BUNDESRECHTSANWALTSKAMMER

Stellungnahme

der Bundesrechtsanwaltskammer

zur Verfassungsbeschwerde des Herrn J. B.

2 BvR 902/06

gemeinsam erarbeitet vom

Strafrechtsausschuss der Bundesrechtsanwaltskammer

Rechtsanwalt Prof. Dr. Dr. Alexander Ignor, Berlin, Vorsitzender
Rechtsanwalt und Notar Dr. Jochen Heidemeier, Stolzenau
Rechtsanwalt Thomas C. Knierim, Mainz (Berichterstatter)
Rechtsanwalt Dr. Daniel Krause, Berlin
Rechtsanwalt Prof. Dr. Holger Matt, Frankfurt am Main
Rechtsanwältin Anke Müller-Jacobsen, Berlin
Rechtsanwalt Dr. Eckhart Müller, München
Rechtsanwalt Prof. Dr. Reinhold Schlothauer, Bremen
Rechtsanwältin Dr. Anne Wehnert, Düsseldorf

Prof. Dr. Werner Beulke, Passau (Berichterstatter)

und vom

Verfassungsrechtsausschuss der Bundesrechtsanwaltskammer

Rechtsanwalt Dr. Christian Kirchberg, Karlsruhe, Vorsitzender (Berichterstatter)
Rechtsanwalt Prof. Dr. Michael Uechtritz, Stuttgart
Rechtsanwalt Prof. Dr. Michael Quaas, Stuttgart
Rechtsanwalt Dr. Christian Bracher, Berlin
Rechtsanwalt und Notar Dr. Wolfgang Kuhla, Berlin
Rechtsanwalt und Notar Prof. Dr. Bernhard Stüer, Münster
Rechtsanwalt Dr. Christofer Lenz, Stuttgart

Rechtsanwalt Frank Johnigk, Bundesrechtsanwaltskammer, Berlin

Januar 2007

BRAK-Stellungnahme-Nr. 1/2007

A. Überblick über den Verfahrensgegenstand

Mit der Verfassungsbeschwerde vom 28. April 2006 – 2 BvR 902/06- wird die Verletzung der Grundrechte des Beschwerdeführers aus Art. 10 Abs. 1 GG (Post- und Telekommunikationsfreiheit), Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (Grundrecht auf informationelle Selbstbestimmung) durch Beschlüsse des Amtsgerichts Braunschweig vom 14. und 22. März 2006 und des LG Braunschweig vom 12. April 2006 geltend gemacht.

1.)

Der Beschwerdeführer wendet sich im Wesentlichen dagegen, dass seine von einem Serviceprovider für ihn verwaltete private und geschäftliche E-Mail-Korrespondenz in einem Ermittlungsverfahren der Staatsanwaltschaft Braunschweig gegen Dritte nach Maßgabe der angegriffenen Beschlüsse beschlagnahmt und auf für das Verfahren relevante Inhalte durchgesehen werden soll.

Mit einem nicht mit der Verfassungsbeschwerde angegriffenen Durchsuchungsbeschluss vom 9. Februar 2006 (Anlage 7 zur Verfassungsbeschwerde) ordnete das AG Braunschweig gem. den §§ 103, 105, 100g, 100h StPO u.a. die Durchsuchung der Wohnung des Beschwerdeführers zur Auffindung von Beweismitteln an, die aufgrund konkret bezeichneter Tatsachen in der Wohnung des Beschwerdeführers vermutet wurden. Den Ermittlungsbehörden wird außerdem eine Auswertung *„von Datenträgern gestattet, insbesondere von Textdateien und e-mail-Verkehr“.* Unmittelbar im Anschluss an die zeugenschaftliche Vernehmung des Beschwerdeführers am 14. März 2006 durchsuchten Beamte des Landeskriminalamtes unter Leitung eines Staatsanwaltes die Wohnung und den dort befindlichen Computer des Beschwerdeführers. Bei der Überprüfung des Computers stellte sich heraus, dass dort keine E-Mail Korrespondenz gespeichert war, sondern die für den Beschwerdeführer und sein Unternehmen bestimmten elektronischen Nachrichten (E-Mails) von einem gewerblichen Dienstanbieter (sog. Service-Provider), nämlich der Fa. Schlund und Partner, Karlsruhe, verwaltet wurden. Der Beschwerdeführer hatte mit dem Service-Provider einen Vertrag über die Bereitstellung und Verwaltung einer elektronischen Adresse (sog. E-Mail-Account) abgeschlossen, auf dessen Grundlage der Beschwerdeführer über das Internet, d.h. in einer Online-Kommunikation, Zugang zu den unter diesem Account verwalteten E-Mails erhielt.

Nach dem Beschwerdevorbringen, dem das Nds. Ministerium der Justiz in seiner Stellungnahme vom 2. Juni 2006 insoweit nicht entgegengetreten ist, werden diese E-Mails nicht auf dem Computer des Beschwerdeführers gespeichert, sondern sie werden ausschließlich durch den Serviceprovider verwaltet. Übereinstimmend gehen Beschwerdeführer und Ermittlungsorgane davon aus, dass die E-Mails „*auf dem Mailserver des Providers gespeichert*“ werden und dieser Speicherplatz „*bei dem Service-Provider angemietet*“ sei. Während der laufenden Wohnungsdurchsuchung demonstrierte der Beschwerdeführer auf Verlangen der Ermittler den Onlinezugang am Computerbildschirm, brach diesen Vorgang aber ab, nachdem die Ermittlungsorgane keine Durchsuchungs- und Beschlagnahmeanordnung für Telekommunikationsvorgänge (nach § 100a StPO) vorweisen konnten.

Die Staatsanwaltschaft Braunschweig ordnete daraufhin noch am 14. März 2006 die Beschlagnahme des E-Mail-Accounts an. Mit dem angegriffenen Beschluss des AG Braunschweig vom 14. März 2006 (Anlage 2 zur Verfassungsbeschwerde) wird „*der e-Mail-Account*“ des Beschwerdeführers bei der Schlund und Partner AG, Karlsruhe, ohne Angabe von Gründen gem. den §§ 94, 98 StPO beschlagnahmt. Dagegen richtete sich die Beschwerde des Beschwerdeführers vom 16. März 2006 (Anlage 8 zur Verfassungsbeschwerde), mit der geltend gemacht wurde, dass der Durchsuchungsbeschluss vom 9. Februar 2006 keine ausreichende Durchsuchungs- und Beschlagnahmegrundlage für das E-Mail-Account und die dort verwalteten E-Mails sei, weil der Abruf von E-Mails über das Internet Teil eines nicht abgeschlossenen Telekommunikationsvorgangs sei. Da die E-Mails nicht auf dem Computer des Beschwerdeführers in dessen Wohnung gespeichert seien, könne der Telekommunikationsvorgang mit der Zwischenspeicherung bei dem Service-Provider nicht als beendet angesehen werden. Erst wenn die E-Mail von dem Empfänger zur Kenntnis genommen worden sei, sei der Telekommunikationsvorgang abgeschlossen. Folglich könnten die Durchsuchung und die mit Beschluss vom 14. März 2006 angeordnete Beschlagnahme des E-Mail-Accounts nur auf der Grundlage des § 100a StPO gerechtfertigt sein; die Anordnungsvoraussetzungen dafür seien nicht dargetan.

Im Übrigen werde mit der Beschlagnahme in das Recht auf informationelle Selbstbestimmung des Beschwerdeführers und des von ihm geführten Unternehmens eingegriffen, ohne dass nachvollziehbare Begründungen und Begrenzungen der Maßnahme mitgeteilt würden. Eine wahllose Durchsicht der Geschäftskorrespondenz des Beschwerdeführers sei unverhältnismäßig. Auf den Antrag der Staatsanwaltschaft Braunschweig vom 20. März 2006 (Anlage 9 zur Verfassungsbeschwerde) half das AG Braunschweig mit Beschluss vom 22. März 2006 (Anlage 3 zur Verfassungsbeschwerde) der Beschwerde nicht ab. Im Beschluss werden lediglich die zu

beschlagnahmenden E-Mails (*„Dateien“*) nach den dort genannten Suchbegriffen konkretisiert. Der Beschluss ist im Übrigen nicht mit Gründen versehen.

Mit Schreiben vom 30. März 2006 (Anlage 10 zur Verfassungsbeschwerde) vertiefte der Beschwerdeführer seine mit der Beschwerde vorgebrachten Einwände und wies ergänzend darauf hin, dass die – auch nach der Bestimmung von Suchbegriffen - nahezu uneingeschränkte Durchsicht der E-Mail Korrespondenz sein Grundrecht auf informationelle Selbstbestimmung schwerwiegend beeinträchtige. Seine Geschäftsbeziehungen zu Kunden seien auf Vertraulichkeit angelegt. Bereits die nachgewiesene Tatsache, dass durch Indiskretionen der Name des Beschwerdeführers Ende März 2006 im Online-Dienst der Zeitschrift „Stern“ in eine konkrete Beziehung zu der von der Staatsanwaltschaft Braunschweig zu ermittelnden „VW-Affäre“ gesetzt und die Öffentlichkeit über die Wohnungsdurchsuchung unterrichtet worden sei, gefährde seine Geschäftsbeziehungen. Unter Verhältnismäßigkeitsgesichtspunkten sei es außerdem geboten, nur bestimmte, einzeln bezeichnete Nachrichten zu beschlagnahmen. Um den Ermittlungsbehörden eine Durchsicht und Identifikation zu ermöglichen, schlug er eine weitere Eingrenzung von Suchbegriffen oder die Durchsicht der Korrespondenz in seinem Beisein vor.

Das LG Braunschweig verwarf mit Beschluss vom 18. April 2006 die Beschwerde und legte dem Beschwerdeführer die Kosten des Beschwerdeverfahrens auf. Nach Auffassung der Strafkammer ist die Beschlagnahme der E-Mails von den §§ 94, 98 StPO gedeckt und musste nicht –wie vom Beschwerdeführer vorgetragen – nach § 100a StPO entschieden werden. Für die Beurteilung der Frage, ob der durch Art. 10 Abs. 1 GG geschützte Kommunikationsvorgang beendet sei, komme es auf den bestimmungsgemäßen Zugang der E-Mail bei dem Provider an. Die E-Mails stünden dem Empfänger endgültig in einer angemieteten Mailbox zur Verfügung. Damit sei die Fallkonstellation derjenigen einer Speicherung der E-Mail auf dem Computer des Empfängers ohne weiteres vergleichbar. Auf eine weitere Beschränkung des Umfangs der Beschlagnahme durch Eingrenzung der Suchbegriffe oder der Suchauswahl oder durch eine vorherige gemeinsame Durchsicht habe der Beschwerdeführer keinen Anspruch, da alle Gegenstände zum Beweis geeignet seien, die in irgendeiner geschäftlichen Beziehung zu den Beschuldigten des Verfahrens stünden. Etwaige nicht benötigte Nachrichten seien nach Durchsicht herauszugeben.

2.)

Die Verletzung seiner Grundrechte aus Art. 10 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sieht der Beschwerdeführer in der nicht nach § 100a StPO angeordneten Beschlagnahme des E-Mail-Accounts und der nur geringfügig eingegrenzten Menge der einzelnen E-Mails. Nach überwiegender Ansicht von Rechtsprechung und Literatur sei der Telekommunikationsvorgang erst bei einem Speichern auf dem Computer des Empfängers abgeschlossen. Da es sich bei E-Mails um elektronische Nachrichten handele, die über das Telefonnetz verbreitet würden, sei – ähnlich dem Telefonieren - der Telekommunikationsvorgang erst mit dem „*Herunterladen*“ der Nachricht auf den Computer des Empfängers beendet. Die sofortige Beschlagnahme nahezu aller E-Mails in dem E-Mail Account verstoße gegen das Grundrecht auf informationelle Selbstbestimmung und sei zudem unverhältnismäßig. Die Maßnahme sei nicht vom Ermittlungszweck gedeckt. Es hätten unterscheidungskräftige Suchbegriffe vorgegeben und sodann nach einer ggf. mit dem Beschwerdeführer gemeinsam durchgeführten Sichtung des derart gefilterten Bestandes die tatsächlich verfahrensrelevanten E-Mails sichergestellt werden dürfen.

B. Stellungnahme

Die Bundesrechtsanwaltskammer hält die Verfassungsbeschwerde für begründet. Die angefochtenen Durchsuchungs- und Beschlagnahmeanordnungen stellen einen nicht gerechtfertigten Eingriff in das durch Art 10 GG geschützte Fernmeldegeheimnis dar. Selbst wenn insoweit jedoch nur das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) einschlägig wäre, könnten die zum Gegenstand der Verfassungsbeschwerde gemachten Gerichtsentscheidungen mangels einer ausreichenden gesetzlichen Grundlage und darüber hinaus wegen Verletzung des Verhältnismäßigkeitsprinzips keinen Bestand haben.:

1.)

Die mit der Verfassungsbeschwerde angesprochenen Fragen gehen über den einfachen strafprozessualen Zugriff auf E-Mails, die vertraglichen Absprachen entsprechend bei einem Service-Provider verwaltet werden, hinaus. Der Strafrechtsausschuss der Bundesrechtsanwaltskammer beobachtet in der Strafverfolgungspraxis erhebliche Unsicherheiten der Ermittlungsbehörden und

Strafgerichte bei der Einordnung von E-Mails zu den Grundrechten aus Art. 10 Abs. 1, Art. 13 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Die Beschlagnahmefähigkeit von E-Mails und die aus dem Verhältnismäßigkeitsgrundsatz heraus gebotene Begrenzung des Zugriffs auf Datenbestände, die E-Mails enthalten, ist sowohl bei Überwachung des Telekommunikationsverkehrs (§§ 100a ff. StPO), der Abfrage von Verkehrs- und Positionsdaten (§§ 100g-i StPO), bei der verdeckten „Internet-Fahndung“ (§§ 110a ff StPO) als auch bei der einfachen Wohnungsdurchsuchung (§§ 102 ff. StPO) von enormer praktischer Bedeutung. Da E-Mails ihrem Inhalt nach aus Nachrichten bestehen, die typischerweise durch einen Telekommunikationsvorgang übertragen werden, gehören sie zur Gruppe der bei der Telekommunikation anfallenden sog. Inhaltsdaten[1], die sich –je nach physikalischer und vertragsrechtlicher Situation- an verschiedenen Stellen „im Internet“, in einer nur durch Online-Kommunikation zugänglichen Mailbox oder auch planmäßig in einem lokalen Netzwerk oder auf einem lokalen Arbeitsplatzcomputer befinden können.[2]

a) Schon über die Reichweite der Grundrechte aus Art. 10 Abs. 1, Art. 13 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bei E-Mails besteht in der Rechtsprechung der Fachgerichte (BGH[3] und Strafkammern der Landgerichte[4]) und in der dazu veröffentlichten Literatur[5] Uneinigkeit. Als Ursachen dafür sind

(1) ein zuweilen mangelndes Verständnis der technischen Zusammenhänge,

(2) das Bedürfnis der Strafverfolgungspraxis, möglichst umfassend Nachweismöglichkeiten auszuschöpfen und schließlich

(3) ein allgemeines Unbehagen angesichts der hinter der technischen Entwicklung der Telekommunikation –insbesondere der virtuellen Datenwelt des Internet- zurückbleibenden strafprozessualen Eingriffsnormen (besonders die §§ 94, 98, 102, 103 StPO)

auszumachen.

[1] *Marberth-Kubicki*, Computer- und Internetstrafrecht, München 2005, Rn. 175ff. unterscheidet Inhaltsdaten, Verbindungs-/Verkehrsdaten, Nutzungsdaten, Bestands-/Benutzerdaten, Zugangs- und Positionsdaten.
[2] *Kemper* NStZ 2005, 538.
[3] BGH –Ermittlungsrichter NStZ 1997, 247 m. zust. Anm. *Vassilaki* JR 2000, 447 (zur polizeilichen Abfrage von Mailboxen im Internet).
[4] LG Hanau, StV 2000, 354 m. zust. Anm. *Dübbers*; LG Mannheim StV 2002, 242 m. zust. Anm. *Jäger* StV 2002, 244; LG Ravensburg CR 2003, 933; LG Bonn wistra 2005, 76.
[5] KK-*Nack* § 100a StPO Rn. 8; LR-*Schäfer* § 100a StPO Rn. 58; *Lührs* wistra 1995, 19; *Bär* CR 1995, 159ff, 227ff; 489, 495; *Palm/Roy* NJW 1996, 1791; *Marberth-Kubicki*, a.a.O., Rn. 193f, 195, 266; *Malek*, Straftsachen im Internet, Heidelberg 2005 Rn. 372f.; *Jahn* JuS 2006,491; *Kemper* NStZ 2005, 538.

b) Das Fernmeldegeheimnis des Art. 10 Abs. 1 GG umfasst jede Art von Fernmeldeverkehr ohne Rücksicht auf die konkrete Übermittlungsart und Ausdrucksform[6]. Der Grundrechtsschutz ist auch auf moderne Formen der Telekommunikation, bspw. Telefax, E-Mail, Mobilfunk, Pager etc. anzuwenden, weil das Grundrecht für neuere Entwicklungen offen ist[7]. Von dem Fernmeldegeheimnis sind sowohl Kommunikationsinhalte[8] als auch die näheren Kommunikationsumstände erfasst, insbesondere ob, wann und wie oft zwischen welchen Personen oder Fernmeldeeinrichtungen Fernmeldeverkehr stattgefunden hat oder versucht worden ist[9]. Dem durch Art. 10 Abs. 1 GG geschützten Fernmeldegeheimnis wird einfachgesetzlich durch die § 206 StGB, §§ 88ff, 91ff TKG (n.F.), § 5 AfuG (Amateurfunk) Geltung verschafft. Danach ist das unbefugte Eindringen in die Telekommunikation, die für die Telekommunikationsübertragung vorgehaltenen Einrichtungen und die Endgeräte für Telekommunikation ebenso wie die unbefugte Aufzeichnung und Verwertung erlangter Erkenntnisse daraus oder die sich daran anschließende Datenverarbeitung verboten.

Eingriffe in das Grundrecht auf ungestörte Telekommunikation sind zwar nach Art. 10 Abs. 2 GG aufgrund eines Gesetzes möglich. Solche Eingriffsnormen (bspw. die §§ 99 S. 1, 100b Abs. 3 S. 1, 100g Abs. 1 StPO) haben aber den Kernbestand des Grundrechtes zu gewährleisten. Die Reichweite des Grundrechtsschutzes aus Art. 10 Abs. 1 GG ergibt sich nach dem Urteil des BVerfG vom 2. März 2006 – 2 BvR 2099/04[10] aus der Dauer des Kommunikationsvorgangs. Der Schutz beginnt mithin bei der Aufnahme des Gespräches oder des Übermittlungsvorgangs. Er endet, wenn der Kommunikationsvorgang abgeschlossen ist, also die Nachricht bestimmungsgemäß am Endgerät des Empfängers angekommen ist[11]. Für die nach dem abgeschlossenen Kommunikationsvorgang verbleibenden Daten, d.h. vor allem Inhalts- und Verbindungsdaten, kann der Schutzbereich des Grundrechtes auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG betroffen sein. Der Schutz der Menschenwürde in der Privatsphäre umfasst das Recht des Einzelnen, von staatlicher Verfolgung „in Ruhe gelassen zu werden“, unbeobachtet Gespräche zu führen, seinen privaten Interessen nachzugehen und auch besonders private, vertrauliche Informationen mit den Empfängern eigener Wahl zu beliebigen Zeitpunkten und auf beliebigen Wegen auszutauschen. Dieses Recht gewährleistet nicht nur die Freiheit von staatlicher Beobachtung während eines solchen Tuns,

[6] BVerfGE 106, 28, 36 f.
[7] *Gercke* StV 2006, 453/455.
[8] BVerfGE 100, 313, 358; BFHE 194, 44.
[9] BVerfGE 67, 172; 85, 396; 100, 313, 358; BGHSt. 39, 335; KK-*Nack*, § 100a StPO, Rz. 2, 13.
[10] veröffentlicht im Internet unter www.bundesverfassungsgericht.de; NJW 2006, 976; dazu Anm. von *Gercke* StV 2006, 454; *Sachs* JuS 2006, 552; *Eckhardt* DuD 2006, 365; *Störing* CR 2006, 392; *Geis/Geis* K&R 2006, 279.
[11] so auch BGHSt. 42, 139/154; BGH NStZ 1997, 247; KK-*Nack*, a.a.O., Rz. 5,6.

sondern auch die Freiheit, eine abgeschlossene Handlung für sich zu behalten oder es nur eigenverantwortlich einem staatlichen Organ preiszugeben[12] Zu Recht wird im Übrigen im Urteil des Ersten Senats des BVerfG zur präventiven polizeilichen Telefonüberwachung ausgeführt, dass ein Zugriff auf solche Daten nur aufgrund eines hinreichend bestimmten Gesetzes erfolgen darf[13].

c) Das Urteil des BVerfG vom 2. März 2006[14] erlaubt eindeutige Zuordnungen für die auf einem Datenträger (d.h. bspw. Computerfestplatte, SIM-Karte oder Telefonspeicher, mobiler Datenträger) gespeicherten Datenbestände im Herrschaftsbereich des Betroffenen. Die über Telekommunikationswege versandten E-Mails werden während des Kommunikationsvorgangs vom Schutz des Art. 10 Abs. 1 GG erfasst. Für die auf dem persönlichen Computer oder einem sonstigen Endgerät empfangene E-Mail-Kommunikation ist deshalb mit dem BVerfG[15] und den Fachgerichten[16] davon auszugehen, dass der Kommunikationsvorgang erst beendet ist, wenn die Nachricht auf dem im Verfügungsbereich des Empfängers befindlichen Computer gespeichert ist. Nach Abschluss des Kommunikationsvorgangs sind die im Herrschaftsbereich des Empfängers verbleibenden Kommunikationsdaten, d.h. sowohl Inhalts- als auch Verbindungsdaten, durch das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützt. Mit dem Speichervorgang kann der Empfänger die Nachricht grundsätzlich vom unerlaubten Zugriff Dritter ausschließen, d.h. er kann sie „beherrschen“. Solche gespeicherten Datenbestände werden einem gegenstandsbezogen-sächlichem Verständnis folgend als Beweismittel im Sinne der §§ 94, 98 StPO angesehen.

2.)

Die Abgrenzung des Anwendungsbereichs des Art. 10 Abs. 1 GG vom Anwendungsbereich des Rechts auf informationelle Selbstbestimmung wirft Zweifelsfragen auf, wenn und soweit Daten „im Internet“ betroffen sind. Das „Internet“ ist ein nicht überschaubares, internationales Netzwerk[17], das aus den verschiedensten Großrechneranlagen, Betriebssystemen und Programmen besteht, die durch Telekommunikationsnetze miteinander verbunden sind. Für die „im Internet“ durch einen Kommunikationsvorgang anfallenden Datenbestände bestehen unterschiedlich weit reichende Zugangs-, Lese-, Bearbeitungs-, Speicher-, Kopier- und

[12] BVerfGE 110, 33, 52 f.
[13] BVerfGE 113, 348, 375 ff.
[14] Vgl. erneut BVerfG, NJW 2006, 976.
[15] BVerfGE 106, 28; 110, 33; BVerfG NJW 2005, 2603; NStZ 2005, 337.
[16] BGH NStZ 1997, 247; LG Hanau, StV 2000, 354 m. zust. Anm. *Dübbers*; LG Mannheim StV 2002, 242 m. zust. Anm. *Jäger* StV 2002, 244; LG Ravensburg CR 2003, 933.
[17] Unter Netzwerken werden Kabelnetze, Funknetze, Infrarotnetze etc. verstanden.

Löschungsrechte, die zugleich auch mehreren Personen und Unternehmen zustehen können.

a) Die Datenverwaltung „im Internet“ lässt sich trotz der Anlehnungen der Begriffe „E-Mail, Mailbox, Mailserver, Mail-Account“ an die herkömmlichen Erscheinungsformen des Briefverkehrs (Brief, Briefkasten, Postfach, postlagernde Sendung) nicht mit der Postbeförderung vergleichen. Die „im Internet“ kursierenden Daten sind Bestandteile einer weiterentwickelten Telekommunikation. An der Verwaltung dieser Netzwerke sind hauptsächlich gewerbliche Dienstleistungsunternehmen (sog. Provider)[18] beteiligt. Sie halten Speicherkapazitäten vor, vermitteln den Zugang dazu, verfügen über Datenzugriffsrechte und können Daten lesen, verändern, kopieren oder löschen.

b) Eine elektronische Kommunikation „im Internet“ löst verschieden abrufbare Daten aus, die sich wenigstens in Inhaltsdaten, Verbindungs-/Verkehrsdaten, Nutzungsdaten, Bestands-/Benutzerdaten, Zugangs- und Positionsdaten unterteilen lassen. E-Mails sind im Wesentlichen Inhaltsdaten, die zwischen den Kommunikationsteilnehmern ausgetauscht werden. Für den Empfang solcher E-Mails stellen Service-Provider[19] dem Individualkunden in der Praxis nur Verwaltungsrechte an einem Speichermedium (das ist das sog. „E-Mail-Account“) zur Verfügung, ohne selbst im sachenrechtlichen Sinne Eigentümer oder Besitzer dieses Speichermediums sein zu müssen.

Weder der Absender noch der Empfänger der E-Mail haben einen genauen Überblick darüber, welcher Übertragungsweg von dem jeweiligen Telekommunikationsunternehmen genutzt, über welche Netzwerke (Kabelnetze, Funknetzwerke, satellitengestützte Netze, Infrarotnetze etc.) welche Daten geleitet werden, welche Datenarten und Datenmengen dabei im Einzelnen entstehen und wie diese Daten ggf. vor unbefugtem Zugriff geschützt oder wie sie gelöscht werden können. So kann bspw. bereits im Verlauf einer ununterbrochenen Verbindung zwischen den Telekommunikationsteilnehmern wegen des Umfangs, des Übertragungsweges oder der fehlenden Kommunikationsfähigkeit der Endgeräte (bspw. unterschiedliche Betriebssysteme, E-Mailprogramme usw.) automatisch eine (von den Teilnehmern unbemerkte) Zwischenspeicherung stattfinden, um Datenverluste zu vermeiden. Man muss berücksichtigen, dass in keinem Fall einer Internet-Telekommunikation direkte

[18] Es werden Access-Provider (z.B. T-Online, AOL als Zugangsvermittler), Network-Provider (Deutsche Telekom, regionale Telefongesellschaften), Content-Provider (bspw. gewerbliche Internetshops, Onlinedienste) und Service-Provider (bspw. 1&1 Internet AG) unterschieden.

[19] Nach einhelliger Auffassung verwaltet der Service-Provider lediglich fremde Daten auf eigenen oder von ihm betriebenen Computern im Unterschied zum sog. Content-Provider, der eigene Inhalte auf von ihm betriebenen Computern für das Internet bereitstellt. Der Service-Provider gewährleistet in der Regel nicht den Netzzugang (Access-Provider) und bietet auch keine Übertragungswege an (Network-Provider); vgl. *Barton*, a.a.O., Rn. 77ff.; *Marberth-Kubicki*, a.a.O. Rn. 10ff.; *Malek*, a.a.O. Rn. 47ff..

Leitungsverbindungen zwischen den Teilnehmern bestehen. Auch wird die Nachricht nicht als „Einzelstück“ (etwa wie bei der Postbeförderung) verschickt, sondern sie wird in zahlreiche Datenpakete zerlegt, als Datenstrom durch verschiedene Leitungswege geschickt und erst bei der Empfangsadresse durch ein Transportprotokoll (bspw. TCP) wieder zusammengesetzt[20]. Bereits während der geöffneten Verbindung entstehen Datenpakete, die je nach Art und Umfang der Gesamtnachricht zwischengespeichert werden, ohne dass die Teilnehmer sich dessen bewusst sind. Lediglich die auf den persönlichen PC oder ein vergleichbares Endgerät herunter geladenen Daten können von dem Empfänger vollständig beherrscht, d.h. gelesen, bearbeitet oder gelöscht werden.

c) Die Daten- und Speicherverwaltung „im Internet“ obliegt unterschiedlichen Administratoren- und Benutzerrechten. Ein Service-Provider als Administrator räumt seinem Kunden vertraglich lediglich Benutzerrechte an dem „Account“ ein, das durch eine eindeutig zuordenbare Internetadresse definiert wird. Dadurch stehen dem Kunden keine umfassenden Zugriffs-, Lese-, Schreib-, Kopier- und Löschungsrechte an dem so von anderen Daten abgegrenzten Datenbestand zu, sondern hauptsächlich Lese-, Kopier- und Löschungsrechte. Anders als bei der Speicherung einer elektronischen Nachricht im Speicher des Endgerätes bleiben die Ausschließlichkeitsrechte bei dem Administrator. Ein Administrator kann selbst Löschungsanweisungen des Benutzers blockieren oder rückgängig machen. Von einer Kenntnis und dem Zugriff Unberechtigter schützen lediglich Zugangssperren und die Rechteverwaltung des Service-Providers.

d) Beim Abruf von E-Mails vom Mailserver des Service-Providers durch den Benutzer müssen wenigstens vier Wege unterschieden werden[21]:

(1) Der Benutzer eines Internetzugangs kann die von seinem Service-Provider verwalteten Nachrichten durch Öffnen der Internetverbindung auf dem Bildschirm „ansehen“. Man spricht hier von dem sog. „Webmail“, eine Konstellation, die der Verfassungsbeschwerde zugrunde liegt. Dabei werden die Daten zwar als Bestandteil des Internetbrowsers in den Arbeitsspeicher des Benutzer-Computers geladen, nicht aber auf eine Festplatte. Die im Mail-Account verwalteten Daten werden weiterhin von dem Service-Provider verwaltet.

[20] *Malek*, a.a.O., Rn. 23, wobei das Routenwahlprotokoll “IP“ nur von untergeordneter Bedeutung ist.
[21] Von drei Abrufvarianten spricht *Gercke*, StV 2006, 453.

(2) Es ist auch üblich, dass ein Programm dem Endgerät lediglich nur bestimmte Adressdaten[22] (sog. Header) mitteilt, ohne damit die E-Mail vollständig zu öffnen oder bereits zu speichern. Der Header stellt nur eine Benachrichtigung über den Eingang einer E-Mail in der Mailbox bzw. dem Mail-Account dar und ist mit einer SMS vergleichbar.

(3) Die für den Benutzer bestimmten E-Mails können auch von dem Service-Provider an den Mailserver eines lokalen Firmennetzwerks weitergeleitet und von dort eingesehen werden. Auch hier kann eine Nachricht auf dem lokalen Mailserver verbleiben, ohne dass der Benutzer die Nachricht auf der Festplatte seines persönlichen Computers abspeichert.

(4) Schließlich kann die E-Mail durch ein Mailprogramm auf den persönlichen Computer vollständig herunter geladen[23] und dort abgespeichert werden. Dieses Verfahren wird im Privatbereich häufig verwendet. In dieser Weise werden regelmäßig auch andere Endgeräte, bspw. moderne Mobilfunkgeräte zum Empfang von E-Mails eingesetzt. Der Anwender hat – ob ihm das bekannt ist oder nicht – regelmäßig auch die Möglichkeit, über den Verbleib von E-Mails auf dem Mailserver des Service-Providers zu entscheiden. Eine vergleichbare Konstellation lag dem Urteil des BVerfG vom 2. März 2006 zugrunde.

3.)

Die Grundrechte aus Art. 10 Abs. 1 GG bzw. aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG sind nicht abhängig von der in einem Einzelfall angewandten Technik, weil diese der Forschung und Entwicklung unterworfen ist[24]. Die multiplen Zugriffsmöglichkeiten auf die bei der Telekommunikation entstehenden Daten werfen die Frage auf, ob die bislang gefundene Abgrenzung nach dem Kriterium des „ausschließlichen Herrschaftsbereichs“ des Datenempfängers ausreicht, um den Schutzbereich des Art. 10 GG einerseits und den Schutzbereich des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG andererseits (Recht auf informationelle Selbstbestimmung) voneinander abzugrenzen..

[22] das sind mindestens Absender, Empfänger und Betreffzeile.
[23] In technischer Hinsicht handelt es sich um einen Kopiervorgang!
[24] Zur technischen Ausgestaltung der Übertragungswege vgl. beispielsweise *Barton*, Multimedia-Strafrecht, Neuwied 1999, Rn. 45ff, 57ff; *Marberth-Kubicki*, a.a.O., Rn 5ff..

a) Nur in den in Ziff. 2.d) (3) und (4) geschilderten Abrufvarianten befinden sich Daten im „ausschließlichen Herrschaftsbereich“ auf einem Datenträger des Empfängers. Die Abgrenzung nach diesem Kriterium führt in diesen Fallgruppen für die Strafverfolgungspraxis zu befriedigenden Ergebnissen, weil Gegenstand des strafprozessualen Zugriffs nur der jeweilige Datenträger ist, auf dem sich die tatsächlich abgespeicherten Daten befinden. In den Abrufvarianten der Ziff. 2.d) (1), (2) sowie in Variante (3) für die bei dem Service-Provider verbleibenden Inhaltsdaten liegen dagegen keine Daten im unmittelbaren Herrschaftsbereich des Empfängers vor.

b) Nicht tragfähig wäre eine Unterscheidung nach dem Kriterium der „**Wahrnehmbarkeit**“ oder der „**Kenntnis**“ vom Eingang einer Nachricht für den Empfänger. Dem stünde speziell in der unter Ziff. 2.d) (1) genannten Abrufvariante entgegen, dass das „Herunterladen“ in den Arbeitsspeicher des Personalcomputers und die Wahrnehmung am Bildschirm im Regelfall noch als zum einheitlichen Übermittlungsvorgang gehörend angesehen werden muss, auf den sich das Fernmeldegeheimnis insgesamt bezieht[25]. Auch in diesem Fall dürfen die Ermittlungsorgane dem seine E-Mails abfragenden PC-Benutzer also nur unter den besonderen Voraussetzungen, die für Art. 10 GG einschränkende Gesetze und ihre Anwendung gelten, gewissermaßen über die Schulter schauen.

c) Es wäre weiter zu erwägen, zwischen einem Datenbestand einerseits und einem Datenfluss **zu Zwecken der Telekommunikation** andererseits zu differenzieren**.** Da das Internet aus einer Vielzahl angeschlossener Netzwerkcomputer (bspw. auch in Firmennetzwerken, Intranet, Usernet etc.), Großrechneranlagen, Netzvermittlungsstellen und Personalcomputer mit jeweils unterschiedlichen Datenspeichern (Arbeitsspeicher, Festplattenspeicher, Speichersoftware, transportable Speichermedien etc.) besteht, unterliegt nicht automatisch jeder technische Bestandteil dieser Einrichtungen dem Schutzbereich des Art. 10 Abs. 1 GG, auf den nur entsprechend den §§ 100a ff. StPO zugegriffen werden könnte. Der Schutzbereich des Art. 10 Abs. 1 GG ist nur dann eröffnet, wenn die jeweiligen Einrichtungen den Telekommunikationsprozess durchführen, indem sie planmäßig in den Datenfluss eingebunden und als End- oder Zwischenspeicher die zu übertragenden Daten transportieren. In diesem Sinne ist auch nicht jeder Computer oder nicht jeder sonstige technische Speicher automatisch Teil des Telekommunikationsprozesses. Davon geht auch der Beschwerdeführer aus, wenn er die Wohnungsdurchsuchung und die damit

[25] BVerfGE 106, 28; BVerfG, NJW 2006, 976, 979.

verbundene Durchsuchung seines Personalcomputers nicht mit der Verfassungsbeschwerde angreift.

Zu einem Teil der durch Art. 10 Abs. 1 GG geschützten Telekommunikationsprozess gehören Personalcomputer des Absenders und des Empfängers nur für die Zeit und nur mit den Systemteilen, die die eigentliche Nachrichtenübertragung ausführen. Nach Abschluss des Datenflusses sind die jeweils ortsverschieden vorgehaltenen Geräte[26] wie Endgeräte der klassischen Telefone zu behandeln. Ebenso ist Bestandteil der Telekommunikation der jeweilige Übertragungsweg, der sich – mangels Beeinflussbarkeit der an der Telekommunikation Beteiligten - auf jede Leitung, Vermittlungsstelle und jeden Computer erstreckt, der nach dem Willen der mit der Telekommunikation gewerblich befassten Dienstleistungsunternehmen laufender Bestandteil des Übertragungsweges sein soll. Soweit während der Übertragung von Daten eine Zwischenspeicherung bei einem Access-, Network- oder Service-Provider stattfindet, erfolgt diese planmäßig aufgrund technischer Vorgaben und Notwendigkeiten. Ein Abschluss der Telekommunikation ist damit nicht beabsichtigt und auch in der Regel nicht verbunden. Ein Eingriff in solche Bestandteile der Telekommunikation während eines laufenden Kommunikationsvorgangs oder beim Dienstanbieter wegen Inhalts-, Verbindungs-, Zugangs- und Positionsdaten ist deshalb nur nach den §§ 100a ff., 100g ff. StPO zulässig.

Damit stellt sich die entscheidende Frage, ob nicht nur ein Datenspeicher, der bestimmungsgemäß als Endgerät fungiert (bspw. ein Personalcomputer in der Wohnung), sondern auch ein Datenspeicher, der gewissermaßen als externer Ersatz für ein solches Endgerät genutzt wird (bspw. ein Mailserver), nicht mehr zu den Telekommunikationseinrichtungen gehört, die an der übertragenden Telekommunikation teilnehmen. Verwaltet ein Service-Provider für den Benutzer E-Mail-Daten in einem eigens dazu bereit gestellten Datenspeicher (hier: einem Mailserver), so ließe sich argumentieren, dann sind die derart nicht zur weiteren Durchleitung bestimmten Daten nicht mehr Bestandteil der übertragenden Telekommunikation, sondern Teil der Lebensführung des Benutzers. Zwar verfügt dieser nicht über Ausschließlichkeitsrechte an diesem Datenbestand; die mittels Account verwalteten Daten haben aber ihre Endbestimmung erreicht, sie sind – wie bei einem Anrufbeantworter - an der Adresse des Benutzers angekommen.

[26] KK-*Nack* § 100a StPO Rz. 8; LR-*Schäfer* § 100a StPO Rz. 58; *Beulke*, StPO, 9. Aufl. 2006, Rn. 253; *Lührs* wistra 1995, 19; *Bär* CR 1995, 489, 495; *Palm/Roy* NJW 1996, 1791; *Marberth-Kubicki*, a.a.O. Rn. 193f, 195, 266; *Malek* a.a.O. Rz, 372f.; *Jahn*, JuS 2006, 491.

Diese Gleichsetzung des Datenbestandes auf dem Endgerät und auf dem E-Mail-Account würde jedoch vollkommen den Umstand ausblenden, dass der Empfänger – mit Ausnahme des ihm vertraglich eingeräumten Zugriffs auf die für ihn vom Provider verwalteten E-Mails – ansonsten keinerlei Kontroll- und insbesondere Ausschließlichkeitsrechte bezüglich „seines“ Datenbestands hat. Dahingehende Rechte und Pflichten hat vielmehr ausschließlich der TK-Dienstleister, wie sich aus den §§ 110 – 115 TKG i.V.m. der TelekommunikationsüberwachungsVO (TKÜV) ergibt; das gilt auch und gerade im Blick auf die Eingriffs- und Überwachungsbefugnisse der Ermittlungs- und Sicherheitsbehörden. Es sind aber gerade, wie das BVerfG in seinem Beschluss v. 2.3.2006 mit allem Nachdruck noch einmal deutlich gemacht hat[27] die Herrschaftssphäre des Empfängers einerseits und die Offenheit des Übermittlungsvorgangs andererseits, die in dem einen Fall zwar den Schutz des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) genügen lassen, in dem anderen Fall aber den weitergehenden, bereichspezifischen Schutz durch das Fernmeldegeheimnis (Art. 10 GG) gebieten. Deshalb führt kein Weg daran vorbei, auch noch die Speicherung bzw. Verwaltung der E-Mails auf dem Mailserver des TK-Dienstleisters dem Übermittlungsvorgang zuzuordnen, und zwar grundsätzlich unabhängig davon, ob der Empfänger sie bereits abgerufen hat oder nicht.

4.)

Selbst wenn man aber die Datenbestände auf dem E-Mail-Account eines Providers genauso wie die auf dem PC des Empfängers gespeicherten E-Mails nur dem Schutz des Grundrechts auf informationelle Selbstbestimmung für E-Mails unterstellen würde[28], stellte sich die in dem mehrfach zitierten Urteil des BVerfG vom 2. März 2006 (im Falle der auf dem Empfänger-PC gespeicherten E-Mails) noch bejahte Frage, ob die Eingriffsnormen der §§ 102, 103, 94, 98 StPO für derartige strafprozessuale Zugriffe geeignet sind, den Kernbereich des Grundrechts zu gewährleisten.

Die strafprozessualen Eingriffsbefugnisse der §§ 94ff, 102f, 163 StPO sind bislang nicht umfassend an die fortschreitende technische Entwicklung in der Telekommunikation und die Entwicklung des Internet angepasst worden. Lediglich zur Ablösung des § 12 FAG sind für Verbindungs- und Positionsdaten spezielle Eingriffsermächtigungen in den §§ 100g-i StPO geschaffen worden. Die Ermächtigungen in den §§ 102, 103 StPO betreffen lediglich sachliche Gegenstände,

[27] NJW 2006, 976, 978 f.
[28] So etwa Löffelmann, AnwBl 2006, 598, 599 f. unter gleichzeitigem Hinweis auf die davon abweichenden Auffassungen in Lit. u. Rspr. (Fn 37).

nicht aber Rechte, Augenscheinsobjekte und Internet-Daten. Dem gleichen sachbezogenen Verständnis folgen die §§ 94ff StPO. Die §§ 100a ff StPO sind zwar geeignete Eingriffsgrundlage für die Inhalte von Telekommunikation, gleichwohl erfasst der Wortlaut dieser Regelungen nicht die Ablage von Inhaltsdaten in einem nicht vom Benutzer beherrschten Computernetz, auch wenn die Ablage über das Ende eines Telekommunikationsvorgangs hinausreicht. Die Suche, Sichtung und das Kopieren von Daten, die im Internet von Service-Providern empfängerbezogen verwaltet und i.d.R. durch Zugangssperren gesichert sind, wird von den §§ 94ff, 102f StPO nicht erfasst.

Bislang behilft sich die Rechtsprechung mit der nur entsprechenden Anwendung von Eingriffnormen, um Strafverfolgungslücken zu vermeiden. Im vorliegenden Verfahren wird die Schwierigkeit eines sachgerechten Eingehens auf die technischen Abläufe, die Zugangsrechte zu Datenbeständen und die strafprozessuale Behandlung von (abgestuften) Verwaltungsrechten an solchen Daten deutlich. Auch wegen der mitunter tiefgreifenden staatlichen Eingriffe in persönliche und betriebliche Geheimnisse müssen Eingriffsnormen für den Zugriff auf, die Durchsicht und das dauerhafte Speichern von internetbasierten Inhaltsdaten geschaffen werden, um in rechtsstaatlicher Weise Eingriffsgrundlage, Eingriffsintensität und Eingriffsdauer vorhersehbar und nachvollziehbar zu machen. Das gilt insbesondere auch für die für den Umfang und für die Modalitäten des vom BVerfG in seinem Urteil vom 3.3.2004 zum sog. großen Lauschangriff[29] insoweit entwickelten und in der Entscheidung des BVerfG vom 27.7.2005 zur vorbeugenden (polizeilichen) Telefonüberwachung[30] wieder aufgegriffenen „Kernbereichsschutz“[31].

Da bisher solche Regelungen nicht bestehen, wäre die Verfassungsbeschwerde auch dann begründet, wenn „nur“ eine Verletzung des Rechts auf informationelle Selbstbestimmung in Frage kommen sollte.

5.)

Schließlich bestehen grundsätzliche Bedenken gegen die Auffassungen des AG Braunschweig, des LG Braunschweig und des Nds. Justizministeriums, über die Reichweite des Eingriffs in einen E-Mail-Datenbestand. Selbst (nur) gemessen an dem Schutzbereich des Grundrechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und dem Verhältnismäßigkeitsprinzip hätten weder eine begründungslose umfassende „Beschlagnahme des E-Mail Account“ (Beschlüsse des AG Braunschweig vom 14.03.2006 und 22.03.2006, des LG Braunschweig vom 18.04.2006) noch eine schrankenlose, nach formelhaften, nur eine Scheinbegrenzung

[29] BVerfGE 109, 279, 318 ff.
[30] BVerfGE 113, 348, 390.
[31] Vgl dazu erneut Löffelmann, AnwBl 2006, 598, 601.

darstellenden Suchbegriffen kaum eingeschränkte Beschlagnahme aller E-Mails des Beschwerdeführers in der Datenbank des Service-Providers beschlossen werden dürfen.

a) Eine gegenständliche Herrschaftsmacht des Account-Inhabers an dem durch den Service-Provider verwalteten Datenbestand besteht nicht. Die den Beschlüssen des AG Braunschweig und des LG Braunschweig[32] zugrunde liegende Vorstellung, das „Account“ könne mit einem Postfach oder Schließfach gleichgesetzt werden und die ankommenden E-Mails wären auf einem dauerhaften Speichermedium „gespeichert“, entspricht –wie oben erläutert- nicht den Vereinbarungen und der Technik, die bei der Verwaltung von Inhaltsdaten „im Internet“ angewendet wird. Das Internet-Account stellt nur einen über Telekommunikationsleitungen zugänglichen, nach Benutzermerkmalen abgegrenzten Datenspeicher dar. Die technische Ausgestaltung als Festplattenspeicher ist nicht zwingend. Herrschafts- und Verwaltungsrechte an diesem Datenbestand haben neben dem Benutzer mindestens auch der Service-Provider und alle Personen, die erlaubt im Besitz der Zugangsdaten sind.

b) Da der Service-Provider mit Hilfe des Accounts die für den Benutzer eingehenden Daten verwaltet, lässt sich ein solcher Datenbestand durch eine gegen den Service-Provider (als Administrator) gerichtete Ermittlungsmaßnahme sicherstellen. Da der Datenbestand aber weit umfangreicher ist, als dies für den jeweiligen Untersuchungszweck benötigt wird, haben die Ermittlungsorgane durch geeignete, praktikable und wirksame, den Betroffenen geringstmöglich belastende Maßnahmen eine Vorauswahl zu treffen. Mit dieser einschränkenden Auswahl kann der Datenbestand gesichtet werden. Erst die durch die Sichtung tatsächlich als verfahrensrelevant erkannten Daten können einem dauerhaften strafprozessualen Zugriff, d.h. einem Kopieren für Zwecke des Ermittlungsverfahrens, unterworfen werden.

Das BVerfG hat im Beschluss vom 12. April 2005 – 2 BvR 1072/02- zur Bedeutung des Verhältnismäßigkeitsprinzips bei der Beschlagnahme eines Datenbestandes zutreffend ausgeführt, dass der Ermittlungsrichter eine verfahrensbezogene Konkretisierung der gesuchten Daten bereits im Durchsuchungsbeschluss zu treffen hat[33]. Eine strenge Begrenzung des staatlichen Zugriffs auf den Ermittlungszweck sei zur Bestimmung des Eingriffs erforderlich. Der Senat führt aus[34]:

[32] und auch dem des LG Bonn, wistra 2005, 76.
[33] BVerfGE 113, 29.
[34] BVerfGE 113, 29, 53.

> Die besondere Eingriffsintensität des Datenzugriffs ergibt sich daraus, dass die strafprozessuale Maßnahme wegen der Vielzahl verfahrensunerheblicher Daten eine Streubreite aufweist und daher zahlreiche Personen in den Wirkungsbereich der Maßnahme mit einbezogen werden, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben (vgl. BVerfGE 100, 313 <380>; 107, 299 <320 f.>).

Zur Durchsetzung nur geeigneter, mit der jeweils geringsten Eingriffsintensität verbundener Konkretisierungen fordert der Beschluss:

> Dem staatlichen Handeln werden durch den Grundsatz der Verhältnismäßigkeit Grenzen gesetzt. Die Sicherstellung und Beschlagnahme der Datenträger und der darauf gespeicherten Daten muss nicht nur zur Verfolgung des gesetzlichen Strafverfolgungszwecks Erfolg versprechend sein. Vor allem muss gerade die zu überprüfende Zwangsmaßnahme zur Ermittlung und Verfolgung der Straftat erforderlich sein; dies ist nicht der Fall, wenn andere, weniger einschneidende Mittel zur Verfügung stehen. Schließlich muss der jeweilige Eingriff in einem angemessenen Verhältnis zu der Schwere der Straftat und der Stärke des Tatverdachts stehen (vgl. BVerfGE 96, 44 <51>).

(Auch) diesen Anforderungen werden die mit der Verfassungsbeschwerde angegriffenen Beschlüsse, wie der Beschwerdeführer im Einzelnen nachvollziehbar darlegt, nicht gerecht.

- - -