Dr. Jürgen-Peter Graf
Richter am Bundesgerichtshof

76133 Karlsruhe
Herrenstraße 45a
Telefon: 0721-159-0
www.internet-strafrecht.de

Stellungnahme zur öffentlichen Anhörung des Rechtsausschusses des Deutschen Bundestages am 19. September 2007 in Berlin

zum Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BT-Drs. 16/5846)

sowie zum Entwurf eines Gesetzes zur Reform der Telekommunikationsüberwachung der Fraktion BÜNDNIS 90/DIE GRÜNEN (BT-Drs. 16/3827)

I. Allgemeines

Bedingt durch die rasanten technischen Fortschritte im gesamten Bereich der Telekommunikation, insbesondere den seit etwa 15 Jahren stark zunehmenden Telekommunikationsverkehr über die Mobilfunknetze sowie den ebenfalls nahezu explosionsartig gewachsenen Datenaustausch über und unter Benutzung des Internets, war der Gesetzgeber in den letzten zehn Jahren mehrfach veranlasst, sowohl gesetzliche Neuregelungen zu beschließen, als auch bestehende gesetzliche Regelungen anzupassen. Dies gilt nicht zuletzt für die Zulässigkeit und den Umfang strafprozessualer Ermittlungsmaßnahmen sowie die hierzu erforderlichen Auskunfts- und Mitwirkungsverpflichtungen von Telekommunikationsdienstleistern. Als Folge dieser jeweils notwendigen gesetzlichen Änderungen und Ergänzungen ergibt sich heute ein nur schwer zu durchschauendes Geflecht von Bestimmungen, welche die Eingriffsbefugnisse und -schranken im Rahmen von strafrechtlichen Ermittlungen regeln. Dabei sind nicht nur die Eingriffsschwellen teilweise unterschiedlich ausgestaltet; auf Grund der Vielschichtigkeit einzelner Dienste müssen beispielsweise bei der Überwachung einer DSL-Verbindung ggf. unterschiedliche gesetzliche Anordnungsgrundlagen geprüft und herangezogen werden.

Wie auch im Gesetzentwurf der Bundesregierung ausgeführt, besteht daher ein erheblicher Bedarf dafür, die Voraussetzungen strafprozessualer Ermittlungsmaßnahmen entsprechend ihrer jeweiligen Eingriffstiefe zu harmonisieren und dabei auch die rechtsstaatlichen Erfordernisse zu berücksichtigen, wie diese in der jüngsten Rechtsprechung des Bundesverfassungsgerichts ihren Ausdruck gefunden haben.
Die vorgeschlagenen gesetzlichen Änderungen vermögen die Zielvorgabe teilweise zu erreichen, teilweise werden aber bestehende Rechtsprobleme ohne Not offen gelassen und bleiben damit notwendigerweise einer Entscheidung durch die Rechtsprechung als "Ersatzgesetzgeber" überlassen. Die Fülle der teilweise auf einen Sachverhalt anzuwendenden Vorschriften wird künftig wohl ebenso erhalten bleiben wie die Notwendigkeit, für die Überwachung nur eines

einzigen Beschuldigten teilweise zehn oder mehr Überwachungsanordnungen zu erlassen.

Die nachfolgende Stellungnahme beschränkt sich auf einzelne, besonders herauszuhebende Änderungsvorschläge, welche in ihren Auswirkungen für die Praxis, die Ermittlungsbehörden sowie die Rechtsprechung bedeutsam erscheinen sowie auf einige wenige Fragen, welche im vorliegenden Gesetzentwurf der Bundesregierung nicht angesprochen sind, jedoch regelungsbedürftig erscheinen.

II. Zu den einzelnen Änderungsvorschlägen

1. § 53b StPO-E

Die geplante Neuregelung eines Beweiserhebungs- und -verwertungsverbots für Erkenntnisse, die vom Zeugnisverweigerungsrecht eines Geistlichen, Verteidigers oder Abgeordneten im Sinne von § 53 Abs. 1 Satz 1 StPO umfasst sind, erscheint insgesamt sachgerecht und dürfte die verfassungsrechtlichen Vorgaben erfüllen. Soweit allerdings für die Anwendung der sog. Verstrickungsregelung in § 53b Abs. 4 Satz 1 StPO-E, welche zur Nichtanwendbarkeit von § 53b Abs. 1 bis 3 StPO-E führt, die Einleitung eines Strafverfahrens gegen die zeugnisverweigerungsberechtigte Person verlangt wird, ist dies abzulehnen. Der Bundesrat hat bereits in seiner Stellungnahme darauf hingewiesen, dass es nach den gesetzlichen Vorgaben der §§ 151 f. StPO keinen formalen Akt der Einleitung eines Ermittlungsverfahrens gibt. Vielmehr beginnt ein Ermittlungsverfahren in aller Regel dadurch, dass die zuständige Staatsanwaltschaft den Anfangsverdacht einer Straftat gegen einen Beschuldigten bejaht und zeitgleich entsprechende Registereinträge veranlasst und ein Aktenzeichen für das Verfahren vergibt. Somit ist die im Regierungsentwurf erhoffte Sensibilisierung der Ermittlungsbehörden durch das Erfordernis der Einleitung eines Ermittlungsverfahrens eher nicht zu erwarten. Daher erscheint es im Sinne einer einheitlichen Systematik der Regelungen der Strafprozessordnung sinnvoll und ge-

boten, entsprechend der gleichartigen Regelungen in § 97 Abs. 2 Satz 3 und § 100c Abs. 6 Satz 3 StPO auch in § 53b Abs. 4 Satz 1 StPO-E darauf abzustellen, ob der Berufsgeheimnisträger der Beteiligung oder einer Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist. Verfassungsrechtliche Bedenken bestehen insoweit nicht, zumal nicht einmal der noch weitaus schwerwiegendere Eingriff des Erlasses eines Haftbefehls an die Einleitung eines Ermittlungsverfahrens sondern an das Bestehen eines dringenden Tatverdachts gebunden ist.

2. § 100a StPO-E

Auch wenn die Überlegungen in dem Gesetzentwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN durchaus erwägenswert erscheinen, anstelle des bisherigen Straftatenkatalogs einen allgemeinen Katalog mit Kriterien einzuführen, welche sich im Wesentlichen an der Mindesthöchststrafe eines Delikts orientieren, reicht dies nicht hin, um alle Delikte zu erfassen, für deren Verfolgung Telekommunikationsüberwachung eine zulässige und gebotene Ermittlungsmaßnahme sein kann. Somit erscheint die Beibehaltung des Straftatenkatalogs, wie auch im vorliegenden Regierungsentwurf vorgeschlagen, letztlich vorzuziehen, weil hierdurch auch eine den verfassungsmäßigen Vorgaben eher entsprechende "Feinsteuerung" bei den in Betracht kommenden Straftaten vorgenommen werden kann.

Dementsprechend sollte aber auch die im Regierungsentwurf vorgesehene Streichung der Vergehen nach § 86 StGB sowie § 20 Abs. 1 VereinsG unterbleiben. Zwar ist die Verbreitung von Propagandamitteln in verfassungswidriger Organisation nach § 86 StGB nur mit einer Höchstfreiheitsstrafe von drei Jahren bedroht, jedoch erscheint es dringend erforderlich, gerade im Hinblick auf die jüngst wieder aufgekommenen Diskussionen um die Verbreitung von NS-Propagandamitteln sowie die Zugänglichmachung über das Internet (vgl. Fall Zündel) die Telekommunikationsüberwachung zur Ermittlung von Tätern weiterhin zuzulassen. Der Umstand, dass eine Strei-

chung des § 86 StGB im Straftatenkatalog des § 100a StPO im Ausland sicherlich Beachtung finden würde, sollte hierbei ebenfalls Berücksichtigung finden.

Auch die Streichung des § 20 VereinsG im Straftatenkatalog des § 100a StPO sollte unterbleiben. Die Vorschrift des § 20 VereinsG lässt allein eine wirksame Möglichkeit, auf die Einhaltung eines Vereinsverbots hinzuwirken. Dies betrifft vor allem die in den letzten zwei Jahrzehnten erlassenen Vereinsverbote gegen rechtsextremistische Gruppierungen sowie verbotene Strukturen der PKK sowie weiterer im Wesentlichen vom Ausland gesteuerter Vereinigungen. Da aber gerade verbotene Gruppierungen sich regelmäßig noch stärker nach außen abschotten, lässt sich die Einhaltung des Verbots regelmäßig nur dadurch kontrollieren, dass bei Personen, welche der Zuwiderhandlung gegen das Vereinsverbot verdächtig sind, die Telekommunikation in eine Überwachung mit einbezogen wird. Würde § 20 VereinsG aus dem Straftatenkatalog gestrichen, bliebe den Ermittlungsbehörden meist nur die Einschleusung von Personen in diese Gruppierungen, um den Sachverhalt weiter aufzuklären, was jedoch u.U. mit erheblichen Gefahren für Gesundheit und Leben der eingesetzten Personen verbunden wäre.

3. § 100b StPO-E

a) Zweifel bestehen hinsichtlich der ins Auge gefassten Reduzierung der Dauer der Überwachungsanordnung von drei auf zwei Monate. Diese kann zu einem erheblichem Mehraufwand für die Gerichte führen, welcher jedenfalls mit der im Regierungsentwurf gegebenen Begründung kaum zu rechtfertigen ist. Wenn nämlich die rechtstatsächlichen Untersuchungen ergeben haben, dass eine Vielzahl der Telekommunikationsmaßnahmen allenfalls bis zu zwei Monaten durchgeführt und innerhalb dieses Zeitraumes dann offenbar auch beendet worden sind, ergibt sich daraus nur allzu deutlich, dass die Staatsanwaltschaften der ihnen

übertragenen Aufgabe, eine Überwachungsmaßnahme zu beenden, sobald sie nicht mehr erforderlich ist, sehr gut nachkommen. Hieraus den Schluss zu ziehen, dann Maßnahmen überhaupt nur noch für die Dauer von zwei Monaten zuzulassen, würde das Vertrauen in die offensichtlich objektive Arbeit der Staatsanwaltschaften konterkarieren. Im Gegenteil führt die durch den Regierungsentwurf beabsichtigte verkürzte Fristenregelung dazu, dass dann die weiteren Verfahren, welche länger als zwei Monate Überwachungsdauer benötigen, automatisch mittels der Folgeanordnung möglicherweise vier Monate überwacht werden anstelle von drei Monaten Dauer bei einer Überwachungsanordnung nach geltendem Recht.

Ob die weiterhin vorgesehene Übertragung des Erlasses weiterer Verlängerungsanordnungen ab sechsmonatiger Dauer einer Maßnahme auf das im Rechtszug übergeordnete Gericht, somit meist das Landgericht, die Gewähr für eine "bessere" Kontrolle bietet, erscheint zumindest nicht gesichert. Für die dann zuständigen Kammern handelt es sich um eine zusätzliche Mehraufgabe, welche zudem gerade bei Verfahren, in denen die Überwachungsanordnungen bereits sechs Monate oder länger dauern, regelmäßig erheblichen Einarbeitungsaufwand benötigen - ein Zeitaufwand, welcher neben den vielfältigen Rechtssprechungsaufgaben kaum zu bewältigen ist.

b) Das in § 100b Abs. 1 Satz 2 StPO-E vorgesehene Beweisverwertungsverbot von Daten, welche infolge einer Eilanordnung der Staatsanwaltschaft erlangt worden sind und bei der das erkennende Gericht später zur Auffassung gelangt, die für die Eilanordnung erforderliche Gefahr im Verzug habe nicht bestanden, erscheint wenig praktikabel und zudem in ihren Auswürdigungen fragwürdig. Allein die für diese Fallgestaltung eingeräumte Möglichkeit eines Beweisverwertungsverbots muss jeden Verteidiger pflichtgemäß zu dem Versuch veranlassen, das Vorliegen von Gefahr im Verzug bei Erlass der Eilanordnung in der späteren Hauptverhandlung auf jede mögliche Art und Weise zu widerlegen und

entsprechende Beweisanträge zu stellen. Dass in einem solchen Fall - entgegen dem Beschleunigungsgrundsatz - Verfahren unter Umständen erheblich verlängert, wenn nicht gar verschleppt werden, liegt auf der Hand. Zum anderen wird es für viele Bürger kaum nachvollziehbar sein, wenn ein Täter, welcher unmittelbar nach der Tat diese bei einem Telefonat gestanden hat, im Übrigen aber keine Angaben zur Sache (mehr) macht, deswegen freizusprechen ist, weil der Inhalt dieses Telefonats nicht verwertbar ist - wenn z.B. der Staatsanwalt bei Antragstellung übersehen hat, dass neben dem nicht erreichbaren zuständigen Ermittlungsrichter auch noch ein weiterer Kollege als dessen Vertreter im Gericht anzutreffen gewesen wäre. Allein die Gefahr, dass später sich solch ein Irrtum herausstellt und damit Beweismittel nicht verwertbar wären, wird dazu führen, dass Staatsanwälte eher die Antragstellung und damit den Beginn einer Überwachungsmaßnahme hinauszögern als in dringenden Fällen das Vorliegen von Gefahr im Verzuge zu bejahen. Keiner Erwähnung bedarf es insoweit, dass in Fällen willkürlicher Annahme der Voraussetzungen einer Eilanordnung die vorgenannten Überlegungen keine Gültigkeit haben und hier ein Verwertungsverbot angebracht ist, im Übrigen auch von der Rechtsprechung ohnehin wohl bejaht werden würde.

c) Die weiterhin vorgeschlagene Benennung des Endzeitpunktes in einer Anordnung fördert zwar die Klarheit und exakte Fristberechnung, berücksichtigt jedoch nicht die tatsächlichen Gegebenheiten und Schwierigkeiten bis zur Schaltung einer Maßnahme - beispielsweise an Wochenenden. Dabei lässt sich auch bislang schon infolge der Mitteilungen der Telekommunikationsdienstleister stets feststellen, ab welchem Zeitpunkt die Maßnahme begonnen wurde, sodass deren Ende leicht berechenbar ist. Zudem stehen schon bei der gegenwärtigen Gesetzeslage die Ermittlungsrichter zutreffend auf dem Standpunkt, dass sog. Vorratsbeschlüsse nicht zulässig sind und daher eine Überwachungsmaßnahme spätestens innerhalb von drei bis fünf Tagen zu beginnen hat. Diese Auslegung der aktuellen Vorschriften ermöglicht dann aber auch

in schwierigen technischen Umgebungen eine frühzeitige Vorbereitung und einen pünktlichen Beginn der Überwachungsmaßnahme.

d) Soweit schließlich in § 100d Abs. 4 Satz 2 StPO-E festgelegt werden soll, dass nach Beendigung einer Maßnahme das anordnende Gericht über den Verlauf und die Ergebnisse zu unterrichten ist, mag dies einer so beabsichtigten Erfolgskontrolle dienen. Eine solche ist aber von Verfassungs wegen nicht veranlasst und zudem den jeweils am einzelnen Sachverhalt orientierten Anordnungen nicht angemessen. Indem Straftaten und Strafverfahren keinem vorgegebenen Muster folgen, wird weder ein mit der Sache befasster Richter noch der zuständige Staatsanwalt voraussagen können, welchen Inhalt etwa aufgezeichnete Telefonate haben werden. Allein aus dem Umstand, dass möglicherweise zwei Anordnungen ohne Erfolg geblieben sind, lässt sich nicht vorhersagen, dass auch die dritte Anordnung keine Ergebnisse bringen wird. Letztlich wird die Unterrichtung des Gerichts nur einen Mehraufwand für den zuständigen Dezernenten der Staatsanwaltschaft mit sich bringen, welcher im Ergebnis dazu führt, dass ihm die hierfür erforderliche Zeit fehlen wird, um entsprechend des Beschleunigungsgrundsatzes die abschließende Entscheidung in dem zugrunde liegenden Verfahren entweder im Sinne einer Einstellung oder aber gerichtet auf eine Anklage schnellstmöglich zu treffen.

4. § 100g StPO-E

Während § 100a StPO die Aufzeichnung und Erhebung von Kommunikations- bzw. Inhaltsdaten betrifft, soll § 100g StPO-E künftighin allgemein die Erhebung von **Verkehrs**daten regeln. Aus Sicht der Rechtsprechung und insbesondere aus ermittlungsrichterlicher Sicht scheinen in dieser neu gestalteten Vorschrift sowohl die Interessen der Strafverfolgungsbehörden wie auch der von Anordnungen Betroffenen ausreichend gewichtet. Die in der Vorschrift aufgeführten Beschränkungen einzelner Sachverhalte entspre-

chen, soweit ersichtlich, dem Verhältnismäßigkeitsgrundsatz und den zu beachtenden verfassungsrechtlichen Anforderungen. Besonders wichtig für die Praxis der Aufklärung und damit zugleich auch der Vermeidung künftiger Straftaten ist die Beibehaltung der Anordnungsbefugnis bei Sachverhalten, bei denen eine Straftat mittels Telekommunikation begangen wurde (§ 100g Abs. 1 Satz 1 Nr. 2 StPO-E). Gerade die zunehmende Internetkriminalität kann hierdurch leichter aufgeklärt werden, sofern die Erhebung der Daten überhaupt in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Ob diese Voraussetzungen im Einzelnen vorliegen, wird Tatfrage sein; jedoch könnte gerade bei Betrugstaten, unter Berücksichtigung des in § 263 Abs. 4 StGB enthaltenen Verweises auf § 248a StGB, eine Datenerhebung möglicherweise bereits dann für zulässig gehalten werden, wenn es sich nicht um Schäden im Bereich der Geringwertigkeit handelt.

5. § 101 StPO-E

Die in § 101 Abs. 4 vorgeschlagene Konkretisierung der Benachrichtigungspflichten hinsichtlich der Betroffenen und sonstigen Beteiligten, abhängig von der jeweiligen Maßnahme, stellt eine erhebliche Erleichterung für die Praxis dar. Zudem werden bislang offene Streitfragen gerade im Zusammenhang mit den Regelungen in § 101 Abs. 4 Satz 3 und 4 StPO-E eher zu lösen sein. Dies gilt vor allem, wenn beispielsweise ein Betroffener mit seinem Friseur oder der Autowerkstatt einen Termin abspricht und diese Gesprächspartner nach der bislang geltenden Regelung darüber hätten unterrichtet werden müssen, dass ihr Telefonat überwacht worden war. Gerade wenn ein Tatverdacht sich nicht bestätigt und der Betroffene etwa „nur“ als möglicher Nachrichtenmittler überwacht worden wäre, könnte eine solche Benachrichtigung zu Lasten des Betroffenen zumindest erheblichen gesellschaftlichen Schaden herbeiführen. Auch die Regelung in § 101 Abs. 4 Satz 5 StPO-E, wonach Nachforschungen zur Feststellung der Identität einer grundsätzlich zu benachrichtigenden Person nur in bestimmten Fällen

vorzunehmen sind, entspricht der bisherigen Praxis und beseitigt eine derzeit noch vorhandene Grauzone.

6. § 110 Abs. 3 StPO-E

Eine wichtige Klärung der bislang umstrittenen Frage, ob im Rahmen einer offenen Durchsuchung auch auf räumlich vom Durchsuchungsort getrennte Speichermedien zugegriffen und die Durchsuchung darauf erstreckt werden kann, ergibt sich nach der in § 110 Abs. 3 StPO-E enthaltenen Ermächtigung. Allerdings betrifft diese Regelung zunächst nur die Daten, die im Bereich der Bundesrepublik Deutschland (an anderen Orten als dem Durchsuchungsort) abgespeichert sind.

7. § 162 StPO-E

Die im Gegensatz zur bisherigen Rechtslage nunmehr vorgesehene Konzentrationsregelung für Antragstellungen der Staatsanwaltschaft bei dem Amtsgericht, in dessen Bezirk die jeweilige Staatsanwaltschaft ihren Sitz hat, kann zu einer nicht unerheblichen Vereinfachung und Beschleunigung von Untersuchungshandlungen führen. Allerdings besteht gerade im Bereich von Anordnungen gegen Telekommunikationsprovider die Gefahr, dass künftighin - abhängig vom jeweiligen Landgerichtsbezirk - differierende Entscheidungen ergehen. Dies wurde bislang dadurch vermieden, dass solche Anträge allesamt dort zu stellen und zu entscheiden waren, wo der Provider oder die entsprechende technische Abteilung des Providers ihren Sitz hatte, was jedoch eine erhebliche Arbeitsbelastung für das betroffene Amtsgericht mit sich brachte. Es wird daher bei der künftigen Regelung Aufgabe der Staatsanwaltschaften und Generalstaatsanwaltschaften sein, schon frühzeitig bei entsprechenden Streitfragen auf die Herbeiführung obergerichtlicher Entscheidungen anzutragen.

8. Auskunft über den Inhaber einer dynamischen IP-Adresse

In der Begründung des Regierungsentwurfs wird ausgeführt, dass im Hinblick auf Auskunftsersuchen nach dem Inhaber einer dynamischen IP-Adresse eine klarstellende Regelung in § 113 TKG erwogen wurde, eine solche Regelung jedoch aufgrund einer "inzwischen gefestigten und zutreffenden Rechtsprechung" nicht mehr erforderlich sei. Der Begründung des Regierungsentwurfes ist insoweit zuzustimmen, dass ein solches Auskunftsersuchen richtigerweise auf § 113 TKG gestützt werden kann und dabei nicht die Voraussetzungen nach §§ 100g, 100h StPO zu erfüllen sind. Nicht zuzustimmen ist der Begründung des Regierungsentwurfes dagegen, dass es eine eindeutige oder vielleicht gar bundeseinheitliche Rechtsprechung zu dieser Problematik gibt. Gerade große Mengen von Strafanzeigen wegen Verstößen gegen urheberrechtliche Regelungen im Zusammenhang mit Tauschbörsen und anderen Möglichkeiten, über das Internet urheberrechtlich geschütztes Ton- und Bildmaterial ohne Erlaubnis des Berechtigten zu erlangen, haben dazu geführt, dass auf verschiedene Art und Weise versucht wird, solchen Massen-Anzeigen (mit dem faktischen Ziel einer Auskunftserlangung zur weiteren Verfolgung zivilrechtlicher Ansprüche) Einhalt zu gebieten. Ein Möglichkeit bestünde darin, Auskunftsersuchen hinsichtlich des Inhabers einer dynamischen IP-Adresse in Voraussetzungen nach §§ 100g, 100h StPO zu unterwerfen. Einen entsprechenden Beschluss hat beispielsweise das Amtsgericht Offenburg vom 20. Juli 2007 (4 Gs 442/07) erlassen, welcher allerdings noch nicht rechtskräftig ist. Über die eingelegte Beschwerde hat das zuständige Landgericht noch nicht entschieden. Wie Meldungen der Fachpresse hier zu entnehmen ist, haben sich daraufhin bundesweit zahlreiche Staatsanwaltschaften um den vorgenannten Beschluss bemüht, um in ihrem Zuständigkeitsbereich ähnliche Entscheidungen herbeizuführen. Daher besteht in dieser Frage die Gefahr einer Rechtszersplitterung. Eine obergerichtliche Entscheidung durch den Bundesgerichtshof ist in naher Zukunft nicht zu erwarten, da die entsprechenden Strafverfahren aufgrund ihrer Bedeutung und der mögli-

chen Straferwartung in aller Regel nicht den Bundesgerichtshof erreichen können. Es wird daher angeregt, diese Rechtsfrage im vorgenannten Sinne ausdrücklich in § 113 TKG zu regeln.

9. Email-Überwachung

Eine Regelung der Anordnung für die Überwachung des Email-Verkehrs eines Beschuldigten ist im vorliegenden Regierungsentwurf nicht vorgesehen. Dies erstaunt, denn hinsichtlich der Art der erforderlichen Anordnung bestehen seit Jahren verschiedene Rechtsauffassungen, welche bislang nicht höchstrichterlich einer Klärung zugeführt werden konnten. Dabei werden bezüglich einer Email drei oder besser sogar sieben Phasen unterschieden:

a) Erstellung der Email auf dem Rechner des Absenders
b) Versendung der Email
c) Ankunft der Email beim Email-Provider des Absenders, Überprüfung des Accounts vor einer Weiterleitung
d) Versendung der Email zum Email-Provider des Empfängers
e) Ankunft beim Email-Provider des Empfängers, Überprüfung des zugehörigen Accounts, Zwischenspeicherung bis zum Abruf
f) Abholung der Email vom Empfänger
g) Speicherung auf dem Rechner des Empfängers zur weiteren Verarbeitung

Nach der Entscheidung des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 - ist davon auszugehen, dass die Phase a) [Erstellung der Email auf dem Rechner] und die Phase g) [Speicherung der angekommenen Nachricht auf dem Rechner des Empfängers] nicht unter dem Schutz des Fernmeldegeheimnisses steht, sondern nur durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) geschützt wird. Somit können Emails vor dem Absenden und nach der Ankunft auf herkömmlichem Wege nach §§ 94, 98 StPO beschlagnahmt werden. Kein Zweifel besteht auch für die Phasen b), d) und f), in denen die

Nachrichten auf Telekommunikationswegen transportiert werden und damit nur entsprechend § 100a StPO aufgezeichnet werden können. Strittig sind sonach allein die Phasen c) und e), bei denen sich die Nachrichten im Rechnersystem des jeweiligen Providers befinden und dort zumindest kurzzeitig zwischengespeichert werden. Nach wohl zutreffender Ansicht sind die Daten in diesen beiden Phasen nicht Gegenstand eines Telekommunikationsvorgangs (vgl. hierzu KK/StPO-Nack § 100a Rdn. 8; Münch.Komm. StGB/Graf § 202a Rdn. 57 m.w.N.; Wolfgang Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, Stuttgart 2007, S. 77 ff.). Danach spricht viel dafür, eine Email wegen ihrer Offenheit und der grundsätzlich gegebenen Zugreifbarkeit und Sichtbarkeit des Inhalts durch verschiedenste Personen auf dem Transportweg eher einer Postkarte als einem Brief gleichzustellen. Auf jeden Fall scheinen die Vorschriften der Postbeschlagnahme nach § 99 StPO am ehesten anwendbar und gewähren auch entsprechenden Schutz durch die erforderliche richterliche Anordnung nebst der Kontrollbefugnis des Gerichts. Da es aber zu dieser Frage bis in die jüngste Zeit divergierende Rechtsprechung gibt (vgl. Bär a.a.O.), eine höchstrichterliche Klärung derzeit nicht absehbar ist, wird ebenfalls angeregt, die Frage der Anordnung einer Email-Überwachung beim Email-Provider ausdrücklich gesetzlich zu regeln, indem beispielsweise eine entsprechende Formulierung in § 99 StPO eingefügt wird.