persönlichen Telefonrechnung Positionen finden, die sie als unberechtigt ansehen.

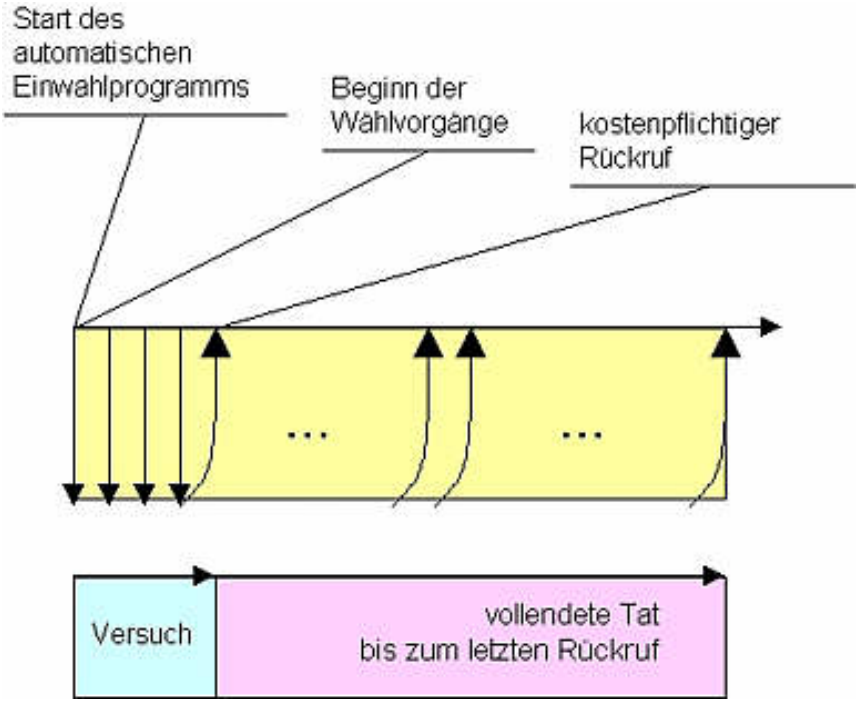
Schon im Zusammenhang mit call centern, deren Personal zum Hinhalten der anrufenden Kunden angehalten wird, wird deutlich, dass der Täter nicht eigenhändig tätig wird, sondern durch andere handelt. In Anlehnung an die gefestigte Rechtsprechung zum Anlegerbetrug durch Vermittler wird man die strafbaren Handlungen des Haupttäters daran orientieren müssen, zu welchem Zeitpunkt er das Personal angewiesen hat, unlauter zu handeln und die Anrufer dazu zu bewegen, die Verbindung aufrecht zu erhalten. Dadurch stellen sich eine Vielzahl von Einzeltelefonaten als Teile einer einzigen prozessualen Tat dar.

Dasselbe gilt dann, wenn unnötige Warteschleifen eingerichtet werden. Die Tathandlung des Täters besteht nicht darin, für jedes Telefonat die Schaltung der Warteschleife vorzunehmen, sondern Anweisungen zu geben oder selber die eingesetzte Technik so einzustellen, dass die ankommenden Anrufe in eine (unsinnige) Warteschleife geraten oder nur ein sehr teures Freizeichen erhalten (siehe oben). Der Rest läuft von alleine.

Auch wegen der "Anrufe in Abwesenheit" an Handy-Besitzer oder die Aufforderungen zum Rückruf per SMS (short message service) muss man sich davon freimachen, an einen eigenhändig handelnden Täter zu denken. Die Vorwahlen und aktiven Rufnummernbereiche (RNB) sind bekannt und werden von der RegTP veröffentlicht. Es ist dann einfach möglich, programmgesteuert systematisch oder mittels einer Zufallssteuerung die RNB abzuarbeiten und Rückrufaufforderungen in so kurzer Zeit zu senden, dass der Angerufene gar nicht die Chance hat, das ankommende Gespräch anzunehmen.

1.1.2. **prozessuale Tat**

Der Einsatz von Mittelspersonen oder einer automatisch ablaufenden Technik hat großen Einfluss darauf, wie die Tat des Täters prozessual zu beurteilen ist.



Grafik: Handlungs- und Tatschema bei automatisierten Rückrufaktionen

Die Strafverfolgungsbehörden werden sich davon freimachen müssen, den betrügerischen TK-Dienstleister als eigenhändig tätigen Täter zu behandeln. Der Betrug liegt in aller Regel nicht darin, dass der einzelne Anzeigeerstatter einen einzelnen Anruf teuer berechnet bekommt, sondern darin, dass der Täter sein Personal zu unlauterem Handeln anweist (Hinhalten, Starten eines Computerprogramms) oder Programmeinstellungen selber vornimmt. Das einzelne Telefongespräch ist dann nur ein Teilakt eines räumlich-zeitlich zusammenhängenden Geschehensablaufs, also einer einheitlichen Tat, die mit der Handlung (Anweisung, Programmstart) bereits einen versuchten Betrug darstellt, weil der Täter nichts weiter tun muss, um den Erfolg (die Animation der Anrufer und ihre Vermögensverfügungen durch Anwahl) zu erreichen.

endgültig eingestellt, Strafbefehl erlassen wird oder ein Urteil ergeht: Wegen aller anderen Schadenshandlungen des Haupttäters tritt dann Strafklageverbrauch ein.

Die praktischen Konsequenzen daraus können fatal werden - wenn wegen einer überhöhten Telefonrechnung das Ermittlungsverfahren vorschnell gemäß § 153a StPO

1.2. **versteckte Nummern (Netz- und Auslandsvorwahlen)**

Mit der Möglichkeit, Telekommunikations-Dienstleistungen mittels einer 0190er Nummer anbieten zu können, wurde auch der Missbrauch möglich. Hinterhältig und teuer können vor allem die frei tarifierbaren Telefonnummern 0190 0 und künftig 0900 (Premium-Rate-Dienste) werden - insbesondere dann, wenn der Telekommunikations- Dienstleister die "teure" Nummer maskiert - was sicherlich auch ein Anzeichen für eine betrügerische Absicht ist.

Sowohl in Telefongesprächen wie in Werbeanzeigen werden gelegentlich die Identität der Servicenummern versteckt, indem die Ziffernfolgen anders gruppiert werden. Beispiel unter Verwendung der nationalen Vorwahl (0049):

004 - 919 - 001 - 234 - 567 - 890

Eine andere Masche besteht darin, die Servicenummer hinter der Netzvorwahl der Deutschen Telekom zu verstecken. Das sähe dann so aus:

0103319001234567890.

Teilt man die Nummer in ihre Elemente auf, erhält man folgende Einzelheiten:

Netzvorwahl der Telekom	Premium-Rate-Dienst	Anschlussnummer
01033	**1900**	1234567890

Eine Variante davon dient zur Erschwerung der Arbeit der Ermittlungsbehörden und der Privatleute, die gegen einen TK-Diensteanbieter Forderungen durchsetzen wollen: Rechts werden an die Anschlussnummer noch eine oder mehrere Ziffern angefügt, so dass der Provider, der einen Rufnummernblock (RNB) von der Regulierungsbehörde für Telekommunikation und Post erhalten hat, zunächst die Auskunft gibt, dass es die erfragte Anschlussnummer nicht gibt. Beispiel:

..1234567890-47.

Während die Sensibilität der Mitbürger wegen der 0190er Nummern stark gestiegen ist, sind die Kosten anderer Servicenummern nicht allgemein bekannt. Die Neue Presse meldete am 04.10.02 im Zusammenhang mit der Kurzwahlnummer 11845 (Auszug):

> 11845 - Die neue Abzocke per Telefon
>
> Das Landeskriminalamt (LKA) warnt vor einer neuen Telefonbetrugs-Masche.
>
> "Die Täter antworten auf Zeitungsanzeigen und bitten die Inserenten auf Mailbox und Anrufbeantworter um einen Rückruf", sagt LKA-Sprecher Frank Federau. Dazu geben sie die Kurzwahlnummer 11845 an.
>
> Das Problem: "Wer diese Nummer wählt, tritt in die Kostenfalle", so Federau. Denn dort melde sich ein angeblicher Telekom-Auftragsdienst. Der Anrufer werde in eine aussichtslose Warteschleife geschickt - und die kostet 1,99 Euro pro Minute. Der gewünschte Teilnehmer werde nicht erreicht. Nach Auskunft der Telekorn hat das Unternehmen nichts mit der Servicenummer zu tun. ...

Über die Verwendung einer sehr teuren TK-Verbindung kann der Täter auch täuschen, indem er als Rückruf-Nummer eine Auslandsvorwahl angibt, die teure Tarife möglich macht. Dies gilt z.B. für die Salomonen mit der Vorwahl +677 oder 00677, bei deren Verwendung ähnlich hohe Kosten wie bei einer 01908-Nummer entstehen [101]. Auch Nauru mit der Vorwahl ...674 ist als Netzadresse eines automatischen Dialers bekannt geworden, der seit der Nacht zum 23.11.2002 den Rufnummernbereich des Mobilfunkproviders O2 (früher Viag Interkom) mit Kurzanrufen abarbeitete. Dies war die dritte Rückrufserie unter Verwendung von Naurus Netzvorwahl.

Zur zivilrechtlichen Wirksamkeit der Entgeltabrede bei verschleierten Auslandsvorwahlen hat das LG München I mit seinem Grundurteil vom 10.01.03 - 5 HK O 19188/01 - ausgeführt:

> Ein Vertrag, durch den die Telefonkunden mittels eines angebotenen und beworbenen Telekommunikationsdienstes planmäßig mit Gebühren für eine besonders teure internationale Verbindung (hier: Guinea in

[101] vergl. c't 10/02, S. 39

Afrika) belastet werden, ohne dass eine solche internationale Verbindung den Kunden tatsächlich zur Verfügung gestellt und von diesen genutzt wird, ist sittenwidrig, wenn durch Benutzung einer 01055-Vorwahl verschleiert wird, dass der Anruf über Guinea in Afrika geleitet wird.

1.3. **Anrufe an eigene Rufnummer (Computerbetrug)**

Über einen eher seltenen Fall hatte das Landgericht Hannover zu befinden. Es ordnete am 25.06.01 - 33 Qs 123/01 - als Beschwerdegericht die Untersuchungshaft gegen einen Beschuldigten an, dem 47 Straftaten des Computerbetruges (§ 263a StGB) mit folgenden Besonderheiten vorgeworfen wurden:

Der Beschuldigte war als Kontrolleur einer Putzkolonne in einem Hotel tätig. Er ließ sich zunächst eine 0190-Servicenummer einrichten. Im Mai 2001 benutzte er unberechtigt verschiedene Telefongeräte des Hotels und das Handy eines Hotelgastes, um seine kostenintensive Servicenummer anzurufen. Die dadurch entstandenen Gebühren in Höhe von mehreren tausend DM wurden seinem Konto gutgeschrieben.

Zur rechtlichen Würdigung hat der Kammervorsitzende vermerkt (Auszug):

" Der dem Beschuldigten zur Last gelegte Sachverhalt ist als Computerbetrug in der Tatbestandsalternative des "unbefugten Verwendens von Daten" im Sinne des § 263 a StGB strafbar. Das Herstellen der Telekommunikationsverbindung, entweder vom Festanschluss ... oder vom Mobiltelefon des Geschädigten O. ..., ist als Datenverarbeitungsvorgang zu werten.

Denn bei der Herstellung solcher Verbindungen handelt es sich um automatisierte Vorgänge, bei denen durch Aufnahme von Daten und deren Verknüpfung Arbeitsergebnisse - namentlich gebührenpflichtige Telekommunikationsverbindungen - erzielt werden. Über eine bloße Manipulation an der Hardware gehen die Tathandlungen des Beschuldigten demnach hinaus.

Der Beschuldigte hat diesen Datenverarbeitungsvorgang missbraucht, indem er als Unbefugter die Daten, die zur Herstellung der Verbindungen vom jeweils konkret genutzten Anschluss zu der von ihm betriebenen 0190ger Telefonnummer notwendig waren, eingesetzt hat, obwohl er zur Herstellung dieser Verbindungen nicht berechtigt war. Berechtigt waren die M.-Hotelgesellschaft in den Fällen in denen Verbindungen von hoteleigenen Anschlüssen hergestellt wurden; bzw. in den Fällen in denen die Telefonverbindungen vom Mobiltelefon aus erfolgten, der Geschädigte O. Eine vertragliche Befugnis, die jeweiligen Telefonanschlüsse in irgendeiner Form zu nutzen, hatte der Beschuldigte nicht.

... Im vorliegenden Fall ist Grundlage der Taten dagegen eine verbotene Eigenmacht des Beschuldigten. Dem Beschuldigten ist letztlich im Rahmen der Begrenzung des weit gefassten Tatbestandsmerkmals "unbefugt", welches jedes vertragswidrige Verhalten umfassen würde, ein betrugsspezifisches Verhalten zur Last zu legen. Geschäftsgrundlage eines jeden Telekommunikationsvertrages ist die in diesem Rahmen bestehende Berechtigung zur Nutzung der Anlage sowie der Inanspruchnahme der daraus resultierenden Leistung. Gehört aber die Befugnis des Täters zur Inanspruchnahme der Compu-

terleistung zur Geschäftsgrundlage, ist das Schweigen über den Mangel der Befugnis als schlüssiges Vorspiegeln der Verwendungsberechtigung zu werten. Dies ist vorliegend der Fall. Der Umstand, dass der Beschuldigte keinen Zugangscode überwinden musste, weil sowohl die Telefonanlage im Hotel als auch das Mobiltelefon freigeschaltet waren, spielt dabei keine Rolle, weil die Eingabe eines bestimmten Zugangscodes nur eine besonders evidente Form der Täuschung über die Berechtigung darstellt. "

1.4. **direkter Rückruf**

Rückruf-Abzocke nennt Urs Mansmann [102] den Missbrauch mit einem ganz neu geschaffenen "Mehrwertdienst". Wenn der Kunde es wünscht, kann er jetzt auf seine Kosten den Rückruf eines Dienstleisters zulassen. Den Tarif für den Rückruf bestimmt der Dienstleister durch die Auswahl seiner Rufnummer.

Gegen einen möglichen Missbrauch kann man sich kaum wehren. Selbst wenn man die Anwahl einer 0190-Nummer vom Telefonprovider, von der eigenen Telefonanlage oder per Software unterbinden kann, so gilt das nicht für ankommende Rufe. Grundsätzlich ist es nicht ausgeschlossen, dass der Kunde eine x-beliebige, fremde Rufnummer für den Rückruf nennt. Auch wenn man aufpasst und keine Anrufe von 0190-Nummern annimmt, könnte es passieren, dass das Faxgerät oder der Anrufbeantworter nicht so wachsam sind - das zeigt sich dann in der nächsten Telefonrechnung. Zitat aus dem Artikel von Mansmann:

"Die Telefongesellschaft Prompt hat den Rückruf als neue Einnahmequelle erschlossen. Für einen Anruf beim Kunden kassiert der Anbieter 0190-Gebühren. Der Ablauf ist einfach: Der Kunde ruft eine kostenfreie 0800-Rufnummer an und gibt dort die Nummer des Anschlusses an, auf dem er einen Rückruf wünscht. Anschließend erfolgt ein Anruf von Prompt - zu 0190-Konditionen. Den Posten findet der Angerufene anschließend auf der Telefonrechnung mit dem Stichwort TeleInternet Services.

Offensichtlich rechnet Prompt bereits damit, dass die Kunden für die Abrechnung kommender Anrufe kein Verständnis aufbringen: Auf der Webseite findet sich eine Information darüber, wie der fragliche Rechnungsposten zu Stande gekommen ist. Nach diesen Angaben kann der Rückruf entweder über den Anruf bei einer kostenfreien Rufnummer oder über das Internet angefordert werden. In beiden Fällen wird die Identität des Anrufers nicht überprüft.

Eines der ersten entsprechenden Angebote, 'Recall Direct' der Firma EST24, ging im Juli in Betrieb. Nach Angaben der Firma handelte es sich nur um einen Testlauf, allerdings tauchten die entsprechenden Posten bereits auf Telefonrechnungen von Kunden auf. Bei EST24 konnte man während des Tests von jedem beliebigen deutschen Anschluss aus anrufen, sogar vom Handy. Der Anrufer erhielt eine Ansage mit dem Hinweis, dass der Rückruf kostenpflichtig sein werde und der Aufforderung, die gewünschte Telefonnummer im Festnetz einzutippen. An dieser Stelle nannte der Anbieter einen Minutenpreis von 1,99 Euro."

[102] c't 10/02, S. 94

Knapp einen Monat später berichtete Mansmann [103] von einem Fall in einem Behindertenwohnheim, in dem alle Telefone für abgehende Anrufe gesperrt waren. Einer der Bewohner forderte jedoch per Handy Rückrufe auf sein stationäres Telefon an, die schließlich mit Kosten von rund 440 Euro zu Buche schlugen.

1.5. **0190-Dialer**

0190-Dialer sind Programme, die der Internet-Anwender installieren kann, um spezielle, aber kostenpflichtige Angebote aus dem Internet zu nutzen. In aller Regel wird dazu eine neue DFÜ-Verbindung installiert und als Standard für die Verbindung in das Internet per Modem oder ISDN-Verbindung definiert. Dadurch, dass die Verbindung als Standard eingestellt wird, wird zugleich bewirkt, dass künftig alle Verbindungen zum Internet über die teure 0190-Nummer hergestellt werden, auch ohne dass der "besondere Dienst" in Anspruch genommen wird.

Die "umlaufenden" Programme haben aber unterschiedliche Funktionsweisen und manche von ihnen verwenden gemeine, hinterhältige Tricks: Ohne das Wissen und ohne Kontrolle des Anwenders werden teilweise tiefgreifende Systemeinstellungen modifiziert, so dass der Anwender möglicherweise und unbemerkt alle seine künftigen Internetverbindungen über eine exorbitant teure 0190-Nummer abwickelt.

Urteil des LG Berlin vom 28.05.02 - 102 O 48/02 -:

> Im Anwendungsbereich von § 312 e BGB hat der Dienstleister dem Kunden bei Installation eines Dialers über eine 0190-Einwahl-Verbindung auch die in der BGB-InfoV bestimmten Informationen rechtzeitig vor Abgabe der Bestellung klar und verständlich mitzuteilen. Zu diesen Informationen gehören auch Angaben über die technischen Schritte, die zu einem Vertragsschluss führen sowie Informationen darüber, ob der Vertragstext nach dem Vertragsschluss vom Unternehmer gespeichert wird und dem Kunden zugänglich ist.

Vereinzelt ist davon berichtet worden, dass sich Dialer nicht rückstandsfrei deinstallieren lassen. Nach der Methode von Würmern sollen sich die Installationsdateien umbenennen und in andere Dateiverzeichnisse kopieren. Sie sollen dann bei jedem Computerstart neu installiert werden, weil die Installationsanweisung in die Registry oder andere Systemdateien geschrieben ist, die bei jedem Computerstart von Windows automatisch aufgerufen werden.

Hinterhältig und teuer sind vor allem die frei tarifierbaren Telefonnummern 0190 0 ... und künftig 0900 ... (Premium-Rate-Dienste). Missbrauchs-Beispiele werden von den Heise-Meldungen unten dokumentiert. In einem Fallbeispiel hat die einfache Anwahl einer Telefonnummer zu abgerechneten Kosten von 900 € geführt.

Im Oktober 2002 ist der erste "DSL-Dialer" des Betreibers GeoPhone unter der Auskunftsnummer 11845 aufgetaucht.

---

[103] c't 22/02, S. 46, Erste Rückruf-Opfer. Die neue 'Mehrwert'-Masche bringt schon Profit)

Ausgewählte Links zum Thema Mehrwertdienste und Dialer

FST	Verbraucher- informationen der fst-ev
Reg TP	Verbraucher- informationen der RegTP
DIALER UND RECHT	Dialer und Recht
Dialer Schutz Keine Chance 0190-Tricks	Dialerschutz
dialer hilfe.de	Dialerhilfe
Trojaner - Info	Trojaner - Info

Die Freiwillige Selbstkontrolle Mehrwertdienste (e.V.) und die Regulierungsbehörde für Telekommunikation und Post vermitteln hilfreiche Informationen.

Dialer und Recht konzentriert sich auf die rechtlichen Fragen bei der Nutzung von Dialern und Mehrwertdiensten.

Dialerschutz, Dialerhilfe und Trojaner-Info widmen sich verstärkt den technischen Einzelheiten und bieten Hinweise zum Verbraucherschutz.

Holger Bleich und Axel Kossel [104] haben die bekannten Dialer-Programme unter die Lupe genommen und festgestellt:

> "Trotz intensiver Suche haben wir keinen 0190-Dialer entdeckt, der sich völlig unbemerkt von uns ins Netz einwählt. Jedes der Programme versucht lediglich, sich mangelnde Vorsicht oder schlichte Unkenntnis der Surfer zunutze zu machen. Die kursierenden Horrorgeschichten von Software, die sich wie ein Trojanisches Pferd ohne irgendeine Nachfrage im System einnistet und unbemerkt ins Netz einwählt, halten wir für Legenden oder, um es im Netzjargon auszudrücken, für Hoaxes."

Die Rückruf-Masche wird auch gerne im Zusammenhang mit (unverlangt zugehenden) Spam-eMails versucht [105]:

> Hallo mein Schatz,
>
> Ich hatte es Dir ja schon letzte Woche versprochen. Meine neue Webcam läuft!!
>
> Sie befindet zwar noch in der Testphase aber läuft recht stabil. Schau es Dir mal an, denn uns trennen immerhin fast 700 km. Ich hoffe es versüßt Dir die 3 Wochen, die wir uns nicht sehen. Komm gesund von der Montage wieder nach Hause, Deine Melanie . (ihgdl!)
>
> Starte die Webcam HIER
>
> Du musst Dir noch das Webcamplugin installieren, da es sonst nicht funktioniert. (Erweiterung des IExplorer)

Wie das Bundeskriminalamt rate auch ich: Wegschmeißen!

---

104 Holger Bleich und Axel Kossel, Abzocke abblocken. Tipps gegen ungewollte 0190-Dialer, c't 1/02, S. 180

105 Diese nette Nachricht wurde von melanie-pauls0n@web.de an spochtfreun-de@ricklingen.de gerichtet. Ich bekomme den Schrott, weil ich noch immer der Webmaster der ricklingen-SLD bin.

Für die **strafrechtliche Beurteilung** schlage ich vor:

a) Erklärt die Menü- und Programmführung alle Funktionsweisen offen und deutlich - dass eine neue DFÜ-Netzwerkverbindung erzeugt oder eine bestehende überschrieben wird, dass alle künftigen Verbindungen über die 0190er Nummer abgewickelt werden - und muss der Kunde die Installation bewusst mit einem Klick bestätigen, dann liegt gar keine Strafbarkeit vor.

b) Werden Teile der Funktionsweise weniger offen erläutert - also etwa der Umstand, dass künftig alle Internetverbindungen mit der teuren Nummer abgewickelt werden oder dass bereits die einmalige Verbindungsaufnahme zu unerwarteten Kosten in Höhe von mehreren 100 € führt, dann kommt in Anlehnung an die Rechtsprechung zum Offertenbetrug § 263 StGB in Betracht (die Vermögensverfügung besteht in der unüberlegten, auf einer Täuschung beruhenden Installation des Programms; sie verwirklicht sich bei den künftigen, kostenauslösenden Einwahlen).

c) Werden Teile der Funktionsweise verschwiegen und erfolgt eine teilweise Installation ohne Kenntnis des Anwenders, so dürfte dies mindestens eine Datenveränderung i.S.v. § 303a StGB sein (Veränderung der DFÜ-Verbindung oder - ganz gemein - der Registry-Eintragungen). Wird die DFÜ-Verbindung zum teuren Anschluss unbewusst vom Anwender hergestellt, so dürfte § 263a StGB zum Tragen kommen. Die heimliche Installation stellt dann Beginn des Versuchsstadium dar.

d) Wird das Programm insgesamt heimlich oder sogar gegen den ausdrücklichen Willen des Anwenders gestartet (deaktivierter "Abbrechen"-Button), handelt es sich ebenfalls um eine Datenveränderung in Tateinheit mit versuchtem Computerbetrug. Die Abgrenzung zwischen Vorbereitungshandlung und Versuch muss im Einzelfall geklärt werden. Die Tat wird bei der nächsten Internetverbindung vollendet.

1.6. **URLs mit LogIn-Account**

Stellt man vor einem URL (Uniform Resource Locator, siehe auch im Handbuch: Hintergrund: Adressierung) das @-Zeichen ("Ät"), so können links davon Angaben für ein Zugangskonto und z.B. ein Zugangskennwort vermerkt werden. Ein solcher URL könnte so aussehen:

Konto-Angaben			Second Level Domain		Top Level Domain
http://www.sta-h.de%7c:powermaus	@	www	EDV-Workshop	.	de

Die Verwendung des @-Zeichen in einem Uniform Resource Identifier ist im RFC 2396 als Standard vorgesehen.

Man kann damit aber auch Surfer über die richtige Zieladresse täuschen:

1.7. **Angriff auf ISDN-Anlagen**

Fernwartungsfähige Telefonanlagen sind anfällig für Angriffe von außen. Lassen sie die Fernwartung zu und die Grundeinstellungen der Hersteller "offen", so fällt es Hackern leicht, über den ISDN-B-Kanal die Anlage zu manipulieren und z.B. so einzustellen, dass die Anlage selbsttätig teure 0190-Nummern anruft. In einem bekannt gewordenen Fall sind dadurch Kosten in Höhe von 4.000,- Euro verursacht worden. [106]

2. **Mehrwertdienste**

Die besonderen Servicedienste werden von der RegTP ausführlich dargestellt. Neben den (selten vorkommenden) Kurzwahlnummern sind für die strafrechtliche Praxis vor Allem die Mehrwertdienste von Bedeutung, die wegen ihrer hohen Kosten von den 0190-Nummern angesteuert werden. Auf diese Nummernkreise beschränkt sich zunächst die Darstellung.

2.1. **premium rate-Dienste**

Im Zusammenhang mit den Mehrwertdiensten hat die Regulierungsbehörde für Telekommunikation und Post die Ziffernblöcke (0190)-1 bis (0190)-9 verbindlich tarifiert. Wegen des Ziffernblocks (0190)-0 hat die RegTP aber ausdrücklich davon abgesehen, um eine flexible Tarifgestaltung zu ermöglichen. Die Deutsche Telekom AG hat die Folgeziffern (0190-0)-0 bis (0190-0)-9 für die RNB, die sie von der RegTP erhalten hat und Mehrwertdienste-Kunden anbietet, verbindlich tarifiert.

Andere Provider lassen eine Tarifierung zu, die von ihren Kunden bestimmt wird, die Mehrwertdienste anbieten wollen. In der Praxis ist zu beobachten, dass einzelne Mehrwertdienste-Rufnummern über eine Kette von bis zu mehr als zwanzig Zwischenhändlern weiter gegeben werden.

Jo Bager [107] schreibt:

> Der Protest gegen 0190-Abzocke wächst. 0190er-Nummern für ‘Telefonmehrwertdienste’ sind zum unkalkulierbaren Kostenrisiko geworden. Verbraucherschutzministerin Renate Künast fordert mehr Sicherheit für die Kunden.

Das OLG Hamm hat in seinem Urteil vom 05.11.02 - 19 U 41/02 - festgestellt, dass der Telefondienstleistungsanbieter eine aus dem Telefondienstvertrag folgende Nebenpflicht habe, zum Schutz des Kunden bei Dauerverbindungen über 0190-Nummern nach einer Stunde Gesprächsdauer eine automatische Trennung der Verbindung vorzunehmen.

2.2. **frei tarifierbare Nummern**

Die Gebühren für die premium rate-Nummern der RNBe 0190-0 - und jetzt 0900 - sind nicht behördlich festgesetzt, sondern können von den Inhabern selbst bestimmt werden. Im bisher bekannt gewordenen Extremfall wurde durch die einfache Einwahl eine Gebühr von 900 € in Rechnung gestellt.

Die premium rate-Nummern werden häufig über mehrere Zwischenhändler (bis zu mehr als 20 Zwischenhändler) an den Endkunden, den Mehrwertdienste anbietenden Anschlussinhaber abgesetzt. In Einzelfällen

---

[106] Die Einzelheiten werden beschrieben in Betrug per Tk-Anlage, c't 24/2002, S. 71.

[107] c't 6/02, S. 74, Wider die Dialer-Mafia

residiert der (angebliche) Dienstleister / Anschlussinhaber außerhalb des Zugriffs der deutschen Gerichtsbarkeit auf einer karibischen oder pazifischen Insel.

An erster Stelle der Zwischenhändlerkette werden die RegTP und ein Telefonnetzbetreiber (Carrier) oder Provider für TK-Dienste tätig, die große Rufnummernblöcke (RNB) abnehmen. Diese Carrier und Provider geben einen Teil der Rufnummern an andere TK-Provider weiter und erhalten dafür ein Entgelt. Solange es sich um verbindlich tarifierte Rufnummern handelt, ist bei der Weitergabe der Rufnummer klar, welche Gebühren mit ihr berechnet werden können. Bei den frei tarifierbaren 0190-0-Nummern bedarf es hingegen einer weiteren Kommunikation: Der Anschlussinhaber am Ende der Vertragskette muss seinem Vertragspartner mitteilen, welche Gebühren er seiner Anschlussnummer auferlegt. Wenn mehrere Zwischenhändler eingeschaltet sind, dann müssen Sie alle innerhalb ihrer Vertragskette über den genauen Tarif unterrichtet werden - bis hin zu dem "Kopfprovider", der den betreffenden RNB von der RegTP erhalten hat und die Rechnungslegung mit den größten Carriern am TK-Markt (voran die Telekom) organisieren muss. Denkbar ist auch, dass Provider unterhalb der Telefonnetzbetreiber die geschäftliche Abwicklung übernehmen.

Heise-Meldung vom 05.03.03
Aus 0190 wird 0900 (Auszug):

> "... Gemeinsam ist nun allen 0900-Nummern, dass sie frei tarifierbar sind. Die Verbindung kann also wenige Cent kosten, aber auch einige hundert Euro. "Die Kosten der telefonischen Verbindung müssen aber per Ansage angekündigt werden", sagt Boll. 0900-Webdialer sollen deutlich auf die Kosten und die Größe der Download-Datei hinweisen. Bei Missbrauch werden die Nummern sofort entzogen, versprechen die Regulierer.
>
> Trotz der freien Tarifierung vertrauen Verbraucherschützer den 0900-Vorwahlen mehr als den 0190-Nummern. "Die neuen Nummern bieten vor allem mehr Transparenz", so Michael Bobrowski vom Bundesverband der Verbraucherzentralen (vzbv) in Berlin. Denn bisher wurden die Vorwahlen in Blöcken an "Reseller" vergeben und von diesen weiterverkauft. Abzocker waren so kaum ausfindig zu machen. "Alle Anbieter sind bei uns registriert und dürfen die Nummern nicht mehr weitergeben", sagt Boll von der RegTP. "Unseriös arbeitende Anbieter können sich so nicht mehr wie bisher in der Anonymität verstecken", sagt auch Sascha Borowski aus Augsburg, Betreiber der Internetseite dialerschutz.de, die Ratschläge für den Umgang mit Dialern und Mehrwertdiensten gibt. "Betroffene haben endlich einen direkten Ansprechpartner."
>
> Zusätzliche Sicherheit verspricht auch die Deutsche Telekom in Bonn. 0900-Gespräche über das Netz der Telekom, die teurer als drei Euro sind, müssen mit den Tasten 1 und 9 bestätigt werden. "Bereits seit vergangenem Jahr werden 0190-Verbindungen nach 60 Minuten aus Sicherheitsgründen unterbrochen", so Sprecher Frank Domagala. Dies gelte künftig auch für die 0900-Verbindungen.
>
> Einheitliche Sicherheitsstandards soll die Änderung des Telekommunikationsgesetzes bringen, die sich zurzeit allerdings verzögert. Daher empfiehlt es sich für Verbraucher weiterhin, besonders auf der Hut zu sein. "Jeder sollte einen ungekürzten Einzelverbindungsnachweis anfordern", rät Boll. Nur so können schwarze Schafe ermittelt werden. Für diese speziellen Rechnungen dürfen die Anbieter laut RegTP keine zusätzlichen Gebühren verlangen. Ein anderer sinnvoller Schutz wird jedoch nur halbherzig ermöglicht: Jeder Kunde kann laut Telekommunikations-Kundenschutzverordnung (TKV) ein Rech-

nungslimit festlegen. Lediglich nach ausdrücklicher Zustimmung wird dieses überschritten. Doch die meisten Unternehmen ermöglichen die Funktion nur durch das Mieten eines speziellen Telefons und beschränken sie auf einen Warnton. ..."

2.3. Telekommunikations-Kundenschutzverordnung

Am 20.08.02 ist die Zweite Verordnung zur Telekommunikations- Kundenschutzverordnung in Kraft getreten, die eine Erweiterung des § 15 Abs. 1 S. 2 (angegeben werden müssen „die Namen, ladungsfähigen Anschriften und kostenfreie Servicenummer der einzelnen Anbieter von Netzdienstleistungen“) und mit § 13a eine neue Vorschrift eingefügt hat:

„§ 13a - Nutzung von Mehrwertdiensterufnummern

Diejenigen, die Kunden Nummern, mittels derer neben Telekommunikationsdienstleistungen weitere Dienstleistungen angeboten werden (Mehrwertdiensterufnummern) zur Nutzung überlassen, haben diese Kunden schriftlich darauf hinzuweisen, dass keine Werbung, Sachen oder sonstige Leistungen unter Verstoß gegen gesetzliche Vorschriften zugesandt oder sonst übermittelt werden dürfen. Hat derjenige, der einem Kunden eine Mehrwertdiensterufnummer zur Nutzung überlassen hat, gesicherte Kenntnis, dass diese Rufnummer unter Verstoß gegen Satz 1 genutzt wird, hat er unverzüglich geeignete Maßnahmen zur zukünftigen Unterbindung des Rechtsverstoßes zu ergreifen. Er hat insbesondere nach erfolgloser Mahnung soweit möglich die missbräuchlich verwendete Mehrwertdiensterufnummer zu sperren, wenn er gesicherte Kenntnis von einer wiederholten oder schwerwiegenden Zuwiderhandlung hat."

Die TKV enthält keine Straf- oder Ordnungswidrigkeiten-Vorschriften.

Ihre Anforderungen können deshalb nur im Zivilprozess eingefordert werden oder dadurch, dass im strafrechtlichen Verfahren ein Verstoß gegen sie als Indiz für unlautere Absichten angenommen werden (Garantenstellung). Eine deutlich Erleichterung zivilrechtlicher Streitfragen wird dadurch erreicht, dass der Zugangsprovider in seiner Rechnung den Namen und die Anschrift des Mehrwertdienstleisters angeben muss, dessen Forderung ausgewiesen wird.

TKR-Newsletter vom 08.06.02:

"Nach den neuen Vorschriften müssen alle Diensteanbieter, die Mehrwertdiensterufnummern an Endnutzer vergeben, auf die Einhaltung der gesetzlichen Vorschriften hinweisen und bei Zuwiderhandlung die Nummer entziehen. Im Interesse der Verbraucher können die Diensteanbieter jetzt Unternehmen, die sich wiederholt rechtswidrig verhalten, vom weiteren Angebot aussperren, so die Regierung. Der rechnungsstellende Telefondienstanbieter muss den Kunden künftig ausdrücklich darauf hinweisen, dass er die Zahlung der mit der Rechnung geltend gemachten Forderungen Dritter verweigern kann. So kann sich der Verbraucher bei Betrugsfällen wie dem unbemerkten Aufschalten sogenannter Dialer-Programme wirksamer schützen. Des weiteren verpflichtet die Verordnung die Telefondiensteanbieter in der Telefonrechnung die ladungsfähige Anschrift aller Dienstanbieter anzugeben, für die Forderungen geltend gemacht werden.

So habe der Telefonkunde die Möglichkeit, sich mit seinen Einwendungen direkt an die entsprechenden Anbieter zu wenden, argumentiert die Regierung."

Presseerklärung des Bundesministeriums für Wirtschaft und Technologie vom 31.07.02 :

"... Durch die Änderung der Telekommunikations-Kundenschutzverordnung werden die rechnungstellenden Diensteanbieter verpflichtet, die Telefonkunden in der Rechnung darauf hinzuweisen, dass sie gegenüber einzelnen strittigen Forderungen begründete Einwendungen erheben können.

Um die unerwünschte Werbung per Fax, E-Mail und SMS einzudämmen, erweitert die TKV-Änderung die Haftung des Netzbetreibers. Diejenigen Netzbetreiber, die Mehrwertdiensterufnummern zur Nutzung überlassen, werden verpflichtet, bei gesicherter Kenntnis einer rechtswidrigen Nutzung die missbräuchlich genutzte Mehrwertdiensterufnummer zu sperren.

Durch Erweiterung des § 15 Absatz 2 Satz 1 wird die weitgehend bereits bestehende Praxis, auch Namen und ladungsfähige Anschrift des jeweiligen Netzbetreibers auszuweisen, zur zwingenden Regelung. Darüber hinaus muss eine kostenfreie Servicenummer angegeben werden. ..."

TKR-Newsletter vom 25.11.02:

"Mit einem Gesetzentwurf, der kurzfristig erarbeitet und bereits Anfang Dezember der Öffentlichkeit zugeleitet werden soll, will die Bundesregierung den Missbrauch von Mehrwertdiensten bekämpfen und gleichzeitig die Verbraucherrechte stärken. So soll etwa die Transparenz bei den Preisangaben dadurch verbessert werden, dass künftig bei jedem Telefongespräch eine Preisansage vorgeschrieben werden soll. Dies geht aus einer Pressemitteilung des Bundesministeriums für Wirtschaft und Arbeit (BMWA) vom 19.11.2002 hervor. ... Die Vorschläge sehen unter anderem vor, eine Datenbank bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) für alle Mehrwertdiensterufnummern einzurichten (0190/0900er-Nummern, Auskunftsnummern 118 und die so genannten Nummern für Massenverkehr zu bestimmten Zielen wie 136, 137, 138). Insgesamt soll die Stellung der RegTP gestärkt werden ..."

3. **Inkasso**

Die teilweise als betrügerisch zu bewertenden Erlöse aus premium rate-Angeboten werden in aller Regel über das Rechnungswesen von Teilnehmernetzbetreibern (namentlich der Deutschen Telekom und anderen großen Carriern) eingezogen und an die Täter abgeführt.

Die Teilnehmernetzbetreiber sind nach § 15 TKV verpflichtet, ihren Kunden eine "Gesamtrechnung" zu stellen, die zugleich auch die "fremden Kosten" anderer Verbindungsnetzbetreiber (z.B. Call by Call-Anbieter) und Telekommunikations- einschließlich Mehrwertdiensteanbieter ausweist. Grundlage für die Rechnungsstellung und Forderungseinziehung sind im Einzelnen zwischen den Teilnehmernetzbetreibern abgeschlossene Abrechnungs- und Inkassoverträge.

Wegen der frei tarifierbaren (0190)-0-Rufnummern erhält der Teilnehmernetzbetreiber noch während der Verbindung die genaue Tarifierung von dem Netzbetreiber übermittelt, aus dessen Kontingent die angewählte Rufnummer stammt (also des Mehrwertdienstes). An den Netzbetreiber werden auch die Einnahmen abgeführt, die der Teilnehmernetzbetreiber von seinem

angeschlossenen Kunden einzieht. Der Netzbetreiber des angerufenen Mehrwertdiensteanbieters (MWDA) zahlt dann - möglicherweise über mehrere Stufen zwischengeschalteter Provider - den Erlös an den MWDA.

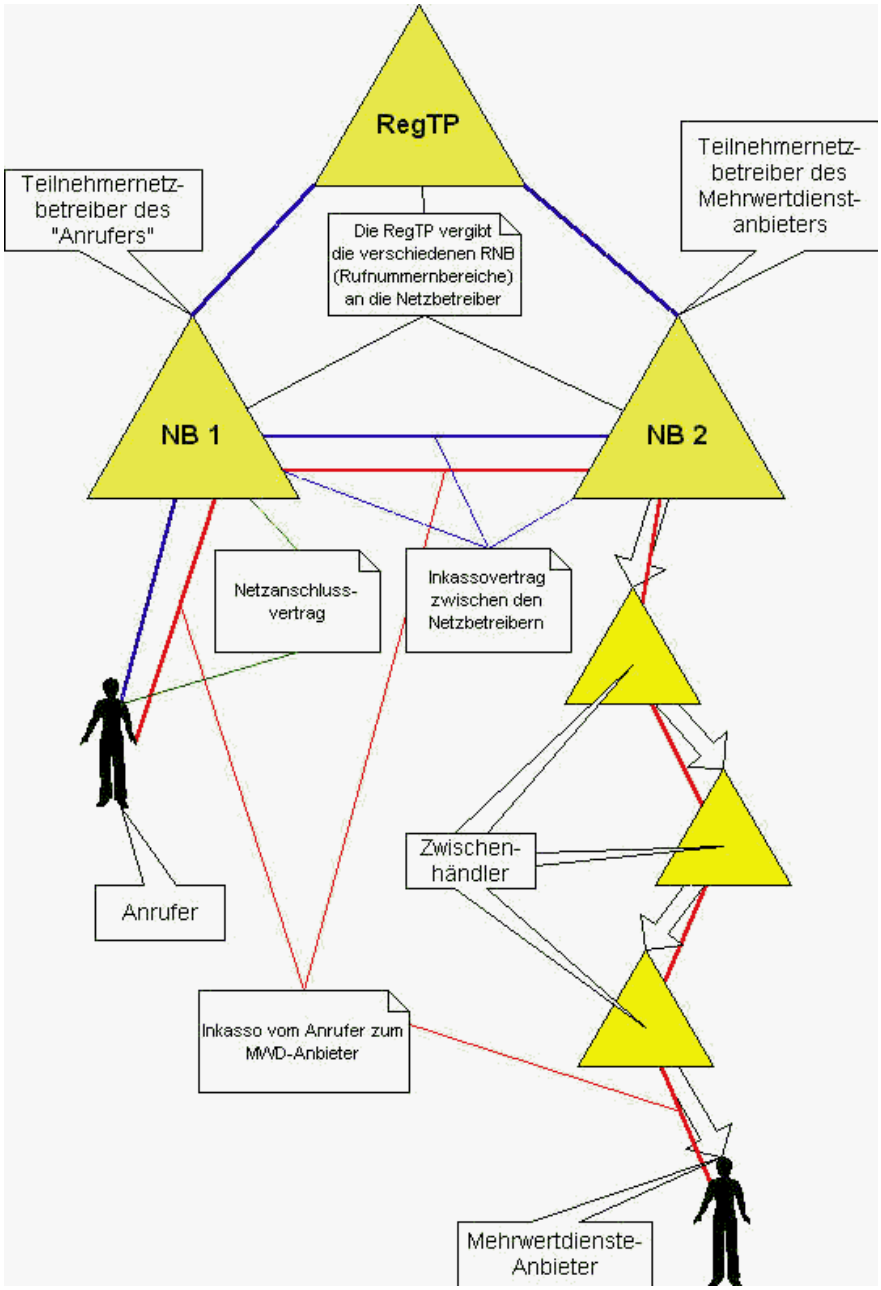
Der Tarif im einzelnen wird zwischen dem MWDA und seinem direkten Provider vereinbart, wobei es sich um den letzten aus einer ganzen Reihe von Zwischenhändlern handeln kann.

und Auskunftsdienste müssten weiterhin über die Telekom abgerechnet werden ...

Die Deutsche Telekom hatte 1998 mit anderen Netzbetreibern der Telekommunikation sogenannte Inkasso- und Fakturierungsverträge abgeschlossen, worin sie sich unter anderem verpflichtete, die von den Wettbewerbern erbrachten Leistungen in der Telekom-Rechnung auszuweisen, einzuziehen und Forderungen zu verfolgen (Mahnverfahren). Im April 2000 kündigte die Telekom den Vertrag für Mehrwertdienste (Internet-by-Call, 0180er oder 0190er Rufnummern) auf. Die Regulie-

TKR-Newsletter vom 08.12.02 (Auszug):

> VG Köln: Telekom muss Internet-by-Call-Leistungen fremder Anbieter nicht über Telefonrechnung abrechnen
>
> Die Deutsche Telekom ist nicht verpflichtet ist, Leistungen von Mehrwertdiensten (Internet-by-Call, 0180er und 0190er Rufnummern) anderer Netzanbieter über die Telekom-Rechnung abzurechnen, da die Entgelte für diese Leistungen nicht im Wesentlichen für Telefondienstleistungen erbracht werden. Mit dieser Begründung hat das Verwaltungsgericht Köln mit Urteil vom 14.11.2002 (Az. 1 K 2788/00) die Entscheidung der Regulierungsbehörde für Telekommunikation und Post (RegTP) insoweit aufgehoben, als die Telekom darin verpflichtet wurde, auch für diese Mehrdienstleistungen ihren vertraglichen Fakturierungs- und Inkassoverpflichtungen nachzukommen.
>
> Lediglich Call-by-Call Leistungen über 010xy-Rufnummern



rungsbehörde sah darin einen Missbrauch der marktbeherrschenden Stellung ...

Zwar sei gemäß § 33 Abs. 1 Satz 1 TKG die Telekom aufgrund ihrer marktbeherrschenden Stellung verpflichtet, Wettbewerbern diskriminierungsfrei den Zugang zu ihren intern genutzten und dem Markt angebotenen Leistungen zu ermöglichen, wobei der Zweck dieser Leistung auf die Erbringung gerade einer Telekommunikationsdienstleistung im Sinne des § 3 Nr. 16 TKG gerichtet sein müsse. Nach Auffassung der Kölner Richter lag letzteres im konkreten Fall nicht vor, so dass die Kammer einen Verstoß gegen § 33 TKG verneinte. Denn nach § 3 Nr. 16 TKG ist eine Telekommunikationsdienstleistung jeder "technische Vorgang zur Übermittlung von Nachrichten jeglicher Art". Bei den zeittaktabhängigen Mehrwertdiensten / Internet-by-Call ginge es aber gerade nicht allein um den technischen Vorgang ... Das Gesamtentgelt orientiere sich nicht an den Kosten einer effizienten Leistungsbereitstellung, sondern zu einem erheblichen Teil an dem Wert des übermittelten Leistungsinhalts. Dieses Ergebnis wird nach Auffassung der Richter auch durch die Änderungsverordnung zu § 13 a Satz 1 TKV (2. Änderungsverordnung vom 20.08.2002, BGBl. I 3365) bestätigt, worin der Verordnungsgeber die mit Mehrwertdiensterufnummern verbundenen "weiteren Dienstleistungen" nicht mit den Telekommunikationsdienstleistungen gleichsetzt.

Online-Strafrecht
Straftaten und Ordnungswidrigkeiten im besonderen Telekommunikations- und Multimediarecht

Wie auch das Wirtschaftsrecht verfügt das Telekommunikations- und Multimediarecht (kurz: TMR) über eine kleine Zahl besonderer Strafvorschriften und über eine Vielzahl von Bußgeldvorschriften, die über verschiedene Gesetze verstreut sind.

In solchen "strafrechtlichen Nebengesetzen" erfolgt häufig eine wechselseitige Bezugnahme zwischen förmlichen, also parlamentarisch beschlossenen Gesetzen und Rechtsverordnungen. Rechtsverordnungen müssen aufgrund einer gesetzlichen Ermächtigung erlassen werden. Wenn ein Zuwiderhandeln gegen die Anordnungen aufgrund einer Rechtsverordnung mit einer Strafe oder mit einem Bußgeld bedroht werden soll, so muss diese aus einer ausdrücklich in einem Gesetz aufgeführten Ermächtigung abgeleitet werden. Dies macht - vor Allem wegen der Bußgeldvorschriften - es nötig, die Verweise zwischen verschiedenen Normen nach zu vollziehen und zu verstehen, welche Regelungen schließlich sanktionsbewehrt sind welche nicht.

Überblick

Für das Telekommunikationsrecht stehen die Fragen der technischen Versorgung mit den neuen Medien im Vordergrund (Zugang, access). Seine Sanktionsnormen berühren deshalb vor Allem die technische Sicherheit der Informationstechnik (Netze, Endgeräte usw.), die Sicherheit der übertragenen Daten (Abhörsicherheit) und die Überwachung der Telekommunikation sowie den wettbewerbsrechtlichen Missbrauchsschutz.

Das Multimediarecht nimmt auf die Inhalte der neuen Medien Bezug (content) und greift besonders die Frage der Verantwortlichkeit für Inhalte, das Verbot strafbarer Inhalte, die klare Kennzeichnung des Anbieters von Leistungen und die Sicherheit des elektronischen Geschäftsverkehrs auf.

Dieser Aufsatz unternimmt eine Bestandsaufnahme, die im Wesentlichen die Strafnormen des TMR vorstellt. Dies geht in einigen Fällen nicht ohne dass auch eine Reihe von Ordnungswidrigkeitstatbestände (OWi) dokumentiert werden müssen, weil sich die betreffende Strafnorm unmittelbar an Bußgeldtatbestände anlehnt.

1. **Telekommunikationsrecht**

Das Telekommunikationsgesetz (TKG) hat wesentliche Teile des früheren Fernmeldeanlagengesetzes übernommen und neu geregelt. Es enthält deshalb auch verwaltungsstrafrechtliche Vorschriften im Zusammenhang mit Fernmeldeanlagen.

Die Strafvorschriften des TKG flankieren vor Allem den Schutz des Inhalts übermittelter, persönlicher Daten (Abhörschutz). Sie ergänzen die allgemeinen Straftatbestände zum Schutz des persönlichen Lebens- und Geheimbereichs im Strafgesetzbuch (StGB):

§ 201 Verletzung der Vertraulichkeit des Wortes

§ 202 Verletzung des Briefgeheimnisses

§ 202 a Ausspähen von Daten

§ 203 Verletzung von Privatgeheimnissen

§ 204 Verwertung fremder Geheimnisse

§ 205 Strafantrag

§ 206 Verletzung des Post- oder Fernmeldegeheimnisses

Anmerkung zu § 203 StGB:

Nach dem Urteil des Bundesgerichtshofes vom 08.10.02 - 1 StR 150/02 - sind z.B. auch Fahrzeug- und Halterdaten, die im Rahmen einer einfachen Registerauskunft nach § 39 Abs. 1 StVG übermittelt werden, nicht offenkundig und fallen damit unter den Schutz des § 203 Abs. 2 Satz 2 StGB.

...

2. **Multimediadiensterecht**

Das Recht der Multimediadienste ist gekennzeichnet durch schwierige Abgrenzungsfragen zwischen den Telediensten nach dem Gesetz über die Nutzung von Telediensten (Teledienstegesetz - TDG) und den Mediendiensten im Regelungsbereich des Staatsvertrages über Mediendienste (MDStV). Auf die Einzelheiten wird in Online-Strafrecht III unter Teledienste und Mediendienste eingegangen.

Für die Teledienste hat der Gesetzgeber keine Strafnormen geschaffen. ...

Die Straftaten und Ordnungswidrigkeiten im Mediendiensterecht werden von einer erweiterten Haftung der Zugangs- und Hostprovider einschließlich der Proxy-Dienste begleitet. Wegen der Tätigkeitsbereiche der Provider wird auf Provider und Netze und wegen der Einzelheiten der Haftungserweiterung auf die Ausführungen zur erweiterten Verantwortlichkeit der Zugangs- und Hostprovider nach dem MDStV 2002 verwiesen.

Die Strafnormen des Mediendiensterecht beschränken sich auf den Jugendschutz.

Jugendschutz im Mediendiensterecht

Die klassischen strafrechtlichen Vorschriften zum Schutz der Jugend vor Gewalt und sexuellem Missbrauch sowie gegen die Verbreitung jugendgefährdender Schriften befinden sich im Strafgesetzbuch (StGB - Straftaten gegen die sexuelle Selbstbestimmung):

§ 174 Sexueller Mißbrauch von Schutzbefohlenen

§ 176 Sexueller Mißbrauch von Kindern

§ 176 a Schwerer sexueller Mißbrauch von Kindern

§ 176 b Sexueller Mißbrauch von Kindern mit Todesfolge

§ 177 Sexuelle Nötigung; Vergewaltigung

§ 178 Sexuelle Nötigung und Vergewaltigung mit Todesfolge

§ 179 Sexueller Mißbrauch widerstandsunfähiger Personen

§ 180 Förderung sexueller Handlungen Minderjähriger

§ 180 a Förderung der Prostitution

§ 180 b Menschenhandel

§ 181 Schwerer Menschenhandel

§ 181 a Zuhälterei

§ 182 Sexueller Mißbrauch von Jugendlichen

§ 184 Verbreitung pornographischer Schriften

§ 184 a Ausübung der verbotenen Prostitution

§ 184 b Jugendgefährdende Prostitution

§ 184 c Begriffsbestimmungen

Heise-Meldung vom 31.07.02 (Auszug):

Spielen verboten: Berliner Polizei schließt Internet-Cafés

"... Der Hauptvorwurf gegen die beiden beanstanden Cafés lautet, das in solchen Internet-Cafés, in denen mehrere Computer zu lokalen Netzwerken zusammengeschlossen sind und in denen überwiegend die Teilnahme an Computerspielen angeboten wird, eher von einem Spielhallenbetrieb und kommerzieller Nutzung von Unterhaltungsspielen auszugehen sei als vom Betreiben eines Internet-Cafés, erklärte die Berliner Polizei.

Damit ist ein Verstoß gegen das Gesetz zum Schutze der Jugend in der Öffentlichkeit (JÖSchG) angesprochen. Nach diesem Gesetz darf Kindern und Jugendlichen die Anwesenheit in öffentlichen Spielhallen oder ähnlichen "vorwiegend dem Spielbetrieb dienenden Räumen" nicht gestatt werden. Ebenso darf das kostenpflichtige Spielen an "elektronischen Bildschirmen-Unterhaltungsspielgeräten ohne Gewinnmöglichkeit" Kindern und Jugendlichen unter 16 Jahren ohne Begleitung eines Erziehungsberechtigten nicht gestattet werden (§ 8 Abs. 1 und 4 JÖSchG). ..."

Beschluss des OVG Berlin vom 16.12.02 - 1 S 55.02 - (Leitsatz, Quelle: jurpc.de):

Ein multifunktionales Gerät wie ein Computer ist bereits dann von § 33 i Abs. 1 Satz 1 GewO erfasst, wenn es auch zu dem Zweck aufgestellt ist, als Unterhaltungsspiel genutzt zu werden. Lassen die Geräte zumindest überwiegend eine Nutzung als Unterhaltungsspiel zu, kommt es nicht darauf an, ob sie tatsächlich überwiegend zu diesem Zweck genutzt werden.

Jugendgefährdende Schriften

Von zentraler Bedeutung ist das Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte (Jugendmedienschutzgesetz - GjS, PDF-Datei), das wegen seiner allgemeinen Bedeutung für Print- und elektronische Medien nicht zum besonderen TMR zählt.

...

Jugendschutz im MDStV

Der Staatsvertrag über Mediendienste (MDStV) unterwirft die Verbreitung oder unzureichende Sperrung strafbarer, die Menschenwürde verletzender oder jugendgefährdender Inhalte durch Mediendienste-Anbieter sowie die Nichtbestellung eines Jugendschutzbeauftragten mit hohen Bußgelddrohungen ...

Das damit geschaffene Sanktionssystem wird von § 24a MDStV um eine Strafnorm ergänzt:

Mit einer Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer entgegen § 12 Abs. 1 Nr. 3 Mediendienste anbietet, die wegen ihrer offensichtlichen Eignung, Kinder oder

Jugendliche sittlich schwer zu gefährden, unzulässig sind. Handelt der Täter fahrlässig, so ist die Freiheitsstrafe bis zu sechs

Monate oder die Geldstrafe bis zu 180 Tagessätze.

Der davon in Bezug genommene § 12 Abs. 1 Nr. 3 MDStV lautet (Auszug):

(1) Angebote sind unzulässig, wenn sie ...

3. offensichtlich geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden ...

Jugendschutz im JMStV

Der Staatsvertrag über den Schutz der Menschenwürde und dem Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag - JMStV) wurde von den Ministerpräsidenten der Bundesländer im September 2002 unterzeichnet und der Niedersächsische Landtag hat zum Beispiel dem Staatsvertrag am 20.11.02 zugestimmt (Nds. GVBl. Nr. 31/2002, S. 705). Er enthält eine eigene Strafvorschrift und umfangreiche OWi-Vorschriften...

Ordnungswidrigkeiten im Telekommunikationsrecht

...

§ 96 TKG

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4 Satz 1 eine Anzeige nicht, nicht richtig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig erstattet,
2. entgegen § 5 einen Bericht nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zur Verfügung stellt,
3. ohne Lizenz nach § 6 Abs. 1 Übertragungswege betreibt oder Sprachtelefondienst anbietet,
4. entgegen § 14 Abs. 1 oder 2 Satz 1 Telekommunikationsdienstleistungen für die Öffentlichkeit nicht in rechtlich selbständigen Unternehmen führt oder die Nachvollziehbarkeit der finanziellen Beziehungen nicht oder nicht in der vorgeschriebenen Weise gewährleistet,
5. entgegen § 22 Abs. 1 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
6. ohne Genehmigung nach § 25 Abs. 1 ein Entgelt erhebt,
7. einer vollziehbaren Anordnung nach § 29 Abs. 2 Satz 2, auch in Verbindung mit § 30 Abs. 5 Satz 2, nach § 31 Abs. 1 Nr. 1, § 33 Abs. 2 Satz 1, auch in Verbindung mit § 38 Abs. 2, nach § 34 Abs. 1, § 43 Abs. 4 Satz 4, Abs. 5 Satz 1 oder Abs. 6 Satz 1, § 44 Abs. 2 oder § 49 Satz 2 zuwiderhandelt,
8. einer vollziehbaren Auflage nach § 32 zuwiderhandelt,
9. einer Rechtsverordnung nach § 35 Abs. 5 Satz 1, § 47 Abs. 4, § 59 Abs. 4 Satz 1, § 62 Abs. 1 Satz 1, § 63 Abs. 1 Satz 3, § 87 Abs. 3 Satz 1 oder 89 Abs. 1 Satz 1 oder einer vollziehbaren Anordnung auf Grund einer solchen Rechtsverordnung zuwiderhandelt, soweit die Rechtsverordnung für einen bestimmten Tatbestand auf diese Bußgeldvorschrift verweist,
10. ohne Frequenzzuteilung nach § 47 Abs. 1 Satz 1 Frequenzen nutzt,
11. entgegen § 60 Abs. 6 Satz 1 eine Ausfertigung der Erklärung über den Verwen-

dungszweck nicht oder nicht rechtzeitig übermittelt,

12. entgegen § 65 Abs. 3 für eine Sendeanlage wirbt,

13. entgegen § 88 Abs. 2 Satz 4 Nr. 1 in Verbindung mit einer Rechtsverordnung nach § 88 Abs. 2 Satz 2 Nr. 1 den Betrieb einer Telekommunikationsanlage aufnimmt,

14. entgegen § 88 Abs. 2 Satz 4 Nr. 2 oder 3 den Betrieb einer Telekommunikationsanlage aufnimmt,

14a. entgegen § 88 Abs. 2 Satz 6 eine Einrichtung nicht oder nicht rechtzeitig nachbessert,

15. entgegen § 88 Abs. 4 Satz 1 einen Netzzugang nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bereitstellt oder

16. entgegen § 90 Abs. 2 Satz 1 eine Kundendatei nicht oder nicht in der vorgeschriebenen Weise verfügbar hält, entgegen § 90 Abs. 5 Satz 2 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt, entgegen § 90 Abs. 2 Satz 2 Kenntnis von Abrufen nimmt oder entgegen § 90 Abs. 5 Satz 3 Stillschweigen nicht wahrt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nr. 3, 4, 6, 7, 8, 9, 10, 13 und 14a mit einer Geldbuße bis zu fünfhunderttausend Euro, in den Fällen des Absatzes 1 Nr. 1, 2, 5, 11, 12, 14, 15 und 16 mit einer Geldbuße bis zu zehntausend Euro geahndet werden. Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die Regulierungsbehörde.

Für alle Tatbestände des § 96 Abs. 1 TKG gilt: Die Regulierungsbehörde für Telekommunikation und Post (RegTP) ist die zuständige Verwaltungsbehörde für die Verfolgung von Ordnungswidrigkeiten nach dem TKG (§ 96 Abs. 2 TKG). Dabei handelt es sich um breit gefächerte Gesetzesziele, die sich nach der systematischen Aufzählung in § 96 Abs. 1 TKG (siehe oben) nicht sofort aufdrängen.

...

OWi-Tatbestände zur Sicherung der Auskunftspflichten gegenüber Strafverfolgungsorganen und anderen Behörden

Für die Praxis der Strafverfolgungsbehörden sind die §§ 89, 90 TKG besonders wichtig, weil sie die Pflichten der TK-Unternehmen zur Auskunft über Kundendaten und das automatische Abrufverfahren über einen Datenzugriff der RegTP regeln. Die Details sind in der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations- Überwachungsverordnung - TKÜV) vom 22.01.2002 bestimmt worden (die neue Fassung der Telekommunikations-Überwachungsverordnung (TKÜV) ist am 24.08.02 in Kraft getreten).. Außerdem bestimmen § 5 Satz 2 des Teledienstedatenschutzgesetzes (TDDSG) vom 22.07.1997 und § 19 Abs. 1, 6 des Staatsvertrages über Mediendienste (MDStV) ausdrücklich, dass Anbieter von Telediensten Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung erteilen dürfen.

Neben der oben genannten Verpflichtung des "erweiterten" Auskunftsverpflichteten zum Stillschweigen über die Tatsache und den Inhalt seiner Auskünfte stellt § 96 Abs. 1 TKG weitere Bußgeldtatbestände bereit, um die Überwachung der Telekommunikation zu sichern.

...

Ordnungswidrigkeiten im besonderen Multimediarecht

...

Teledienste und Mediendienste

Nach der Begriffsbestimmung des § 3 Nr. 16 Telekommunikationsgesetzes (TKG) ist die Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bilder oder Tönen mittels Telekommunikationsanlagen. Im Anschluss daran sind Telekommunikationsdienste (§ 3 Nr. 18 TKG) die gewerblichen Angebote von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte.

Wegen der Multimediadienste ist nach den Telediensten (Gesetzgebungskompetenz des Bundes) und den Mediendiensten (Kulturhoheit der Bundesländer) zu unterscheiden.

Teledienste sind nach § 2 Abs. 1 TDG elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Zur Abgrenzung bestimmt § 2 Abs. 4 Nr. 3 TDG, dass die inhaltlichen Angebote von Verteildiensten und Abrufdiensten dann Mediendienste sind, wenn ihre redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht.

Anhand dieser abstrakten Definitionen kann die Abgrenzung im Einzelfall äußerst schwierig werden. Auch die Anwendungsbeispiele, die das TDG und der Staatsvertrag über Mediendienste (MDStV) anführen, helfen nur bei der Zuordnung der ausdrücklich genannten Dienste.

Ausdrücklich journalistisch ausgerichtete Angebote (siehe z.B. die Links in der Sammlung Presse) dürften als Mediendienste und die katalogartigen Angebote von Amazon und anderen Kaufhäusern als Teledienste anzusehen sein. Ungeklärt bleibt aber die genaue Zuordnung "normaler" Internet-Websites, z.B. des EDV-Workshops. Er übermittelt vor Allem Text-, aber auch Ton- oder Bilddarbietungen auf Anforderung und richtet sich an die Öffentlichkeit mit dem Ziel der Informationsvermittlung, also der Meinungsbildung. Demzufolge müsste er ein Mediendienst sein. Ob dabei jedoch die redaktionelle Gestaltung zur Meinungsbildung der Allgemeinheit (dann Mediendienst) oder der Datenaustausch (dann Teledienst) im Vordergrund steht, ist eine unsichere Bewertungsfrage (siehe auch Provider und Netze).

Teledienste nach § 2 Abs. 2 bis 4 TDG sind	**Mediendienste nach § 2 Abs. 2 MDStV sind**
Individualkommunikation wie Telebanking und Datenaustausch	
Informations- und Kommunikationsangebote, bei denen nicht die redaktionelle Gestaltung zur Meinungsbildung der Allgemeinheit im Vordergrund steht	Verteildienste in Form von Fernsehtext, Radiotext und vergleichbaren Textdiensten
wie Verkehrs-, Wetter-, Umwelt- und Börsendaten und	Verteildienste, in denen Messergebnisse und Datenermittlungen in Text oder Bild mit oder ohne Begleitton verbreitet werden
Informationen über Waren und Dienstleistungen	Abrufdienste, bei denen Text-, Ton- oder Bilddarbietungen auf Anforderung aus elektronischen Speichern zur Nutzung übermittelt werden, mit Ausnahme von solchen Diensten, bei denen der individuelle Leistungsaustausch oder die reine Übermittlung von Daten im Vordergrund steht
Angebote zur Nutzung des Internets oder anderer Netze	
Telespiele	
Angebote von Waren- und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit	Verteildienste in Form von direkten Angeboten an die Öffentlichkeit für den Absatz von Waren oder Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, gegen Entgelt (Teleshopping)
	vergleichbar **Rundfunk**

Einen sehr interessanten und brauchbaren Ansatz hat Marco Gercke für die Abgrenzung zwischen Tele- und Multimediadienste vorgeschlagen (Lexikon-Beitrag). Er unterscheidet danach, ob eine Datenübermittlung auf Initiative des Anbieters (push, stoßen, drücken) oder des Nutzers erfolgt (pull, ziehen, zerren). Danach weist er die wesentlichen Dienste im Internet grundsätzlich folgenden Regelwerken zu:

Homepage - TDG
Newsgroups ohne Moderation - TDG
Newsgroups mit Moderation - MDStV
Internet Relay Chat - MDStV
Email - TDG

Auch mit Christos Paloubis, IuKDG und Mediendienste-Staatsvertrag, sind einige Zweifel angebracht, ob sich tatsächlich straf- oder ordnungswidrigkeitenrechtliche Sanktionen gegen Hosting-Provider und Onlinedienste aus den geltenden OWi-Vorschriften ableiten lassen (siehe unten: Sperrung von Inhalten. Kontroverse um Provider-Pflichten)

Hier ein Auszug aus dem Text, der sich noch mit der älteren Fassung des MDStV befasst (zur Erläuterung: wenn Paloubis vom Informations- und Kommunikationsdienstegesetz spricht, so umfasst das vor Allem auch das Teledienstegesetz).

" Mediendienste

Nach § 2 I MDStV sind Mediendienste an die Allgemeinheit gerichtete Angebote von Informations- und Kommunikationsdiensten in Text, Ton oder Bild, die unter Benutzung elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters verbreitet werden.

Auch hier erfolgt eine beispielhafte Aufklärung in Absatz 2, was unter der Formulierung des Absatz 1 zu verstehen ist.

Fernseheinkauf

Verteildienste in denen Messergebnisse und Datenermittlungen in Text oder Bild mit oder ohne Begleitton verbreitet werden Verteildienste in Form von Fernsehtext, Radiotext und vergleichbaren Textdiensten und Abrufdienste, bei denen Text-, Ton- oder Bilddarbietungen auf Anforderung aus elektronischen Speichern zur Nutzung übermittelt werden mit Ausnahme solcher Dienste, bei denen der individuelle Leistungsaustausch oder die reine Übermittlung von Daten im Vordergrund stehen.

Die Abgrenzung der beiden Normen für Dienste, die nicht zu den aufgeführten Beispielen gehören ist denkbar unklar. ...

Mit dem Mediendienste-Staatsvertrag ist der BTX-Staatsvertrag gemäß § 23 III MDStV außer Kraft getreten, da der Bereich des Bildschirmtextes durch den neuen Mediendienste-Staatsvertrag ersetzt werden soll. Für viele Anbieter von BTX-Seiten ist nun unklar, ob Ihre Angebote nicht vom IuKDG erfasst werden, insbesondere, wenn sie die gleichen Angebote im Bildschirmtext, wie auch im WWW haben.

Einziges erhebliches Kriterium scheint im IuKDG die Formulierung "für eine individuelle Nutzung" und im MDStV "an die Allgemeinheit gerichtete Angebote" zu sein.

Zum typischen Internetangebot, welches diese Gesetze ja regeln wollen, gehören jedoch in der Regel beide Merkmale. Homepages richten sich an die Allgemeinheit, der Seitenabruf erfolgt aber individuell durch den User. ...

Zu beachten ist hierbei, dass die Regelungen die Inhalte der Angebote zu erfassen angelegt sind. Nach den oben genannten Kriterien kann eine Unterscheidung aber nur schwerlich an den Inhalten erfolgen.

Nach der Formulierung ist eher denkbar, dass die Ausrichtung auf die Zielgruppe das Unterscheidungskriterium sein könnte. In der Praxis wird diese aber kaum zu ermitteln sein.

Eine Unterscheidung nach technischen Aspekten entfällt ebenfalls. Beide Gesetze sehen die gleiche Art der Übermittlung von Daten vor. Zudem wäre dies wohl ein Bereich des Telekommunikationsrechtes, das aber von den Multimediagesetzen streng zu trennen ist.

Einen kleinen Hinweis enthält die Begründung zum Mediendienste-Staatsvertrag. Hier sollen die in der Aufzählung des Absatz 2 genannten Verteildienste dadurch gekennzeichnet sein, dass "der Zeitpunkt der Ausstrahlung von Anbieter einseitig festgelegt wird". Aber auch hier wird wieder auf den technischen Aspekt abgestellt. Ob ein typisches Internetangebot hier erfasst werden soll, bleibt unklar.

Eine Unterscheidung nach der Bezeichnung des Anbieters ist schließlich auch nicht geboten. Oftmals vermischen sich die Leistungsangebote von einzelnen Providern. Der typische Content-Provider ist zwar häufig anzutreffen, wenn eine reine Beschränkung auf die Anmietung von Festplattenspeicher bei einem Netzwerk- oder Serviceprovider vorliegt. Ein reiner Access-Provider, der nur den Zugang zum Internet anbietet ist aber die Ausnahme. In der Praxis werden vielmehr Komplettlösungen angeboten, die sowohl den Zugang, als auch einen eMail-Service oder

auch Festplattenspeicher für die eigene Homepage, beinhalten.

Einziger Anhaltspunkt bleiben wohl die Aufzählungen in den jeweiligen Absätzen 2, sowie die Ausnahme, dass solche Dienste, bei denen der individuelle Leistungsaustausch oder die reine Übermittlung von Daten im Vordergrund steht, nicht unter den Begriff Mediendienste zu fassen sei. Damit unterliegt das typische Internetangebot wohl dem IuKDG.

Verantwortlichkeit (TDG / MDStV)

Der ausgewiesene Zweck des Gesetzes über die Nutzung von Telediensten (Teledienstegesetz - TDG) vom 22.07.1997 ist es "einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kornmunikationsdienste zu schaffen" (§ 1 TDG).

Wegen der Abgrenzung zwischen verschiedenen Provider-Tätigkeiten wird auf den Aufsatz Provider und Netze Bezug genommen.

Die Regelung der Verantwortlichkeit für die Inhalte von Teledienste ist im TDG seit dem 14.12.2001 neu gefasst worden. Die Vorschriften des mit Wirkung vom 01.07.2002 neu gefassten Staatsvertrages über Mediendienste (MDStV) sind wortgleich. Zu beachten ist jedoch, dass § 22 Abs. 3 MDStV eine Verantwortlichkeit der Zugangs- und Host-Provider einschließlich der Proxy-Dienste für die Fälle postuliert, dass eine von der Aufsichtsbehörde betriebene Sperrung rechtswidriger Inhalte nicht gegen den Inhaltsprovider durchgesetzt werden kann oder nicht erfolgversprechend ist.

§ 8 TDG [Allgemeine Grundsätze]

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter im Sinne der §§ 9 bis 11 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 9 bis 11 unberührt. Das Fernmeldegeheimnis nach § 85 des Telekommunikationsgesetzes ist zu wahren.

§ 9 TDG [Durchleitung von Informationen]

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

die Übermittlung nicht veranlasst,

den Adressaten der übermittelten Informationen nicht ausgewählt und

die übermittelten Informationen nicht ausgewählt oder verändert haben.

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die au-

tomatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

§ 10 TDG [Zwischenspeicherung zur beschleunigten Übermittlung von Informationen]

Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung der fremden Information an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie

die Informationen nicht verändern,

die Bedingungen für den Zugang zu den Informationen beachten,

die Regeln für die Aktualisierung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,

die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und

unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

§ 9 Abs. 1 Satz 2 gilt entsprechend.

§ 11 TDG [Speicherung von Informationen]

Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern nicht verantwortlich, sofern

sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder

sie unverzüglich tätig geworden sind, um die Information zu entfernen, oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.

Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Sperrung von Inhalten. Kontroverse um Provider-Pflichten

Über die Verantwortlichkeit von Zugangs- und Hostprovider (siehe Aufsatz Provider und Netze) für die von ihnen bereit gestellten und übermittelten Inhalte hat es seit August 2000 heftige Kontroversen gegeben, weil in Nordrhein-Westfalen die Bezirksregierung Düsseldorf von Providern unter Bußgeldandrohung die Sperrung von gewaltverherrlichenden, rechtsextremen Internetangeboten verlangt wurde.

Beschluss des VG Düsseldorf vom 19.12.02 - 15 L 4148/02 - (Leitsatz, Quelle: jurpc.de):

> 1. Bei der gebotenen summarischen Prüfung im Rahmen des Verfahrens des vorläufigen Rechtsschutzes ist ein offensichtlicher Rechtsfehler der Sperrungsverfügung gegen rechtsextreme Internet-Inhalte nicht zu erkennen und es sind auch keine Gründe ersichtlich, das Suspensivinteresse der Access-Provider höher zu bewerten als das besondere Interesse an der sofortigen Vollziehung der Entscheidung.
>
> 2. Die Access-Provider sind entweder Mediendiensteanbieter i.S.d. § 3 Nr. 1 MDStV 2002 oder Telediensteanbieter i.S.d. § 3 Nr. 1 TDG 2001, nicht aber Telekommunikationsdienstleister i.S.d. § 4 TKG, so dass für Sperrungsverfügungen gegenüber den Access-Providern, die den Zugang zu inhaltlichen Angeboten vermitteln, das TKG nicht herangezogen werden kann.

Aus remus-Newsletter 14/2001 vom 20.12.2001:

> "Im Bundesgesetzblatt 2001 Teil 1 Nr. 70 vom 20.12.2001 ist auf den Seiten 3721 bis 3727 das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz - EGG) vom 14.12.2001 veröffentlicht. ... Die Änderungen des Teledienstegesetzes durch Art. 1, ... die Änderungen des Teledienstedatenschutzgesetzes durch Art. 3 treten gemäß Art. 5 S. 1 am Tag nach der Verkündung - folglich am 21.12.2001 - in Kraft.
>
> ... Zu den wichtigen Änderungen des Teledienstegesetzes gehört zunächst die Neuregelung der Verantwortlichkeit der Diensteanbieter (§§ 8ff. TDG). Von großer Bedeutung ist des weiteren die Einführung des Herkunftslandprinzips (§ 4 Abs. 1 TDG), von dessen Anwendungsbereich der gewerbliche Rechtsschutz und das Urheberrecht allerdings ausdrücklich ausgenommen sind (§ 4 Abs. 4 Nr. 6 TDG).
>
> Zu beachten ist schließlich die Verschärfung der Pflicht zur Anbieterkennzeichnung (§ 6 TDG). Wie bereits bislang im Anwendungsbereich des Mediendienste-Staatsvertrages (MDStV), aber im Unterschied zur früheren Rechtslage nach dem TDG stellt ein Verstoß gegen diese Pflichten nunmehr eine Ordnungswidrigkeit dar (§ 12 TDG).
>
> Diensteanbieter können sich künftig nicht mehr darauf beschränken, nur Name und Anschrift (sowie gegebenenfalls den Vertretungsberechtigten) anzugeben (§ 6 S. 1 Nr. 1 TDG). Erforderlich sind nunmehr auch die Angabe einer E-Mail-Adresse und einer Telefonnummer ("Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post" (§ 6 S. 1 Nr. 2 TDG)).
>
> Soweit der Teledienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, sind Angaben zu der zuständigen Aufsichtsbehörde erforderlich (§ 6 S. 1 Nr. 3 TDG); eine solche Aufsichtsbehörde stellt im Bildungsbereich die Staatliche Zentralstelle für Fernunterricht (ZFU) dar (URL: zfu.de). Insbesondere für privatrechtlich organisierte Einrichtungen aus Forschung, Lehre und Weiterbildung sind des weiteren die Pflichten zur Angabe der Registernummer (§ 6

S. 1 Nr. 4 TDG) und zur Umsatzsteueridentifikationsnummer (§ 6 S. 1 Nr. 6 TDG) von Bedeutung."

Wegen neuer Regelungsintiativen siehe Lexikon-Beitrag zum Gesetz zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern.

Erweiterte Verantwortlichkeit der Zugangs- und Hostprovider nach dem MDStV 2002

Für die Mediendienste hat der Staatsvertrag über Mediendienste (MDStV) in seiner Geltung seit dem 01.07.2002 eine erweiterte Providerhaftung eingeführt. Hierdurch wird der Zugang der Aufsichtsbehörden (Landesbehörden) zu allen Mediendiensten sichergestellt und verwaltungsrechtliche Anordnungen gegen Zugangs- und Hostprovider einschließlich Proxy-Dienste ermöglicht. Mit den Bußgeldtatbeständen gemäß § 24 Abs. 1 Nr. 15 und 16 MDStV werden Sanktionen eingeführt.

...

Strafbare Inhalte und Jugendschutz in Mediendiensten

Der Staatsvertrag über den Schutz der Menschenwürde und dem Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag - JMStV) wurde von den Ministerpräsidenten der Bundesländer im September 2002 unterzeichnet und der Niedersächsische Landtag hat zum Beispiel dem Staatsvertrag am 20.11.02 zugestimmt (Nds. GVBl. Nr. 31/2002, S. 705). Er enthält u.a. eine eigene Strafvorschrift, die oben (Jugendschutz im JMStV) vorgestellt wird.

Daneben enthält § 24 JMStV umfangreiche OWi-Vorschriften. Bußgeldbehörde ist die nach Landesrecht zuständige Landesmedienanstalt (Abs. 4). In Niedersachsen ist das die "Niedersächsische Landesmedienanstalt (NLM), Seelhorststraße 18, D-30175 Hannover (Tel.: 0511 - 28477-0, Fax: 0511 - 28477-36; eMail: info.nlm@t-online.de).

Teil 3: Anhang

Urheberschutz - Software - Internet

Links und Stellungnahmen. Eine Materialsammlung

(Auszug)

Mit der massenhaften Nutzung des Internets als Softwarequelle und der Möglichkeit, große Datenmengen mittels CD-Brenner bequem zu vervielfältigen, haben die Fragen danach, welche Daten zulässigerweise vervielfältigt werden dürfen, eine neue Brisanz erfahren.

Diese Zusammenstellung mit Texten aus dem Internet und eigenen Kommentaren soll einen Einstieg in das Thema ermöglichen.

1. **Einführende Texte**

...

2. **Was ist eine Raubkopie?**

Im Ergebnis ist eine Raubkopie jede vom Urheber nicht gestattete Vervielfältigung durch eine teilweise oder vollständige Kopie des Programmcodes - unabhängig vom Datenmedium (Band, Diskette, Festplatte, CD-R usw.) und unabhängig davon, ob eine dauerhafte oder nur temporäre Kopie erstellt wird.

Das Laden eines Programms in den Arbeitsspeicher ist nach herrschender Meinung bereits ein urheberrechtlicher Vorgang. Sie beruft sich darauf, dass das Urheberrecht dauerhafte und vorübergehende, temporäre Kopien gleich behandelt. Diese Meinung ist nicht unbestritten.

Die Kopie auf einem magnetischen oder anderem wiederbeschreibbaren Datenspeicher ist möglicherweise auch nur eine vorübergehende Kopie. Aufgrund der Entscheidung des Anwenders kann die Kopie wieder gelöscht oder überschrieben werden.

Der Kopiervorgang in den Arbeitsspeicher ist hingegen kein bewusster Vorgang des Anwenders, sondern gehört zum Programmbetrieb und wird von dem gestarteten Programm initiiert. Somit liegt die Überlegung nahe, mit der Betriebssytem-Entscheidung des BGH auch den Kopiervorgang in den Arbeitsspeicher - wie die Ausgabe auf den Bildschirm - als eine reine und erlaubte Nutzung des Programms anzusehen.

Von zentraler Bedeutung sind nach der Strafvorschrift des § 106 i.V.m. §§ 69c ff. UrhG die Akte der Vervielfältigung und der Verbreitung. Letztere setzt in aller Regel aber eine Vervielfältigung voraus, so dass die Alltagsprobleme am Begriff der Vervielfältigung entstehen:

Der schlichte Besitz einer Raubkopie ist straffrei. Der berechtigte Urheber kann aber zivilrechtlich die Herausgabe oder Vernichtung verlangen.

Unzulässig - auch in strafrechtlicher Hinsicht - wäre aber die Verwendung der Raubkopie, d.h. die Installation eines Programms ohne die Erlaubnis des Urhebers. Die Erlaubnis muss im Zusammenhang mit dem Kaufvertrag erteilt oder im Nachhinein vereinbart werden. Es kommt also nicht darauf an, dass man im Besitz eines Original-Datenträgers ist, also in aller Regel eine CD hat, sondern darauf, wie viele nutzbare Programminstallationen man davon herstellen darf. In aller Regel darf man das Programm

nur einmal installieren (z.B. im gewerblichen Bereich gibt es auch Verträge über eine Mehrzahl von Lizenzen). Will man es auf einem anderen Rechner nutzen, muss man die alte Installation zuerst löschen. Dies gilt auch dann, wenn man ein Programm verkaufen oder verschenken will.

Frank Möcke, Dr. M. Michael König in c't 16/01, S. 170, 171:

> Übertragungsprobleme. Urheberrechtliche Forderungen in Lizenzverträgen.
>
> "... In der bekannten und in der rechtswissenschaftlichen Literatur mit viel Engagement kommentierten 'Betriebssystem'-Entscheidung aus dem Jahr 1990 hat" der BGH "ausdrücklich festgestellt, dass allein die Ausgabe auf den Bildschirm als maßgebliche Vervielfältigungshandlung ausscheide, da hierbei keine körperliche Festlegung und Wiedergabe erfolge. Ferner falle die reine Benutzung des Programms aus dem Bereich des Urheberrechts heraus, da auch die Benutzung eines anderen Werkes - zum Beispiel das Lesen eines Buches - keinen urheberrechtlich relevanten Vorgang darstelle. ..."

Vorsicht ist bei der gleichzeitigen Verwendung eines PCs und eines Laptops geboten! Viele Programmhersteller lassen inzwischen die gleichzeitige Nutzung auf beiden Geräten zu. Ist dies nicht der Fall, müssen mehrere Programmlizenzen gekauft werden.

Eine Sicherungskopie vom Originaldatenträger ist vom Gesetz ausdrücklich zugelassen worden. Dies gilt auch für OEM-Versionen: Wer seinen Computer "vorinstalliert" und ohne die erforderlichen Datenträger erhalten hat, darf sich selbstverständlich davon eine Sicherungskopie (auf CD-R, Sicherungsband oder wie auch immer) herstellen.

Drei Problembereiche sind ungeklärt:

a) **OEM-Praxis 1:** Viele Verkäufer kopieren z.B. den Inhalt der Windows-CD auf die Festplatte, installieren das Betriebssystem usw. von dort aus und legen den Original-Datenträger (meist ungeöffnet) dem Gerät bei.

Streng genommen hat der Käufer das Windows-Programm dann dreimal erhalten: auf CD, davon eine Kopie auf Festplatte und schließlich das installierte Programm mit allen Feinheiten der erforderlichen Anpassung. Und in strenger Anwendung des Gesetzes hätte die Vervielfältigung des CD-Inhalts auf die Festplatte nicht erfolgen dürfen.

Bislang ist (noch) kein Strafverfolger auf die Idee gekommen, wegen solcher Vorinstallationen Ermittlungen einzuleiten. Und in der Tat meine ich, dass eine Strafverfolgung aus Rechtsgründen ausgeschlossen ist. Der Käufer erwirbt nämlich zusammen mit dem körperlichen Gegenstand des Datenträgers auch den Anspruch auf das fehlerfreie Funktionieren des Programms und das heißt, dass das Programm in seiner installierten Form das wesentliche Käuferinteresse darstellt. Die CD-Kopie auf der Festplatte ist nur zur Installation, aber nicht als Anwenderprogramm nutzbar.

Muss ich deshalb z.B. die Windows-Kopie auf meinem Rechner löschen, wenn die Programminstallation erfolgreich abgeschlossen ist? Ich meine nein. Windows 9.. z.B. speichert die Laufwerks- und Dateiverzeichnisnamen, von denen aus die Installation stattgefunden hat. Manche Löschvorgänge und Ergänzungsinstallationen sind nur möglich, wenn man auf das Installationsprogramm zurückgreift, wobei die Win-

dows-Routinen aber nicht in jedem Fall das Wechseln der Dateiverzeichnisse zulassen. Eine Abhilfe kann nur der schaffen, der gute Vorkenntnisse hat und in den Tiefen der Registrierung oder in Ini-Dateien die Pfadangaben verändert. Eine Löschung ist somit unzumutbar.

OEM-Praxis 2:

Darf ich OEM-Versionen, die ich mit einem Rechner oder anderen Hardware-Teilen gekauft habe, statt mit diesen Geräten auch auf anderen Rechnern verwenden?

Nach der von US-amerikanischen Rechtsvorstellungen geprägten Meinung vieler Großhersteller soll eine Lizenzbindung eintreten, so dass dies nicht erlaubt wäre. In den USA besteht die Auffassung, dass Software nicht gekauft, sondern nur gemietet oder gepachtet wird und die Verwendungsmöglichkeiten deshalb eingeschränkt werden können.

In Deutschland gilt aber für Software - in aller Regel - deutsches Kaufrecht. Insoweit lassen sich zwar zwischen Hersteller und Großhändler individualvertragliche Einzelregelungen treffen. Diese haben aber keine automatische Wirkung auf die Vertragsverhältnisse zwischen dem Einzelhändler und dem Endverbraucher.

Dies ist inzwischen vom Bundesgerichtshof bestätigt worden (Entscheidung vom 06.07.2000 - I ZR 244/97 -, veröffentlicht bei jurpc), wobei der BGH allein die Frage zu entscheiden hatte, ob sich aus dem Urheberrecht eine "Fernwirkung" entsprechend den üblichen OEM-Regeln ergeben kann:

Der BGH hat Vertragsklauseln zwischen Programmherstellern und Zwischenhändlern für unwirksam erklärt, in denen die Anbindung von OEM-Software an bestimmte Hardware-Produkte verlangt wird.

OEM-Software ist somit auch "unverkoppelt", also eigenständig verkaufbar.

Verlangt wird vom BGH, dass dieselbe, also funktionsgleiche Software mit nachvollziehbaren Preisspannen an den Endverbraucher verkauft werden können muss.

Zwischen einzeln-verkäuflichen und OEM-Versionen (mit demselben Funktionsumfang) besteht danach kein Unterschied.

Bestehen hingegen Funktionsunterschiede - z.B. zwischen Einzelplatz-ausgerichteten und Mehrplatz-ausgerichteten Versionen (z.B. zwischen Windows 98 und Windows NT) -, so können Preisunterschiede von 100 % durchaus gerechtfertigt sein.

b) **Backups:** Zur urheberrechtlichen Beurteilung schweigen offenbar alle Propheten. Zumindest beim Voll-Backup und teilweise auch beim Differenz-Backup vervielfältige ich urheberrechtlich geschützte Programme und Programmteile.

Die "Regeln der Kunst" für den EDV-Bereich verlangen hingegen regelmäßige Datensicherungen. Auch die Zivilrechtsprechung sieht ein Mitverschulden darin, wenn die Datensicherung sensibler Daten unterblieben ist. "Sensible", "weniger sensible" und "unsensible" Daten lassen sich in der Praxis mit angemessenem Aufwand nicht voneinander trennen. Eine solche Trennung müsste etwa so aussehen, dass ich eine Microsoft-exe nicht kopieren dürfte und z.B. eine ini-Datei nur dann, wenn an ihr im Programmbetrieb Änderungen vorgenommen wurden.

Dies zu fordern wäre Quatsch - um es deutlich zu sagen.

Backups sind technisch erforderliche, den reibungslosen Betrieb von Programmen sicherstellende Maßnahmen, die deshalb nicht ausdrücklich, sondern unmittelbar und stillschweigend im Umfang der Lizenz enthalten sein müssen, weil anderenfalls der Programm-Urheber selber keine "kunstgerechte" Laufsicherheit garantieren könnte [108].

c) **Zwischenspeicherung, Caches:** Dieses Problem wird am heftigsten im Zusammenhang mit kinderpornographischen Dateien diskutiert. Alle Standard-Browser speichern die heruntergeladenen Dateien in einen Zwischenspeicher - automatisch und unabhängig vom Willen des Anwenders. Dies können strafbare Inhalte sein, aber auch urheberrechtlich geschützte Programmbestandteile (zum Beispiel Bilder von Autos, Markenzeichen in grafischer Form).

Meines Erachtens sind alle Inhalte in Zwischenspeichern strafrechtlich unbedeutsam, solange der Anwender keine nachweisbare Kenntnis von ihrem Inhalt an dieser Stelle genommen hat.

Selbst Fahrlässigkeit verlangt die Kenntnis von den die Fahrlässigkeit begründenden Umständen. Der Gesetzgeber hat im Sachenrecht eine ganz weise Entscheidung getroffen, indem er z.B. die Begründung eines Besitzverhältnisses von einem "natürlichen" Besitzerwerbswillen abhängig macht. Diesen Besitzerwerbswillen kann man anschaulich mit dem Verhalten von Kleinkindern deutlich machen: Sie greifen nach einem Gegenstand und sagen dabei vielleicht sogar "haben". Genau das ist, auch wenn es banal klingt, Besitzerwerbswillen.

Was ich hingegen nicht wahrnehme, erwerbe ich auch nicht. Übertragen auf die Zwischenspeicherung heißt das: Wenn ich nichts von der Qualität zwischengespeicherter Daten weiß, dann kann ich auch nicht in die Urheberrechte anderer verletzend eingreifen.

In diese Richtung ist auch das Teledienstegesetz (§§ 9 Abs. 2, 11 S. 1 TDG) gegangen, indem es die vorübergehende Zwischenspeicherung von Proxy-Servern der reinen Verschaffung fremder Inhalte gleichgestellt hat. Doch halt: Vorübergehend. In der Begründung des Gesetzes steht dazu ausdrücklich: d.h. stundenweise und niemals über einen Tag hinaus. Für den Privatbereich kann diese enge Begrenzung keine Auswirkung haben, weil der PC des Privatanwenders kein Teledienst ist.

3. **Public Domain, Freeware, Shareware**

Public-Domain-Programme sind frei. Alle open-source- und Freeware-Programme sind nach dem ausdrücklichen Willen ihrer Urheber zur freien Verwendung und Vervielfältigung freigegeben. Der Verkauf, auch des abgeänderten Quellcodes, ist in aller Regel untersagt, nicht jedoch - je nach Gestaltung - die ungeänderte oder veränderte Weitergabe (siehe auch: Was ist Freie Software?).

Gilt das auch für Shareware?

Meine ursprünglich geäußerte Meinung, dass die unbefugte Verwendung von Sha-

[108] Siehe auch Kai Mielke, Fachmann zum Ausbauen gesucht. Haftung für Datenverlust und Pflicht zur Datensicherung, c't 24/2002, S. 194 f.

reware keiner Strafbarkeit unterliegt, muss ich angesichts der überzeugenden Ausführungen von Kai Mielke [109] aufgeben.

Mielke argumentiert (auszugsweise):

> "Wer ein Programm - auch ein Shareware-Programm - nutzen will, braucht dazu grundsätzlich eine Erlaubnis des Urhebers, Von dessen Willen hängen Art und Umfang der erlaubten Nutzung in erster Linie ab. ...
>
> Einschränkungen von Shareware-Versionen gegenüber den jeweiligen Vollversionen betreffen oft den möglichen Nutzungszeitraum, aber auch die Art der Nutzung und den Funktionsumfang. Wenn solche Einschränkungen nicht technisch eingebaut, sondern nur über die Nutzungsbedingungen verordnet sind, wird es kompliziert: Darf man beispielsweise die unregistrierte Version eines Programms nur am Einzelplatz, die registrierte aber auch im Netzwerk nutzen, so würde ein Netzadmin, der die unregistrierte Fassung auf dem Server einrichtet, das Urheberrecht verletzen und sich damit strafbar machen, Das hat nichts mit einem eventuell bestehenden Vertragsverhältnis zwischen ihm und dem Programmentwickler zu tun, sondern damit, dass die vom Urheber verfügte und vom Anwender in den Wind geschlagene Einschränkung eine eigenständige Nutzungsart betrifft. ...
>
> Free- und Shareware-Autoren räumen typischerweise jedem Besitzer einer Programmkopie beziehungsweise Testversion das Recht zur Weiterverbreitung im Sinne der § 69c Nr. 3, 15 Abs. 1 Nr. 2 und 17 UrhG ein. Übliche Einschränkungen, die von vornherein an die Verbreitung oder Nutzung solcher Programme geknüpft werden, wie etwa die Weitergabe nur in vollständiger Form oder das Verbot einer Netzwerknutzung, sind dabei grundsätzlich rechtswirksam. ...
>
> Auch die Bedingung, dass man ein Shareware-Programm ob technisch eingeschränkt oder nicht - ohne Registrierung nur zu Testzwecken nutzen darf, entfaltet urheberrechtliche Wirkung. Nach herrschender juristischer Ansicht gibt es zwar keine feste Antwort auf die Frage, wie lang sich ein angemessener Testzeitraum hinziehen darf, aber in jedem Einzelfall wird es einen Zeitpunkt geben, nach dem man von einer missbräuchlich ausgedehnten Testphase sprechen kann. Obgleich es im Wesentlichen vom Anwender abhängt, wie intensiv und wann er testet, nennt die juristische Standardliteratur als Anhaltspunkt eine Zeitspanne von 30 Tagen. ...
>
> Der Missbrauch von Shareware - entweder als Verstoß gegen das Urheberrecht oder als nicht vertragsgemäße Nutzung - kann auf unterschiedliche Art geahndet werden: Verstößt der Anwender beispielsweise gegen eine wirksam vereinbarte Nutzungsbedingung, so macht er sich dem Programmentwickler gegenüber schadenersatzpflichtig. Die Verletzung von Urheberrechten kann Schadenersatz und Unterlassungsansprüche auslösen (§ 97 UrhG), und zwar nicht nur gegen den Anwendet selbst, sondern gegen jede Person, die das Urheberrecht verletzt - also etwa auch jemanden, der im Web spezielle Knackwerkzeuge bereitstellt, die ein Anwender passender Shareware-Programme zur Herstellung von Raub-Vollversionen nutzt. Daneben kommt auch ein Anspruch auf Vernichtung oder Überlassung aller urhe-

[109] Herr im selbst programmierten Haus. Kleiner juristischer Rundschlag für Shareware-Programmierer, c't 20/02, S. 198 f.

berrechtswidrig hergestellten oder verbreiteten Vervielfältigungsstücke in Betracht (§ 98 UrhG).

Schließlich gibt es im urheberrechtlich relevanten Bereich auch verschiedene Strafvorschriften (§§ 106-108a UrhG), deren Strafrahmen jeweils bis zu drei Jahren reicht. Auch allgemeine Straftatbestände wie das 'Ausspähen von Daten' (§ 202a StGB), 'Datenveränderung' (§ 303a StGB) oder 'Computerbetrug' (§ 263a StGB) kommen im Einzelfall in Betracht. Wer Shareware-Autoren durch Missbrauch von Testversionen um die Früchte ihrer Arbeit bringt, handelt also nicht nur unfair, sondern riskiert auch massiven rechtlichen Ärger."

In einem weiteren Artikel widmet sich Mielke den Crackprogrammen, mit denen Freischalt-Codes für Shareware-Programme generiert werden können [110]. Er kommt zu den Ergebnissen, dass das öffentliche Anbieten solcher Programme kein Urheberrechts-Verstoß ist, weil diese Programme unabhängig von dem Werk des Programmierers entwickelt werden, und auch kein Computerbetrug, weil keine unmittelbare Bereicherungsabsicht besteht. Im Anschluss an § 17 Abs. 2 UWG meint er aber, dass sich sowohl der Programmierer wie auch der Verbreiter dieser Programme strafbar machen können, weil sich der eine ein fremdes Geschäftsgeheimnis unter Einsatz technischer Mittel verschafft und der andere es verbreitet.

Diese Argumentation hilft ein Wenig weiter. In der Praxis wird jedoch die "Geheimnis-Eigenschaft" sehr genau zu prüfen sein, weil eine genaue Abgrenzung zu allgemeinbekannten Kenntnisse vorzunehmen ist, die sich wohl auch auf die verwendeten Algorithmen beziehen muss.

[110] c't 22/02, S. 202; Freischaltcodes für alle? 'Keyz' und 'Serialz' stellen Strafverfolger vor Probleme

4. **Homepages und Urheberrecht**

Eine profunde Zusammenstellung von wirtschaftlichen und rechtlichen Erwägungen bei der Veröffentlichung von Newslettern hat Andreas H. Roemer bei newsletterbuch.de veröffentlicht. Seine Ausführungen und Warnungen lassen sich lückenlos auf die Veröffentlichung von Homepages übertragen.

Eine gute Einführung zum Thema bietet Dietrich Harke, Was muss ich bei meinem Internetauftritt beachten? (PDF, 241 kb); es handelt sich um einen Auszug aus: Dietrich Harke, Urheberrecht. Fragen und Antworten.

In der c't 9/00, S. 236, setzt sich Prof. Dr. Dietrich Harke mit dem Thema "Homepage und Urheberrecht. Rechtsfragen der Multimedia-Produktion" auseinander. Der Artikel ist leider nicht auf dem Heise-Server verfügbar.

In dem Artikel von Harke wurden die Ge- und Verbote für eine Veröffentlichung fremder Dateien auf Homepages listenmäßig zusammen gestellt (c't 9/00, S. 238):

Was darf lizenzfrei veröffentlicht werden?

1. 'Gemeinfreie' Werke, an denen keine Urheber- Leistungsschutzrechte mehr bestehen (z.B. Scan aus alten Büchern)

2. Vom Urheber freigegebenes Quellenmaterial ('freeware')

3. Amtliche Werke

4. Markennamen und Zitate innerhalb der im Artikel benannten Grenzen

- Markennamen dürfen außerhalb des geschäftlichen Verkehrs und Wettbewerbs z.B. zur Berichterstattung, politischen Meinungsäußerung, Satire oder für ein Lexikon und solange verwendet werden, wie sie nicht mit Verleumdungen, Beleidigungen oder falschen Tatsachenbehauptungen verbunden werden (weitere Einzelheiten im Text des Artikels)

- Zum Zitatrecht: "Die Verwertungsrechte der Urheber werden durch das Zitatrecht eingeschränkt (§ 51 UrhG). Zweck der Zitierfreiheit ist es, die Freiheit der Auseinandersetzung mit fremden Gedanken zu fördern, und zwar auch so, dass politische, wissenschaftliche oder geistige Strömungen durch wörtliche Wiedergabe einzelner Stellen aus geschützten Werken deutlich gemacht werden können ('Kleinzitat'). Das Kleinzitat ist auch bei Multimediawerken möglich, wobei, wenn es nicht anders geht, ganze Werke zitiert werden können (Fotos, Bilder, Zeichnungen). Bei wissenschaftlichen Werken ist es grundsätzlich zulässig, ganze Werke anderer aufzunehmen ('Großzitat'). ..." (weitere Einzelheiten im Text des Artikels).

5. Bilder Lebender, soweit sie Personen der Zeitgeschichte sind, für Berichterstattung (nicht für Werbung)

6. Bilder Verstorbener, wenn der postmortale Persönlichkeitsschutz erloschen ist

7. Fremde Ideen können aufgegriffen und in neue Werke mit eigenständigem Charakter umgesetzt werden

Hier ist Vorsicht geboten:

1. Einscannen von alten Fotos, Grafiken, sonstigen Abbildungen aus aktuellen Büchern: Rechte der Fotografen und Verleger sind zu beachten

2. Anhäufung von Zitaten eines einzigen fremden Urhebers

3. Personenbilder: Berechtigte Interessen der Abgebildeten, bei Abbildungen Verstorbener müssen Rechte der Angehörigen berücksichtigt werden

4. Verwendung von Markennamen durch Wettbewerber im geschäftlichen Bereich

5. Alte Musik: Lizenzpflichtig, soweit noch Rechte der Interpreten oder Tonträgerhersteller bestehen

Ergänzung:

Auch redaktionell von einem Verlag "konsolidierte", ggf. auch mit Anmerkungen versehene Gesetzestexte und besonders ihre inhaltliche Zusammenstellung ist eine Datenbank im Sinne des § 87a Abs. 1 Satz 1 UrhG dar. Der mit der Konsolidierung von Gesetzestexten verbundene zeitliche und personelle Aufwand stellt eine wesentliche Investition im Sinne des § 87a UrhG dar. [111]

[111] Leitsätze des Urteils des LG München I vom 08.08.02 - 7 O 205/02 -

Hier sind stets Lizenzen vonnöten:

1. Kopieren, Scannen urheberrechtlich geschützten Materials außerhalb des privaten Bereichs

2. Übernehmen urheberrechtlich geschützten Materials aus dem Internet

3. Kommerzielle Verwendung von Personenbildern, z.B. in der Werbung (bis mindestens 10 Jahre nach dem Tod der abgebildeten Person)

4. Kopieren von Computerprogrammen (außer einer erforderlichen Sicherungskopie durch berechtigten Nutzer) und elektronischen Datenbanken

...

Provokant:

Äußerst engagiert argumentiert Michael H. Goldhaber [112] gegen den gesetzlichen Schutz des Urheberrechts als ein überholtes Hemmnis des späten Feudalrechts.

> "Die Durchsetzung des Urheberrechts unterstützt den Kapitalismus auf besonders einfache Art. Es verhindert echten Wettbewerb, schafft staatlich sanktionierte Monopole für Markenwaren, neue Gerätschaften, Software, Medikamente, Designer-Kleidung, Turnschuhe, Fast-food-Ketten und viele andere Dienstleistungen und, natürlich, fast alle Texte, Filme, Bilder und Musik, die den ganz besonderen Schutz des Urheberrechts genießen.
>
> Trotz seiner anscheinenden Stärke sieht sich der Kapitalismus zunehmend bedrängt. Die Gesetze rund um das geistige Eigentum sind unabdingbar für das Geschäft, nicht für die Künstler. ..."

Haftung für Links?

Die rechtliche Situation ist weiterhin noch sehr unklar.

Im Streit ist, ob die Links von privaten Homepages den Verantwortungszuweisungen im Teledienstegesetz (TDG) und dem Mediendienstestaatsvertrag (MDStV) für private, nichtkommerzielle Homepages gelten,

ob der MDStV Rechtswirkung hat oder ob nicht doch jede Internetpräsentation ungeachtet ihres kommerziellen Charakters zumindest markenrechtlich und wettbewerbsrechtlich als gewerbliches Handeln zu begreifen sind.

Weitere Einzelheiten erfahren Sie im Aufsatz Online-Strafrecht III, Ordnungswidrigkeiten im Multimediarecht.

Das Landgericht Frankenthal hat am 28.11.00 entschieden, dass Linksammlungen nur als eine Art "Türöffner" dienen und man eben nicht für die Inhalte auf fremden Internetsites verantwortlich ist (?.de-News vom 25.01.2001). Die Entscheidung wird dokumentiert bei afs-rechtsanwaelte.de.

Siehe auch Thomas Stadler, Verantwortlichkeit für Hyperlinks nach der Neufassung des TDG (bei jurpc.de)

Das OLG Braunschweig sieht durch "die Setzung des im Streit befindlichen Hyperlinks keine an der Streitmarke bestehenden Rechte der Beklagten verletzt, weil die Klägerin jedenfalls bis zu der im Januar 2000 ausgesprochenen Abmahnung die Privilegierung des § 5 Abs 2 Teledienstegesetz (alte Fassung des TDG) zugute kommt". ...

---

[112] Napster und das Feudalrecht, c't 23/00, S. 311 ff.; Zitat S. 314

5. **Multimedia-Links**

...

6. **MP3 und Urheberrecht, Urheberrechtsabgabe auf PCs**

...

In dieselbe verbraucherfeindliche Richtung gehen zur Zeit die Entwickler sogenannter e-books, also elektronischer Bücher, indem sie Nutzungsbeschränkungen auf die Person des Käufers vorsehen wollen. Trotz der Einsparung der materiellen Druckkosten werden diese e-books eher teurer als billiger als die gedruckten Versionen sein. Sie würden sich aber nicht verleihen oder verkaufen lassen.

Heise-Meldung vom 31.03.02:

> International Federation of the Phonographic Industry: Piraten verderben das Geschäft
>
> "17,1 Millionen Deutsche kopierten Musik auf 182 Millionen CD-Rohlinge, zitiert der Verband die Studie, für die 10.000 Personen befragt wurden. Rund 5 Millionen Personen hätten 492 Millionen Stücke von "meist illegalen Angeboten" aus dem Internet geladen.
>
> Wäre die Musik gekauft worden, so der Verband, wäre ein Umsatz von 3,2 Milliarden Euro erzielt worden. Dagegen sank der Umsatz der Musikwirtschaft im vergangenen Jahr laut Zahlen der IFPI um 10 Prozent auf 2,49 Milliarden Euro. Im Jahr 2001 verkaufte die deutsche Musikwirtschaft 244 Millionen Tonträger, rund 22 Millionen weniger als im Jahr zuvor. Natürlich sei nicht jede Kopie ein entgangener Kauf, aber die Größenordnung des Problems sei erkennbar, meint die IFPI. Zu den 3,2 Milliarden müssten noch rund 50 Millionen Euro illegaler Umsatz für traditionelle gewerbliche Piraterie und 220 Millionen Euro für so genannte Schulhofpiraterie hinzugerechnet werden."

...

Thomas Kniebe in der Süddeutschen Zeitung vom 01.03.03:

Die Drumrum-Industrie. Warum es euch schlecht geht: Ein mitfühlender Brief an die notleidende Musikbranche

> "... Eure Preise müssen kleiner und eure Verpackungen größer, glamouröser, interessanter werden. Nehmt euch ein Beispiel am DVD-Geschäft: Im Grunde keine technische Revolution, sondern eine Revolution des Drumherum. Die Filme sind genauso scharf wie ein normales Fernsehbild, ob man's glaubt oder nicht – aber die Extras, die Stunden von Zusatzmaterial, die liebevollen Kommentare, Editionen, Sammlerboxen! Das kaufen die Leute wie die Irren. Und keiner beschwert sich über die Preise. ..."

...

7. **Hearing zur Umsetzung der EU-Urheberrechtsrichtlinie**

...

7a. **Freiheit für Lehre und Wissenschaft**

...

8. **Softwarepatentierung**

...

9. **"Abmahnunwesen" im Internet**

...

10. **Elektronische Pressespiegel**

...

Akten

Zur Einführung ein Zitat (Auszug) von Seibert (rechtssemiotik.de)

> " Akten sind Dokumente im Plural. "Acta" nannten sie die Römer, die Protokolle von Senatssitzungen sammelten. Aber die Karriere der Akten begann erst mit der neuzeitlichen Staatsverwaltung. Sachakten vereinigen nicht etwa Autoren und Themen, sie spiegeln vor allem den Gang der Sache in der Zeit. Erst als man in den Behörden anfing, Sachakten zu führen, entwickelten sich Rechtsvorgänge zum Zeichenprozess, in dem jede Äußerung einen festgelegten Ort erhielt. Bürokratien richten für die Aktenführung Registraturstellen ein, die Vorgänge nach einem Plan ordnen ... Der Plan ergibt sich zunächst aus dem Ort der Aktenführung. Ermittlungsakten werden bei der Verfolgungsbehörde - das waren historisch die Inquisition, dann die Polizei und später auch die Staatsanwaltschaft - geführt. Der doppelte Wille, Tatsachen nicht nur zu hören, sondern auch zu sammeln und mit der schriftlichen Sammlung Macht auszuüben, steht am Anfang der Aktenführung.

Für die Struktur, den Umfang und die Organisation von Akten im Justizbereich gelten die Aktenordnung (AktO) einschließlich der Sonderregelungen in den einzelnen Bundesländern.

Der Aktenaufbau soll aktuell, vollständig und sachlich geordnet (logisch) sein.

Es gelten einige Grundprinzipien, auf die ich mich an dieser Stelle beschränken möchte.

1. Akten können als Blattsammlungen oder als "feste Akten" geführt werden; im Zweifel sollen sie als feste Akten angelegt werden (§ 3 Abs. 2, § 3 Abs. 4).

2. Feste Akten sind geheftete Bände, die über einen Aktenumschlag als Aktendeckel verfügen (§ 3 Abs. 3). Ihr Inhalt wird mit fortlaufenden Blattzahlen versehen (paginiert). Jeder Aktenband beginnt mit der Ziffer "1". In der Regel sollen die Aktenbände nicht mehr als 250 Blätter enthalten. Die Anlage eines zweiten oder weiteren Bandes ist auf dem geschlossenen Band zu vermerken (i.d.R. auf der Rückseite des letzten Blattes des geschlossenen Bandes).

3. Die Reihenfolge der eingehefteten Blätter richtet sich nach ihrem zeitlichen Eingang (§ 3 Abs. 1 S. 1).

4. Sofern sachlich eine differenzierte Ordnung geboten erscheint, können gesonderte Hefte angelegt werden. Diese bilden zusammen mit dem Hauptband der Akten "Sammelakten" (§ 3 Abs. 1 S. 2).

Je nach den Bedürfnissen des einzelnen Verfahrens können Fall- und Beweisstückakten angelegt werden. Alle übergeordneten und zusammenfassenden Aktengegenstände (Beschuldigtenvernehmung, Zwischenvermerke usw.) müssen in den Hauptakten dokumentiert werden. Nebenakten sollen im Zweifel ausschließlich aus Kopien bestehen.

Vergl. auch Nr. 17 Abs. 2 Richtlinien für das Straf- und Bußgeldverfahren (RiStBV): Hat jemand mehrere selbständige Straftaten begangen, so sorgt der Staatsanwalt dafür, dass die Verfahren verbunden oder die Ergebnisse des einen in dem anderen berücksichtigt werden.

5. Schriften und Ablichtungen, die später zurück zu geben sind (sichergestellte, also amtlich verwahrte Schriftstücke) oder sich nicht zur Einheftung eignen, sind in eine ge-

sonderte Hülle zu nehmen, die ihrerseits einzuheften ist (§ 3 Abs. 1 S. 3).

Anmerkungen:

Bei größerem Umfang sollte für solche Schriftstücke ein Beweismittelheft angelegt werden, auf das im Hauptband verwiesen werden soll (Vermerk).

Original-Schriftstücke sollten in Papierhüllen verwahrt werden. Soweit Klarsichthüllen verwendet werden, sind bestimmte physikalisch-technische Untersuchungen an den Schriftstücken nicht mehr möglich.

Werden - z.B. anlässlich einer Zeugenvernehmung - Originalschriftstücke zu den Akten übergeben, so handelt es sich um eine amtliche Inverwahrnahme (Sicherstellung). Auch wenn dies nirgendwo vorgeschrieben ist, sollte im Interesse der Aktenklarheit ein Sicherstellungsverzeichnis nach § 109 StPO angelegt werden.

In Umfangsverfahren kann sich die Anlage von Sicherstellungsheften empfehlen, in denen die einzelnen Durchsuchungsbeschlüsse, -vermerke, -protokolle und insbesondere der Verbleib der sichergestellten Gegenstände dokumentiert werden.

6. Für förmliche Zustellungen soll ein Zustellungsband angelegt werden. In der gerichtlichen Praxis wird hierzu häufig ein Ladungsband angelegt, in dem die gesamte Korrespondenz im Zusammenhang mit den Ladungen der Verfahrensbeteiligten dokumentiert wird (z.B. auch die erforderlichen EMA-Anfragen und -auskünfte; § 3 Abs. 1 S. 4, 5).

Wird darauf verzichtet, so sind die Zustellungsnahweise hinter die relevante Entscheidung zu heften.

7. Kostenrechnungen sollen als "Vorblätter" vor Bd. I, Bl. 1 d.A. geheftet werden. Sie werden mit römischen Ziffern paginiert (§ 3 Abs. 1 S. 6, 9).

In Umfangsverfahren bietet sich die frühzeitige Anlage von Kostenheften an, in denen alle Kostennoten, Zahlungsein- und -ausgänge und z.B. Dienstreisegenehmigungen dokumentiert werden.

8. Zahlungseingänge werden in ihrer zeitlichen Reihenfolge in den Akten dokumentiert. Sie sollen außerdem in einer gesonderten Aufstellung erfasst werden (§ 3 Abs. 1 S. 8)

9. Die Aktenumschläge sollen beschriftet werden (§ 3 Abs. 5).

Die Beschriftung soll Auskunft geben über

die aktenführende Behörde

die Parteien (in Strafsachen: Beschuldigte und Verteidiger, Nebenkläger)

das Aktenzeichen

Auf der Innenseite der Aktenumschläge soll verzeichnet werden (ggf. auch auf Vorblättern):

Beweis- und Musterstücke (§ 9 Abs. 5)

Sonder- und Beweismittelhefte

Beiakten (derselben oder von anderen Behörden; Beiakten erhalten einen Aufkleber, damit sie den Hauptakten zugeordnet werden können)

In besonderen Fällen erhalten die Aktenumschläge auch Aufkleber, Beispiele:

Haft

Pressestrafsache

Jugendlicher

Heranwachsender

Ausländer

Auslieferung (Spezialitätsvorbehalte)

Eilsache

10. Jedes Aktenstück erhält ein Aktenzeichen, das zugleich die Geschäftsnummer ist (§ 4 Abs. 1 S. 1, 3)

11. Über den Verbleib der Eingänge und Akten ist ein Nachweis zu führen (in aller Regel in den Handakten; § 5).

12. In geeigneten Fällen sind Hilfs- oder Doppelakten anzulegen. Dies gilt besonders, wenn Haftprüfungen oder Haftbeschwerden zu erwarten sind (Nr. 12 Abs. 2 RiStBV)

13. Werden Aktenbestandteile nachträglich entfernt, so ist dies zu vermerken und/oder ein Fehlblatt an ihre Stelle zu heften.

14. Doppelakten sollen ausschließlich aus Kopien bestehen. Originale - z.B. Entscheidungen des Ermittlungsrichters - sollen aus ihnen entheftet und in den Hauptakten dokumentiert werden.

15. Beweismittelordner, also solche Akten, die in dieser Form von Dritten stammen (z.B. sichergestellte Buchführungsteile, Kreditakten), können, wenn ihnen eine Paginierung fehlt, mit Blattzahlen versehen werden.

16. Sonderhefte, die aus Ablichtungen von Akten anderer Justizbehörden stammen (z.B. Handelsregister- und Zivilverfahrensakten), werden nicht neu paginiert. Auch dann, wenn sie nur zum Teil im SH dokumentiert werden, gilt die Paginierung des Ursprungsverfahrens.

17. Original-Akten anderer Behörden sollen möglichst schnell wieder zurück gegeben werden. Im Zweifel sind ihr wesentlicher Inhalt durch Ablichtungen zu dokumentieren, die zu Sonderheften genommen werden.

EDV-Workshop

Der EDV-Workshop - ein Erfahrungsaustausch

Seit 1997 haben im Abstand von jeweils rund neun Monaten fünf ganztägige Veranstaltungen im Bildungsinstitut der Polizei Niedersachsen (BIP Wennigsen) stattgefunden; zuletzt am 16.03.2001. Ihre fachlichen Ergebnisse sind insbesondere in ein Arbeitspapier zur Erhebung und Auswertung von EDV-Daten eingeflossen.

Veranstalter der Treffen ist die Staatsanwaltschaft Hannover gewesen (StA-Hannover.de). Die Erfahrungsaustausche richten sich bevorzugt an Staatsanwälte, Polizeibeamte und Steuerfahnder mit fortgeschrittenen Computerkenntnissen aus dem Bundesland Niedersachsen.

EDV als Arbeitsmittel und Ermittlungsgegenstand

Die Teilnehmer sollen die Kenntnisse und Erfahrungen aus verschiedenen Strafverfolgungsbehörden im Umgang mit der EDV als Arbeitsmittel und als Ermittlungsgegenstand zusammenfassen und weitervermitteln.

Die Themen decken den gesamten Bereich der rechtlichen und tatsächlichen Probleme beim Umgang mit sichergestellten Daten, ihrer Erhebung und Auswertung, der Verwendung des Internets als Informationsquelle, des Datenschutz' und der Netzsicherheit ab.

Daneben werden auch praktische Lösungen z.B. bei der Sicherung und Weiterverarbeitung von Buchführungsdaten oder zur Berechnung von Steuern präsentiert und diskutiert.

Der EDV-Workshop ist auf das persönliche Engagement seiner Teilnehmer angewiesen. Diese arbeiten ehrenamtlich, auf eigene Kosten und ohne Entlastung von ihren sonstigen beruflichen Aufgaben mit. Sie bereiten sich auf Beiträge und Demonstrationen vor, übernehmen die gewonnenen Erfahrungen in ihre Berufspraxis und geben sie an ihre Kollegen weiter.

Hierfür sage ich auch an dieser Stelle meinen besonderen Dank!

OStA Dieter Kochheim

Der EDV-Workshop -eine Website

Die Idee, für den EDV-Workshop eine Plattform im Internet zu schaffen, ist während des 4. EDV-Workshops am 19.11.99 entstanden.

Den Zielen der Veranstaltungsreihe ist auch die Internet-Domain EDV-Workshop.de gewidmet, die seit dem 3. Januar 2000 im Internet installiert ist.

Seither ist die Website von mir mehrfach gründlich überarbeitet und ständig erweitert worden.

Dabei werde ich von einer ganzen Reihe von Kollegen mit Hinweisen und freundlichem Lob unterstützt.

Vier grob unterscheidbare Dienste stellt die Homepage zur Verfügung:

Themen

Hier werden Arbeitspapiere und Aufsätze zum Download bereitgestellt. Neben anderen - bevorzugt - strafverfahrensrechtlichen Themen besteht ihr thematischer Schwerpunkt in der Behandlung von Praxisproblemen im Zusammenhang mit Durchsuchungen und Beschlagnahmen sowie der Behandlung von EDV-Geräten und -Daten.

Die wesentlichen Veränderungen werden in den Redaktions-Beiträgen erläutert, die auf der Startseite dokumentiert sind.

Links

Bei meinen Recherchen im Internet habe ich viele Internetadressen gefunden, die auch über den Einzelfall hinaus für die praktische Arbeit der Ermittlungsbehörden von Interesse sind.

Hierbei handelt es sich ebenso um Gesetzessammlungen, z.B. der Uni Saarbrücken, wie auch um rein praktische Hilfsmittel, wie z.B. die Online-Version der Schwacke-Liste, die Datenbank mit allen von den Industrie- und Handelskammern zugelassenen Sachverständigen oder das Programm zur Berechnung von Bußgeldern der bayerischen Polizei.

Insgesamt werden mehr als 300 geprüfte und als sinnvoll angesehene Links angeboten, die mit Kommentaren und ergänzenden Hinweisen versehen sind.

Neben der anfänglichen Überprüfung suche ich die Adressen sporadisch auf, um zu überprüfen, ob sie noch immer erreichbar sind und weiterhin dem Kriterium der "Brauchbarkeit" entsprechen.

Entsprechen sie ihm nicht, werden sie gelöscht.

Lexikon

Das Lexikon ergänzt die beiden genannten Angebote um eine alphabetisch geordnete Sammlung verschiedener Texte, Tabellen, Link- und Materialsammlungen.

Handbuch

Das Handbuch, das Sie gerade benutzen, stellt zusammenfassende Auskünfte, Erklärungen und Anleitungen zur Verfügung. Es gliedert sich in drei Hauptteile:

Bedeutung des Internets für die Ermittlungsbehörden und Beispiele für Recherchemöglichkeiten.

Technische, sachliche und juristische Erläuterungen zu Sinn, Zweck und Grenzen der Homepage des EDV-Workshops.

Unter Graphiken werden einige Gestaltungselemente erläutert.

Fortentwicklung

Alle vier Angebote werden kontinuierlich aktualisiert und erweitert. Die Veröffentlichung muss sich aber auf solche Hilfsmittel und Auskünfte beschränken, die der Allgemeinheit zugänglich gemacht werden dürfen. Trotz dieser Einschränkung bin ich davon überzeugt, dass ein interessantes und hilfreiches Angebot entstanden ist und sich noch weiter entwickeln wird.

Hinweise und fehlendes Material bitte ich mir mitzuteilen. Die zur Kontaktaufnahme mit dem EDV-Workshop nötigen Angaben werden u.a. hier und im Begrüßungsfenster gezeigt.

zugangsbeschränkter Bereich

Es besteht die Überlegung, einen zugangsgesicherten Homepagebereich für registrierte Mitglieder zu schaffen. In diesem Teil könnten solche Informationen, Programme und Anwendungen angeboten werden, die nicht für die breite Öffentlichkeit bestimmt sind oder die potenziell geheimbehaltungsbedürftig sind. Gedacht ist insoweit nicht an persönliche Daten, sondern an verfahrensbezogene Informationen, die möglicherweise Rückschlüsse auf Personendaten zulassen oder die einen zu intensiven Einblick in die Ermittlungstaktiken der Strafverfolgungsbehörden ermöglichen würden.

Zwei zwingende Voraussetzungen müssten erfüllt sein:

Es müsste ein Bedarf dafür bestehen.

Die Zugangssicherung darf keine Umgehungsmöglichkeiten zulassen.

Nachdem die Zugangsbeschränkung unter Strato nicht funktioniert, kann zur Zeit ein solcher Service nicht angeboten werden.

Schwerpunkt Wirtschaftsstrafrecht

Das vorhandene Angebot des EDV-Workshops hat seinen inhaltlichen Schwerpunkt im Bereich des Wirtschaftsstrafrechts.

Dafür gibt es mehrere Gründe:

1) Bei der Verfolgung von Wirtschaftsstrafsachen werden seit Mitte der achtziger Jahre Computer zur Dezernatsarbeit eingesetzt. Insbesondere zur Bearbeitung von Großverfahren sind sie ein unverzichtbares Hilfsmittel, um die Material- und Informationsmenge überhaupt bewältigen zu können.

2) Seit Anfang der neunziger Jahre ist die Verwendung von sichergestellten elektronischen Daten ein ständiges Problem. Die Beteiligten in Wirtschaftsstrafverfahren haben erheblich früher die EDV als Arbeitsmittel verwendet als die Beteiligten anderer Ermittlungsverfahren.

Beide genannten Gründe haben dazu geführt, dass sich die Dezernenten in den Wirtschaftsabteilungen der Staatsanwaltschaften deutlich eher mit der Praxis und der rechtlichen Beurteilung der EDV auseinandersetzen mussten als ihre Kollegen.

Als zweiter großer Anwendungsbereich haben sich die Ermittlungen im Zusammenhang mit kinder- und gewaltpornographischen Veröffentlichungen ergeben. Alle anderen Kriminalitätsfelder werden innerhalb gewisser Grenzen nachziehen. Es steht jedenfalls zu erwarten, dass der Umgang mit elektronischen Daten bei jedem Ermittlungsverfahren bedeutsam werden kann.

3) Schließlich ein weiterer, eigentlich banaler Grund:

Praxiserfahrungen weitergeben kann nur, wer solche Erfahrungen auch sammelt. Ich selber und der überwiegende Teil der Initiatoren dieser Homepage sind in Wirtschaftsstrafsachen tätig (gewesen), so dass unsere Erkenntnisse auch im wesentlichen einfließen.

Für Hinweise aus anderen Ermittlungs- und Tätigkeitsschwerpunkten bin ich deshalb - das kann ich nur immer wieder betonen - besonders dankbar.

...