Oberstaatsanwalt Ralf Günther
Staatsanwaltschaft Hannover
Volgersweg 67
30175 Hannover

Hannover, 12.09.2007

Stellungnahme zum

a) Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinien 2006/24/EG
BT-Drucksache16/5846

b) Entwurf eines Gesetzes zur Reform der Telekommunikationsüberwachung (Gesetz zur Änderung der Strafprozessordnung)
BT-Drucksache16/3827

c) Antrag einzelner Abgeordneter und der Fraktion der FDP „Reform der Telefonüberwachung zügig umsetzen“
BT-Drucksache 16/1421

I. Allgemeine Anmerkungen

Die in Bezug genommenen Entwürfe sollen nachfolgend vorrangig hinsichtlich derjenigen Aspekte beleuchtet werden, die sich aus Sicht des Rechtsanwenders ergeben. Fragen wie die Zulässigkeit der Vorratsdatenspeicherung und die Vereinbarkeit des § 113a TKG-E mit Verfassungs- bzw. mit Europarecht werden keiner vertiefenden Betrachtung unterzogen.

Zunächst werden einzelne Vorschriften aufgezeigt, die sich in der strafprozessualen Praxis bewährt haben und hinsichtlich derer ein gesetzgeberischer Handlungs-

bedarf auch deshalb nicht besteht, weil sich insoweit eine gefestigte Rechtsprechung gebildet hat (nachfolgend 1.). Sodann wird exemplarisch aufgezeigt, wie schwierig namentlich der Umgang mit telekommunikationsrechtlichen Fragestellungen gelegentlich selbst für den Bundesgerichtshof sowie das Bundesverfassungsgericht ist (nachfolgend 2.) und – daran anknüpfend – gesetzgeberischer Handlungsbedarf insbesondere hinsichtlich der nach wie vor offenen Frage aufgezeigt, was im Hinblick auf die sich ständig entwickelnden Kommunikationstechniken überhaupt unter Telekommunikation im Sinne der §§ 100a, 100b bzw. 100g, 100h StPO zu verstehen ist (nachfolgend 3.)

Schließlich wird weiterer gesetzgeberischer Handlungsbedarf bezüglich des Einsatzes von Vertrauenspersonen sowie zur verdeckten Durchsuchung von Wohnungen aufgezeigt (nachfolgend II.). Anschließend wird auf die vorgesehenen Neuregelungen sowie das Erfordernis der Regelung der „Online-Durchsuchung“ eingegangen (nachfolgend III.).

1. Beibehaltung bewährter Vorschriften

Das Ziel der Bundesregierung, mit dem vorliegenden Entwurf ein harmonisches Gesamtsystem der strafprozessualen heimlichen Ermittlungsmethoden zu schaffen, ist nachdrücklich zu begrüßen. Gleiches gilt, soweit mit dem Regierungsentwurf erklärtermaßen die Ziele verfolgt werden,

- eine Zweckbindung verdeckt erhobener Daten sowie einen effektiven Rechtsschutz der von verdeckten Ermittlungsmaßnahmen Betroffenen zu gewährleisten (vgl. S. 43 ff., Verweise ohne nähere Bezeichnung beziehen sich auf den Regierungsentwurf),
- die Erkenntnisse aus den in Auftrag gegebenen rechtswissenschaftlichen und rechtstatsächlichen Untersuchungen von Albrecht, Dorsch und Krüpe zur “Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den § 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen“ (2003) zu berücksichtigen (vgl. S. 45 ff.),
- in Anlehnung an die von Wolter und Schenke zusammengestellte Textsammlung “Zeugnisverweigerungsrechte bei (verdeckten) Ermitt-

lungsmaßnahmen“ (2002) Beweiserhebungs- und Beweisverwertungsverbote bei zeugnisverweigerungsberechtigten Berufsgeheimnisträgern zu normieren (vgl. S. 48 ff.) sowie

- Unsicherheiten in der Rechtsanwendung bei verdeckten Ermittlungsmaßnahmen zu beheben (vgl. S. 52 ff.) und die notwendigen Konsequenzen aus der Rechtsprechung des Bundesverfassungsgerichts zu den verdeckten Ermittlungsmaßnahmen zu ziehen.

Diese Ziele dürften jedoch ebenso wie die weiteren in der Begründung des Regierungsentwurfs enthaltenen Erwägungen nicht geeignet sein, die Novellierung bestimmter, über Jahre hinweg bewährter Vorschriften zu rechtfertigen, die für eine effektive und geordnete Strafverfolgung von Bedeutung sind. Dies gilt namentlich für die Regelung des § 100b Abs. 1 Satz 2 StPO und damit einhergehend deren Auslegung durch den Bundesgerichtshof sowie § 100b Abs. 2 Satz 4 und 5 StPO und § 163f Abs. 3 Satz 1 StPO.

Die in Aussicht genommenen Novellierungen der genannten Vorschriften, etwa § 100b Abs. 1 Satz 3 Halbsatz 2 StPO, sehen nunmehr u. a. vor, dass personenbezogene Daten, deren Erhebung auf einer Anordnung der Staatsanwaltschaft wegen Gefahr im Verzug beruht, zu Beweiszwecken nur dann Verwendung finden dürfen, wenn Gefahr im Verzug - tatsächlich - bestand. Nach der Vorschrift des § 100b Abs. 1 Satz 4 und 5 StPO-E sollen Anordnungen gemäß §§ 100a, 100b StPO-E zur Telekommunikationsüberwachung bzw. gemäß § 100g StPO-E zur Erhebung von Verkehrsdaten in Zukunft längstens zwei statt wie bisher drei Monate befristet werden können und Verlängerungen dieser Anordnungen nur dann möglich sein, wenn die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Durch § 163f Abs. 3 Satz 1 StPO-E wird schließlich nicht nur wie bisher die Verlängerungs- sondern auch die Erstanordnung einer längerfristigen Observation dem Richtervorbehalt unterstellt (vgl. hierzu nachfolgend III. 3. und 10.).

Gleichwohl für notwendig erachtete Neuregelungen sollten namentlich in das Recht der Telekommunikationsüberwachung angesichts noch offener

Grundsatzfragen wie der, was überhaupt unter „Telekommunikation“ zu verstehen ist, nur besonders behutsam und mit Bedacht implementiert werden.

2. Zur Rechtsprechung von Bundesgerichtshof und Bundesverfassungsgericht zur Telekommunikationsüberwachung

Die Bestimmung des sachlichen Anwendungsbereichs von Artikel 10 GG und damit zugleich auch die Auslegung der §§ 100a, 100b StPO bzw. der §§ 100g, 100h StPO hat sich angesichts der technologischen Entwicklungen und der durch sie bedingten vielfältigen Konvergenzen der Übertragungswege nicht an rein technischen Kriterien zu orientieren (vgl. BVerfG NJW 2002, 3619, 3620 f.).

Beides, die Bestimmung des sachlichen Anwendungsbereichs von Art. 10 GG als auch Auslegung der genannten Eingriffsnormen, hat jedoch sowohl der strafprozessualen Praxis als auch der Rechtsprechung, hier der ober- bzw. höchstrichterlichen Rechtsprechung der Fachgerichte ebenso wie dem Bundesverfassungsgericht, wiederholt Schwierigkeiten bereitet. So hatte

- der Ermittlungsrichter beim Bundesgerichtshof zunächst die Auffassung vertreten, “Positionsmeldungen nicht telefonierender Mobiltelefone“ berührten den Schutzbereich von Art. 10 GG (BGH NJW 01, 1587)
- und hatte das Bundesverfassungsgericht in seiner Entscheidung vom 4. Februar 2005 - 2 BvR 308/04 (NJW 2005, 1637 ff.) - noch ausgeführt, die in einem sichergestellten Mobiltelefon gespeicherten Verbindungsdaten bzw. die Daten in schriftlichen Einzelverbindungsnachweisen der Telekommunikationsdienstleister dürften nur im Falle des Vorliegens einer Straftat erheblicher Bedeutung und nur auf der Grundlage einer dem § 100g, 100h StPO entsprechenden richterlichen bzw. staatsanwaltschaftlichen Anordnung erhoben werden. Wie keine andere hatte diese Entscheidung des Bundesverfassungsgericht in der strafprozessualen Praxis „zu zeitweise erheblicher Unsicherheit geführt“ (vgl. S. 52).

- Weiter hatte das Bundesverfassungsgericht in seiner Entscheidung vom 1. Juli 2005 - 1 BvR 668/04 (NJW 2005, 2603 ff.) in einem obiter dictum angemerkt, der “Bundesgesetzgeber hat die Überwachung der Telekommunikation zu Zwecken der Strafverfolgung in den §§ 100a, 100b, 100g, 100h und 100i geregelt (NJW 2005, 2603 ff)“.

Das Bundesverfassungsgericht hat seine Auffassungen zu diesen tatsächlich wie rechtlich äußerst schwierigen Fragestellungen in seinen weiteren Entscheidungen vom 2. März 2006 - 2 BvR 2099/94 (NJW 2006, 978 ff.) - und 22.08.2006 - 2 BvR 1345/03 - zutreffend - revidiert. So hat es festgestellt, dass die in einem Mobiltelefon gespeicherten Verbindungsdaten bzw. die Daten in schriftlichen Einzelverbindungsnachweisen der Telekommunikationsdienstleister dem Fernmeldegeheimnis (doch) nicht unterliegen und nicht auf der Grundlage einer den §§ 100g, 100h StPO entsprechenden Anordnung erhoben werden müssen. Es hat weiter richtig gestellt, dass die Regelung des § 100i StPO das Fernmeldegeheimnis (doch) nicht berührt. Schließlich hat es hinsichtlich der Entscheidung des Ermittlungsrichters beim BGH klargestellt, dass die Erhebung von Standortdaten den Schutzbereich des Art. 10 GG (ebenfalls) nicht berührt. Dennoch belegen die zitierten Entscheidungen vom 4. Februar 2005 und 1. Juli 2005 eindrucksvoll die Schwierigkeiten, die selbst das Bundesverfassungsgericht als maßgeblicher Interpret des Grundgesetzes bei der verfassungskonformen Auslegung der §§ 100a, 100b StPO bzw. der §§ 100g, 100h StPO hat, wenn der Einsatz neuer Technologien zu strafprozessualen Zwecken zu bewerten ist.

Von zentraler Bedeutung für die Beantwortung dieser sowie weiterer telekommunikationsrechtlicher Fragestellungen (vgl. insoweit auch nachfolgend III. 8) ist ein grundrechtskonformes Verständnis des sachlichen Anwendungsbereich der §§ 100a, 100b bzw. 100g, 100h StPO und damit vom Begriff der „Telekommunikation“. Hierzu verhält sich der Regierungsentwurf nicht.

3. Erfordernis eines genuin strafprozessualen Begriffs „Telekommunikation“

Der Bundesgerichtshof scheint sich bei der Auslegung des Begriffs „Telekommunikation“ in § 100a StPO vorrangig an dessen technischer Komponente zu orientieren. Dies indes erschwert die verfassungskonforme Auslegung der Norm gerade bei modernen Informationstechnologien.
So vertritt der 2. Strafsenat des BGH in seiner Entscheidung vom 14.03.2003 - 2 StR 341/02, BGH NJW 2002, 2034 ff.) die Auffassung, der Begriff der Telekommunikation umfasse „die Vorgänge des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art, also den gesamten Datenverkehr mittels Telekommunikationsanlagen“ und sei „insoweit inhaltsgleich mit der Legaldefinition des § 3 Nr. 16 TKG“ (alte Fassung). An dieser Definition hat sich auch der 3. Strafsenat des BGH in seiner „Online-Entscheidung“ vom 31.01.2007 noch orientiert, indem er auf die Regelung des § 3 Nr. 22 und 23 TKG (neue Fassung) verwiesen hat.

Vor diesem Hintergrund sind Schwierigkeiten bei der Rechtsanwendung absehbar. Beispielhaft soll die Vorschrift des § 100b Abs. 6 Nr. 4 StPO-E und der dort enthaltene Begriff “Telekommunikationsvorgänge“ näher beleuchtet werden.
Soweit nach dieser Regelung in den Berichten an das Bundesamt für Justiz “die Anzahl der überwachten Telekommunikationsvorgänge nach Maßgabe der Unterteilung in Nr. 2 Buchstabe b (Festnetz-, Mobilfunk- oder Internettelekommunikation) anzugeben ist, stellt sich die Frage, ob der Begriff des Telekommunikationsvorgangs im Sinne des TKG, mithin im technischen Sinne auszulegen ist, oder aber - vorzugswürdig – noch stärker im Lichte des Art. 10 GG . Dann indes dürfte von dem Begriff „Telekommunikation“ bzw. „Telekommunikationsvorgänge“ nur die Verständigung zwischen Personen, mithin den Grundrechtsadressaten des Artikel 10 GG und nicht der keine Gedankenerklärung enthaltene, allein technisch bedingte Datenaustausch zwischen Kommunikationsanlagen, mithin zwischen Maschinen, erfasst werden. Namentlich die Internetkommunikation mit ihren vielfältigen Übertragungsmöglichkeiten bereitet hier Abgrenzungsschwierigkeiten.

So stellt die Nutzung von Voice over IP (Internettelefonie) ebenso wie das Versenden von E-Mails zweifelsfrei einen „qualifizierten“, mithin vom Schutzbereich des Art. 10 GG erfassten und damit auch einen den Voraussetzungen der §§ 100a, 100b StPO bzw. der §§ 100g, 100h StPO unterworfenen Telekommunikationsvorgang dar, während andererseits die Nutzung von Streaming-Angeboten wie beispielsweise das Internetradio ebenso wie der Empfang von Fernsehen zwar „Telekommunikation“ im technischen Sinne, mithin im Sinne des TKG, nicht aber von Art. 10 GG erfasste „Telekommunikation“, mithin auch keine Telekommunikation im Sinne der StPO ist.
Anders als bei der klassischen Sprachtelefonie zu „Kaisers Zeiten“, als eine weitestgehende Kongruenz zwischen „Telekommunikation“ und dem Schutzbereich des Artikel 10 GG und damit dem Anwendungsbereich der §§ 100a, 100b StPO bzw. 100g, 100h StPO bestand, liegt bei modernen Kommunikationsformen wie dem Internet regelmäßig eine Inkongruenz zwischen den hier möglichen Formen der „Telekommunikation“ und dem Schutzbereich von Artikel 10 GG vor. So stellt der Abruf von nicht zugangsgeschützten Webseiten auf der Grundlage des http („Hypertext Transfer Protocol“) die Nutzung solcher Daten dar, die sich an die Allgemeinheit richten, dieser Vorgang dürfte mithin nicht als Individualkommunikation im Sinne des Art. 10 GG und damit auch nicht als qualifizierte „Telekommunikation“ anzusehen sein. Er würde somit von § 100b Abs. 6 Nr. 2b und Nr. 4 StPO-E nicht erfasst.

Der Begriff „Telekommunikation“ im Sinne der StPO muss vielmehr in einem technisch-funktionalen Sinne verstanden werden, nämlich als der – indes nicht jeder – technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Kommunikationsanlagen (technischer Aspekt), wobei nur solche Signale (Daten) erfasst werden, die Nachrichten im Sinne einer individuellen Kommunikation von Grundrechtsträgern enthalten und diese auch nur so lange, wie der Nachrichtenübertragungsvorgang nicht abgeschlossen ist. Im Falle einer (Zwischen-)Speicherung, wie sie bei E-Mails technisch bedingt ist, mithin nur, wenn die Speicherung in einem funktionalen, dienendem Bezug zur noch nicht abgeschlossenen

Übertragung steht (funktionaler, an der Schutzfunktion des Artikel 10 GG orientierter Aspekt).

Aus Gründen der Normklarheit und damit der Rechtssicherheit wäre wünschenswert, wenn in den Regierungsentwurf eine verfassungskonforme, klarstellende Regelung in diesem Sinne aufgenommen würde. Dem dürfte nicht entgegenstehen, dass eine solch einfachgesetzliche Regelung nur deklaratorischen Charakter hätte, weil sie sich vorrangig auf eine verfassungsrechtliche Fragestellung bezieht. Der einfache Gesetzgeber sah sich bereits bei anderer Gelegenheit hierzu veranlasst. So hat er in § 113 Abs. 1 Satz 2 TKG festgelegt, Auskünfte über Daten, mittels derer der Zugriff auf Endgeräte oder im Netz eingesetzte Speichereinrichtungen geschützt werde, insbesondere PIN oder PUK, habe der nach Satz 1 Verpflichtete aufgrund eines Auskunftsverlangens nach § 161 Abs. 1 Satz 1, § 163 Abs. 1 der StPO, der Datenerhebungsvorschriften der Polizei, der Gesetze des Bundes oder der Länder oder anderer dort weiter aufgeführter Ermächtigungsgrundlagen zu erteilen. Er hat dadurch für Rechtsklarheit gesorgt und Rechtsfrieden geschaffen. Diese Frage war zwischen den Bedarfsträgern einerseits und den Verpflichteten andererseits heftig umstritten.

Der Aufgabe einer verfassungskonformen Auslegung strafprozessualer Eingriffsnormen hat sich die Praxis – Polizeibehörden, Staatsanwaltschaften und Gerichte ebenso wie die durch die Maßnahmen in ihren Grundrechten Betroffenen und deren Verteidiger – tagtäglich zu stellen. Strafverfahrensrecht ist „angewandtes Verfassungsrecht“ (vgl. Henkel, Lehrbuch zum Strafverfahrensrecht, 1. Auflage). Die einen haben diese Aufgabe regelmäßig unter dem besonderen Druck zu leisten, der namentlich mit der Dynamik komplexer und verdeckt geführter Ermittlungsverfahren einhergeht, die anderen unter der Belastung, die sich regelmäßig mit dem Vorwurf ergibt, erhebliche oder gar schwerwiegende Straftaten begangen zu haben, zu deren Nachweis die zunächst verdeckt geführten Ermittlungsmaßnahmen nach Auffassung der Strafverfolgungsbehörden geeignet sein sollen.

Wie wichtig die Notwendigkeit einer klaren Definition des Begriffs Telekommunikation ist, der sowohl in § 100a Abs. 1 StPO als auch in §§ 3, 88 Abs. 1 TKG Verwendung findet, wird stets dann deutlich, wenn technische Innovationen, die immer neue Möglichkeiten eröffnen, geeignet sind, strafprozessual relevante Umstände festzustellen und sich damit die Frage stellt, ob und wenn ja unter welchen Voraussetzungen ihr Einsatz zu strafprozessualen Zwecken zulässig ist.

In einem Ermittlungsverfahren sollte ein so genannter "Phonetracker" eingesetzt werden. Es handelt sich hierbei um ein technisches Gerät, welches an die Schnittstelle eines handelsüblichen Mobiltelefons (Handy) gesteckt wird und im Zusammenwirken mit diesem weitere Funktionalitäten ermöglicht. So unter anderem eine „Diebstahlsfunktion" mittels Erschütterungssensor (Gerät reagiert auf Erschütterungen), eine „Schutzzonenfunktion", durch die eine Rückmeldung veranlasst wird, wenn eine zu überwachende Person oder ein zu überwachendes bewegliches Objekt einen zuvor definierten Bereich verlässt, sowie eine „Hineinhörfunktion", die die Wahrnehmung bzw. Übertragung der Umgebungsgeräusche durch Mithören an einem anderen Telefon ermöglicht.

Als mögliche Rechtsgrundlage für den Einsatz dieses Gerätes bei Nutzung der „Schutzzonenfunktion" könnten auf den ersten Blick sowohl die Vorschriften der §§ 100a, 100b bzw. der §§ 100g, 100h StPO; zu strafprozessualen Zwecken wird schließlich ein zur Telekommunikation geeignetes Medium genutzt, als auch die Aufgabengeneralklauseln der §§ 161, 163 StPO, die Vorschrift des § 100f, die den Einsatz technischer Mittel erlaubt, die des § 100i StPO (IMSI-Catcher), die des § 163f StPO (längerfristige Observation) oder gar eine Kombination der §§ 100f, 163f StPO zu prüfen sein.
Obwohl die Vorschriften der §§ 100a, 100b StPO nicht einschlägig sein dürften, weil keine qualifizierten, mithin den Schutzbereich des Artikel 10 GG berührenden Telekommunikationsdaten des Betroffenen übertragen werden, stützt sich die erste hier bekannt gewordene gerichtliche Entscheidung zum Einsatz dieses Ermittlungsinstruments

auf die § 100a, 100b StPO. Näherliegend erscheint jedoch, die Maßnahme auf § 100f Abs. 1 Nr. 2 StPO, gegebenenfalls in Verbindung mit § 163 f StPO, zu stützen.

II. Implementierung weiterer Ermittlungsmöglichkeiten

Ein harmonisches Gesamtsystem strafprozessualer heimlicher Ermittlungsmethoden sollte – anders als im Regierungsentwurf vorgesehen – auch die Rechtsgrundlage für die nachfolgend aufgeführten, den Bedürfnissen einer effizienten Strafverfolgung Rechnung tragenden Eingriffsermächtigungen schaffen, die vereinzelt bereits durch Richterrecht anerkannt sind:

1. Einsatz von Vertrauenspersonen (VPs):

Der Gesetzgeber hat es bei der Schaffung des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen organisierter Kriminalität (OrgKG) noch abgelehnt, eine Rechtsgrundlage für den Einsatz dieses Ermittlungsinstruments zu schaffen (vgl. BT Drucksache 12/989, 41). In der Praxis wird es zwischenzeitlich sehr viel häufiger als das gesetzlich geregelte Instrument des Verdeckten Ermittlers eingesetzt.

Zwar ist der Einsatz von Vertrauenspersonen durch die ständige höchstrichterliche Rechtsprechung anerkannt (zu den Nachweisen vgl. Körner BtMG, 5. Auflage § 31 Rdnr. 113). In seiner neueren Rechtsprechung (vgl. die Entscheidungen im sog. Sedlmayr-Prozess, Beschlüsse 2 BvR 2017/04 und 2 BvR 2039/94 v. 01.03.2000) hat das Bundesverfassungsgericht jedoch deutlich gemacht, dass jedenfalls beim Übergang von der passiven Informationserlangung ohne Eingriffscharakter zur aktiven Informationsbeschaffung durch die VP mittels einer gezielten Befragung eine strafprozessuale Maßnahme vorliegt, die, so das Bundesverfassungsgericht weiter, eine spezielle gesetzliche Ermächtigungsgrundlage erforderlich mache. Eine entsprechende Rechtsgrundlage sollte daher in das geplante Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen implementiert werden.

2. Verdeckte Durchsuchung von Wohnungen

In Verfahren der schweren bzw. der Organisierten Kriminalität ergibt sich zur Gewährleistung einer effektiven Strafverfolgung gelegentlich die Notwendigkeit einer heimlichen Durchsuchung. So etwa in den Fällen, in denen sichere Anhaltspunkte dafür vorliegen, dass die Beschuldigten in durch Art. 13 GG geschützten Räumlichkeiten inkriminierte Güter wie Waffen oder Betäubungsmittel lagern und die Aufdeckung namentlich der Täterstrukturen einerseits eine Fortführung der Ermittlungen durch verdeckte Maßnahmen gebieten, andererseits die Vorsorge für die Abwehr von Gefahren für die Volksgesundheit und für Leib und Leben Dritter gleichzeitig eine Sicherstellung der Betäubungsmittel bzw. Waffen erfordern. Dies ist jedoch nur im Rahmen einer heimlichen Durchsuchung möglich.

Nach zutreffender Auffassung ist eine heimlich durchgeführte Durchsuchung von Wohnungen durch die Strafverfolgungsbehörden nach den materiellen und formellen Voraussetzungen der §§ 102, 106 und 107 StPO unzulässig.
Da somit die StPO de lege lata das heimliche Betreten von Wohnungen zum Zwecke ihrer Durchsuchung nicht zulässt, verfassungsrechtliche Aspekte, insbesondere der Regelungsgehalt des Art. 13 Abs. 2 GG, einer solchen Maßnahme grundsätzlich jedoch nicht entgegenstehen, sollte für die heimliche Durchsuchung eine Rechtsgrundlage geschaffen werden. Dieselbe rechtliche Frage stellt sich auch im Zusammenhang mit der zurzeit kontrovers geführten Diskussion zur so genannten „Online-Durchsuchung“.

III. Zu den einzelnen Vorschriften (Vorschriften ohne nähere Erläuterung sind solche des Regierungsentwurfs, BT-Drucksache 16/5846)

1. § 53b StPO-E

Es ist abzusehen, dass die Vorschriften des § 53b Abs. 1 Satz 1 StPO-E sowie des § 53 Abs. 2 Satz 1 StPO-E in Anbetracht der unscharfen Konturierung ihrer materiellen Voraussetzungen der strafprozessualen Praxis erhebliche Schwierigkeiten bereiten werden.

So erfordert das dort jeweils enthaltene Merkmal „voraussichtlich“ eine Prognose, die die Feststellung entsprechender Erkenntnisse nicht nur als möglich, sondern als nahezu wahrscheinlich erscheinen lässt. Bei einer Überwachung des durch § 53b Abs. 1 Satz 1 StPO-E geschützten Personenkreises dürfte indes nie auszuschließen sein, dass jedenfalls auch solche Erkenntnisse erlangt werden, über die dieser Personenkreis das Zeugnis verweigern darf. Damit käme die Vorschrift einem generellen Beweiserhebungsverbot gleich. Absehbar ist auch, dass eine nicht unerhebliche Zeit vergehen dürfte, bis die Vorschrift durch die Rechtsprechung hinreichend scharf konturiert und damit Rechtssicherheit eintreten würde. Dieser – sicher absehbare – Umstand könnte durch die Konstituierung lediglich eines Beweisverwertungsverbotes vermieden werden.

2. § 100a StPO-E:

a) Die Streichung des § 20 VereinsG erscheint nicht sachgerecht. Es handelt sich hierbei um ein Staatsschutzdelikt. Angesichts der – aktuell wieder sichtbar gewordenen – konkreten Bedrohung durch den internationalen Terrorismus erscheint eine effektive Bekämpfung jedweder Form von Staatschutzdelikten zwingend geboten. Auch für die Bekämpfung dieser Delinquenz ist die Telekommunikationsüberwachung das zentrale Ermittlungsinstrument.

b) Die in § 100a Abs. 4 StPO-E enthaltene Regelung zum Schutz des Kernbereichs privater Lebensgestaltung verdient Zustimmung. Sie trägt einerseits den durch die Rechtsprechung des Bundesverfassungsgerichts aufgestellten Forderungen zum Schutz des Kernbereichs privater Lebensgestaltung ausreichend Rechnung. Anderseits ist sie, im Gegensatz zu § 53b Abs. 1 Satz 1 StPO-E, ausreichend scharf konturiert. Dies wird dadurch gewährleistet, dass die Vorschrift ein Beweiserhebungs- und Beweisverwertungsverbot für die Fälle enthält, in denen tatsächliche

Anhaltspunkte für die Annahme vorliegen, dass durch eine entsprechende Maßnahme „allein“ Erkenntnisse aus dem Bereich privater Lebensgestaltung erlangt würden.

Die Überwachung der Telekommunikation ist in ihrer Art und Eingriffstiefe mit der akustischen Wohnraumüberwachung nicht vergleichbar (BVerfG NJW 2005, 2603, 2612). Auch wenn mit jeder Maßnahme dieser Art bei prognostischer Betrachtung in den Kernbereich des Persönlichkeitsrechts eingegriffen werden könnte, wird dieser Bereich durch Maßnahmen der Telekommunikationsüberwachung und bezogenen auf ihre Gesamtzahl nur in seltenen Fällen tangiert.

Die meisten Maßnahmen dieser Art werden im Zusammenhang mit Drogendelikten durchgeführt (circa 55 %, vgl. Studie des Max-Planck-Instituts, S. 53 ff.). Die Tatverdächtigen (nicht nur dieses Deliktsbereichs) rechnen regelmäßig mit der Überwachung ihrer Kommunikation und haben ihr Verhalten entsprechend eingerichtet. Sie reden verklausuliert und thematisieren regelmäßig keine kernbereichsrelevanten Daten.

> *Ein typisches Gespräch dieser Art stellt sich wie folgt dar (Auszug):*
>
> *Anrufer: Hallo*
> *Angerufener: Ja*
> *Anrufer: … unser Team ist bereit, wir hatten gedacht, heute Abend dorthin zu kommen.*
> *Angerufener: Morgen … aber nicht so spät, ja? … seid so gegen sechs, sieben hier.*
> *Anrufer: In Ordnung.*
> *Angerufener: Platz für wie viele Personen organisierst du?*
> *Anrufer: Platz für wie viele Personen? Er braucht Platz für zwanzig Personen. Für fünfzehn, zwanzig Personen*

Polizeibehörden und Staatsanwaltschaft haben im Rahmen einer - wie stets - vorläufigen Bewertung der Sach- und Rechtslage das Gespräch auf der Grundlage der weiteren Ermittlungsergebnisse dahingehend interpretiert, dass der Anrufer von dem Angerufenen Drogen erwerbe und zunächst noch am Tage des Anrufs vorbeikommen wollte, von dem Angerufenen jedoch auf den nächsten Tag verwiesen wurde und diesem auf Nachfrage mitgeteilt hat, er wolle fünfzehn bis zwanzig Kilogramm Drogen kaufen.

Das Landgericht hat die Anklage zur Hauptverhandlung zugelassen und das Hauptverfahren eröffnet. Im Rahmen der Hauptverhandlung wurden die Ermittlungsergebnisse bestätigt.

3. § 100b StPO-E:

a) Die Regelung in § 100b Abs. 1 Satz 3 StPO-E, wonach die staatsanwaltschaftliche Eilanordnung außer Kraft tritt, wenn sie nicht binnen drei „*Werktagen*“ bestätigt wird, ist sachgerecht, weil durch diese Klarstellung bestehende Unsicherheiten bezüglich der Frage, ob bei der Berechnung des Endes der 3-Tages-Frist die Regelung des § 43 Abs. 2 StPO Anwendung findet, einer Klärung zugeführt wird. Bezüglich dieser sowie weiterer Fragen im Zusammenhang mit der Fristberechnung, namentlich hinsichtlich der Fristberechnung bei Verlängerungsanordnungen, bestehen in der strafprozessualen Praxis erhebliche Unsicherheiten.

Noch vor wenigen Tagen hat ein Telekommunikationsdienstleister in einem Ermittlungsverfahren die Frist dergestalt berechnet, dass er den Zeitraum, um den die Maßnahme durch einen zwei Wochen vor Ablauf der Erstanordnung erlassenen Beschluss verlängert worden

sei, an das Fristende der Erstanordnung „angehängt“ habe. Danach liefe die Frist (erst) in 15 Tagen ab.
Die Fristberechnung nach diesem nach hiesiger Auffassung allein richtigen „Modell“ ergab, dass die Maßnahme bereits in wenigen Tagen auslaufen würde.

Nach hier vorliegenden Erfahrungen findet das in diesem Fall von dem Telekommunikationsdienstleister benutzte Modell der Fristberechnung auch bei Strafverfolgungsbehörden und Gerichten Anwendung.

Zutreffend ist deshalb der in der Begründung (vgl. S. 111) enthaltene Hinweis, wonach für den Fristbeginn sowohl bei Erst - als auch bei der Verlängerungsanordnungen der Erlass der jeweiligen Anordnung maßgeblich sei, und dies selbst dann gelte, wenn die Verlängerungsanordnung deutlich vor Ablauf der Erstanordnung erlassen worden sei. Nur so ist eine Berechnung des Fristenlaufs möglich, die der Wert setzenden Bedeutung des durch Art. 10 Abs. 1 GG geschützten Fernmeldegeheimnisses hinreichend Rechnung trägt.

b) Zustimmung verdient weiter die Regelung des § 100b Abs. 1 Satz 3 HS 2 StPO-E, soweit durch sie nunmehr klargestellt wird, dass die aufgrund einer rechtmäßigen staatsanwaltschaftlichen Eilanordnung gewonnen Erkenntnisse auch dann verwertbar sind, wenn eine richterliche Bestätigung nicht erfolgt. Auch bezüglich dieser Frage bestanden in der strafprozessualen Praxis erhebliche Unsicherheiten.

c) Entgegenzutreten ist indes der Regelung des § 100b Abs. 1 Satz 3 HS 2 StPO-E, wonach zwischenzeitlich erlangte personenbezogene Daten zu Beweiszwecken *ausnahmslos* dann nicht verwertet werden dürfen, wenn Gefahr im Verzug nicht bestand, die Anordnung mithin *rechtswidrig* war.

Zum einen stellt die Vorschrift eine Tautologie und damit eine im Verhältnis zu § 100b Abs. 1 Satz 2 StPO-E überflüssige Regelung dar, wonach die Staatsanwaltschaft nur bei Gefahr im Verzug zur Anordnung befugt ist. Lag Gefahr im Verzug nicht vor und war dies der Staatsanwaltschaft zum Zeitpunkt ihrer Anordnung entweder bekannt oder hat sie es grob fehlerhaft verkannt, sind die gewonnenen Erkenntnisse bereits heute aufgrund der gefestigten Rechtsprechung des Bundesgerichtshofs unverwertbar.
Zum anderen könnte die Regelung so verstanden werden, dass sie ein Beweisverwertungsverbot selbst dann konstituiert, wenn Gefahr im Verzug (ebenfalls) nicht vorlag, dies von der die Überwachung anordnenden Staatsanwaltschaft jedoch, anders als in den vorgenannten Fällen, in nicht vorwerfbarer Weise verkannt wurde. Auch insoweit ein Beispiel:

> *Die Strafverfolgungsbehörden erhielten an einem Samstag gegen 16 Uhr durch einen Informanten den Hinweis, wonach eine namentlich benannte Person die Absicht habe, noch am selben Tag um circa 20 Uhr von ihrem Lieferanten eine Menge von einem Kilogramm Kokain zum Zwecke des gewinnbringenden Weiterverkaufs zu erwerben. Der Übergabeort sowie die genaue Übergabezeit sollten zwischen beiden telefonisch abgesprochen werden. Ein Ermittlungsrichter war nicht zu erreichen. Gegen 17 Uhr traf die Staatsanwaltschaft eine Eilanordnung zur Überwachung der Telekommunikation, aufgrund derer der Sachverhalt aufgeklärt werden konnte. Der Informant der Polizei hatte seinen Hinweisgeber jedoch insoweit falsch verstanden, als die Übergabe tatsächlich erst 24 Stunden später erfolgen sollte. Die die Tat vorbereitenden Gespräche konnten überwacht, die Betäubungsmittel am Sonntag gegen 20 Uhr sichergestellt werden.*

Die anordnende Staatsanwaltschaft durfte, ja musste auf der Grundlage der vorliegenden Erkenntnisse davon ausgehen, dass

Gefahr im Verzug vorlag. Tatsächlich hätte eine richterliche Anordnung noch rechtzeitig durch den Bereitschaftsdienst in der Zeit zwischen 10 bis 12 Uhr herbeigeführt werden können. Soll künftig in Fällen dieser Art ein Beweisverwertungsverbot zu diskutieren sein, weil eine die Strafverfolgungsbehörden irrtümlich von Samstag statt von Sonntag ausgegangen war?

Ein Beweisverwertungsverbot auch in derartigen oder ähnlich gelagerten Fällen wäre weder verfassungsrechtlich geboten, noch würde es dem Umstand ausreichend Rechnung tragen, dass bei der Schaffung von Regelungen, die die Ermittlung des wahren Sachverhalts gefährden und damit zu ungerechten, weil materiell unrichtigen Verfahrensergebnissen führen können, besondere Zurückhaltung geboten ist. Dieser gewichtige Aspekt wird in der Begründung des Regierungsentwurfs zu Recht an anderen Stellen wiederholt betont. Dem Rechnung tragend ist in der höchstrichterlichen Rechtsprechung bisher davon ausgegangen worden, dass aufgrund der häufig besonderen Entscheidungssituationen der Strafverfolgungsbehörden mit ihren situationsbedingt begrenzten Erkenntnismöglichkeiten ein Verwertungsverbot dann nicht besteht, wenn bei einer Beurteilung ex ante die Entscheidung als vertretbar, mithin nicht als grob fehlerhaft bzw. willkürlich erscheint (vgl. KK-StPO, 5. Auflage § 98 Rn. 15 mit weiteren Nachweisen).

d) Die in § 100b Abs. 1 Satz 4 und 5 StPO-E vorgesehene Verkürzung der Fristen sowohl für die Erst- als auch für die Verlängerungsanordnung erscheint weder aus rechtlichen noch aus tatsächlichen Gründen geboten.
Auch wenn in der Begründung des Regierungsentwurf – zutreffend – darauf hingewiesen wird, dass ausweislich der Untersuchung von Albrecht/Dorsch/Krüpe etwa ¾ der Telekommunikationsüberwachungsmaßnahmen lediglich über einen Zeitraum von bis zu 2 Monaten und nur etwa 9 % der Maßnahmen über einen Zeitraum von 3 Monaten durchgeführt werden, gilt es zu beden-

ken, dass dieser Prozentsatz namentlich in den Spezialabteilungen der Polizeibehörden und Staatsanwaltschaften für die Bekämpfung der internationalen Rauschgiftkriminalität, der sonstigen Erscheinungsformen der Organisierten Kriminalität sowie des Terrorismus höher ist. Für diese bereits jetzt besonders hoch belasteten Spezialdienststellen und -abteilungen gingen mit der beabsichtigten Fristverkürzung, da Verlängerungsanordnungen häufiger erforderlich würden, weitere, zusätzliche Belastungen einher.

Zudem achten Polizeibehörden und Staatsanwaltschaften selbst durchweg sorgsam darauf, dass aus tatsächlichen Gründen nicht mehr erforderliche beziehungsweise aus rechtlichen Gründen nicht mehr zulässige Maßnahmen gegebenenfalls auch weit vor Fristablauf beendet werden.

> *In der Zentralstelle für Betäubungsmittelstrafsachen der Staatsanwaltschaft Hannover, die für Ermittlungen wegen des Verdachts der bandenmäßigen Betäubungsmittelkriminalität und insoweit für die Landgerichtsbezirke Stade, Verden, Hildesheim, Bückeburg, Lüneburg, Hannover und Göttingen zuständig ist, sind in nahezu jedem Ermittlungsverfahren Maßnahmen zur Überwachung der Telekommunikation erforderlich. Von Rechts wegen, aber auch aufgrund des mit derartigen Maßnahmen stets einhergehenden hohen personellen und finanziellen Aufwands, bitten die zuständigen Polizeidienststellen aus Gründen der Beschleunigung die zuständigen Dezernentinnen und Dezernenten regelmäßig telefonisch, die Maßnahmen augenblicklich abschalten zu können, wenn diese nicht mehr geboten erscheinen.*

Diese Erfahrungswerte werden durch die vorgenannte Studie des Max-Planck-Instituts bestätigt. Danach kommen die Strafverfolgungsbehörden ihrer Verpflichtung nach, Maßnahmen zur Überwachung der Telekommunikation auch vor Fristablauf dann abzu-

schalten, wenn die Voraussetzungen für ihre Fortdauer nicht mehr vorliegen. Insoweit sei zitiert:

> *„Insgesamt ergibt sich aus diesen Verteilungen, dass die gesetzlich zulässig und gerichtlich ermöglichte Dauer der Überwachung bei weitem nicht ausgeschöpft wird. Die Praxis korrigiert somit selbst den in den Anordnungen erzeugten Überschuss an Überwachungs- und Eingriffspotential“ (vgl. S. 438).*

Zudem ist aufgrund der nach § 100b Abs. 2 Nr. 2 StPO-E vorgesehenen IMEI-Überwachung absehbar, dass Verlängerungsanordnungen künftig häufiger herbeizuführen sein werden, weil allein ein Kartenwechsel eine Neuanordnung nicht mehr erforderlich macht und dadurch die Begründung des Regierungsentwurfs jedenfalls insoweit ihre Tragfähigkeit verliert, als sie auf die – bisher – verhältnismäßig geringe Anzahl der Verlängerungsanordnungen abhebt.
Zu berücksichtigen ist weiter, dass es bei einer Beibehaltung der vorgesehenen – verkürzten – Fristenregelung zu einem weiteren statistischen Anstieg der Überwachungsanordnungen kommen wird und damit die rechtspolitische Diskussion weiter “angeheizt“ werden dürfte, im Rahmen derer, mit breiter Resonanz in der Öffentlichkeit, diskutiert und kritisiert wird, dass die Anzahl der Anordnungen zur Überwachung der Telekommunikation in der Bundesrepublik Deutschland jährlich kontinuierlich ansteigt.

Zu bedenken ist letztlich, dass die vorgesehene Verlängerungsfrist von zwei Monaten – wie im Übrigen jede andere Verlängerungsfrist auch – nicht voll ausgeschöpft werden kann. So ist eine Verlängerungsanordnung stets vor Ablauf der Erstanordnung herbeizuführen, um zu gewährleisten, dass keine Zeiträume entstehen, die nicht durch eine richterliche Überwachungsanordnung abgedeckt sind. Dieser Umstand wirkt sich umso deutlicher aus, je kürzer die Fristen sind.

e) Die in § 100b Abs. 1 Satz 5 StPO-E enthaltene Formulierung "soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen" sollte gestrichen werden. Zum einen bedürfen solche Selbstverständlichkeiten, dass die Strafverfolgungsbehörden die im Rahmen der Erstanordnung gewonnenen Ermittlungsergebnisse bei der Frage über die Notwendigkeit einer Verlängerung berücksichtigen, keiner besonderen Erwähnung.

Zum anderen könnte die Formulierung zu der – rechtsfehlerhaften – Auslegung führen, dass eine Verlängerung dann unzulässig sei, wenn im Rahmen der Erstanordnung noch keine Feststellungen getroffen werden konnten, die geeignet sind, den bestehenden Tatverdacht bezüglich einer Katalogtat zu verifizieren.

> *Wie etwa soll der Fall beurteilt werden, in dem sich der Beschuldigte unmittelbar nach der Überwachungsanordnung ins Ausland begibt und seine Kommunikation deshalb über einen Zeitraum von mehreren Wochen nicht mehr aufgezeichnet werden kann?*

Namentlich dann, wenn Gegenstand der Anordnung nicht lediglich eine Straftat von besonderer Bedeutung bzw. eine schwere, sondern eine besonders schwere Straftat (vgl. etwa den Katalog in § 100c Abs. 2 StPO) ist, dürfte dieser Umstand einer Verlängerung nicht entgegenstehen.

f) Für die in § 100b Abs. 1 Satz 6 StPO-E vorgesehene Regelung, wonach das im Rechtzug übergeordnete Gericht über weitere Verlängerungen entscheidet, wenn die Dauer der Anordnung auf insgesamt 6 Monate verlängert worden ist, besteht weder unter praktischen noch unter rechtlichen Aspekten eine Notwendigkeit. Verlängerungsanordnungen über einen Zeitraum von 6 Monaten hinaus sind nicht nur außerordentlich selten, eine Kontrolle durch das im Rechtszug übergeordnete Gericht bringt für den Betroffe-

nen auch keinen effektiveren Rechtschutz mit sich. Insoweit ist zu bedenken, dass der Ermittlungsrichter das Verfahren zu diesem Zeitpunkt bereits über 6 Monate begleitet hat und damit mit dem Sach- und Rechtsstand im besonderen Maße vertraut ist. Darüber hinaus wird mit der beabsichtigten Konzentrationsregelung in § 162 StPO-E eine Kompetenzsteigerung der Ermittlungsrichter einhergehen. Schließlich ist zu berücksichtigen, dass sich die Richter des übergeordneten Gerichts vollständig in einen für sie neuen, zu diesem Zeitpunkt regelmäßig umfangreichen Sachverhalt einarbeiten müssten und damit weiterer Personalbedarf entsteht.

g) Zu begrüßen ist die Regelung in § 100b Abs. 2 Satz 2 Nr. 2 StPO-E, wonach als Kennung des zu überwachenden Kommunikationsanschlusses auch die Kennung des zu überwachenden Anschlusses oder Endgerätes ausreicht. Fraglich ist indes, wie die Regelung auszulegen ist, dass eine an der Kennung des Endgerätes anknüpfende Überwachung zulässig ist, “wenn diese (Kennung) allein dem zu überwachenden Endgerät zuzuordnen ist“. Zwar haben einzelne Telekommunikationsdienstleister wie etwa “T-Mobile“ im Rahmen der Diskussion zu dieser Problematik vorgetragen, im Einzelfall seien mehr als 1000 unterschiedliche Endgeräte mit derselben IMEI-Kennung festgestellt worden. Die Überprüfung, ob eine bestimmte IMEI nur einem oder aber mehreren Endgeräten zuzuordnen ist, kann von den Verpflichteten indes nicht vorgenommen werden. Hierzu sind allein die Telekommunikationsdienstleister in der Lage. Nach alledem sollte die Regelung dahingehend klargestellt werden, dass eine IMEI-basierte Überwachung stets statthaft ist, sofern zum Zeitpunkt der Anordnung keine sicheren Erkenntnisse dahingehend vorliegen, dass die in der Anordnung enthaltene Kennung des Endgerätes mehrfach vergeben bzw. illegal dupliziert wurde. Andernfalls wäre zu besorgen, dass vor Umsetzung der Anordnung die Strafverfolgungsbehörde eine aktive Prüfungspflicht dahingehend trifft, ob

die in der Anordnung enthaltene Kennung des Endgeräts mehrfach vergeben wurde.

h) Die Regelung in § 100b Abs. 4 Satz 2 StPO-E, wonach nach Beendigung der Maßnahme das anordnende Gericht über deren Verlauf und Ergebnisse zu unterrichten ist, ist nicht geeignet, das beabsichtigte Ziel, die Stärkung der mit dem Richtervorbehalt bezweckten rechtsstaatlichen Kontrolle, zu fördern. Sie ist auch nicht geboten, um das anordnende Gericht hinsichtlich einer Erfolgskontrolle ausreichend zu unterrichten.

In der ganz überwiegenden Mehrzahl der Verfahren, in denen Maßnahmen zur Überwachung der Telekommunikation durchgeführt werden, werden auch andere prozessuale Eingriffsmaßnahmen durchgeführt, für die ebenfalls der Ermittlungsrichter (künftig: „das Gericht“) zuständig ist. Diesem soll zudem die Zuständigkeit für weitere Ermittlungsmaßnahmen (Zuständigkeit für Erstanordnungen zur längerfristigen Observation, § 163f Abs. 3 Satz 1 StPO-E) übertragen werden.
Zudem wird das Gericht im Rahmen jedes Verlängerungsantrags der Staatsanwaltschaft, so ein solcher gestellt wird, umfänglich über den Erfolg der bisherigen Maßnahmen unterrichtet. Dem Antrag der Staatsanwaltschaft ist regelmäßig eine Verlängerungsanregung der sachbearbeitenden Polizeidienststelle vorangestellt, in der die wesentlichen bisherigen maßnahmenspezifischen Ergebnisse ausführlich dargelegt sind.

In Verfahren mit verdeckten Ermittlungsmaßnahmen liegen die Ermittlungsakten mithin regelmäßig dem Ermittlungsrichter vor, der dadurch in kurzen Abständen die – notwendige – Rückmeldung erhält. Hinzu kommen nach Offenlegung der Ermittlungen weitere Vorlagen im Zusammenhang mit Haftprüfungsanträgen, Beschwerdeent-

scheidungen und sonstigen Maßnahmen, mit denen jeweils eine Sachprüfung einhergeht.

Darüber hinaus bleibt unklar, wie das anordnende Gericht über Verlauf und Ergebnisse der Maßnahmen zu unterrichten ist.

i) **§§ 100a, 100b StPO Gesetzentwurf der Fraktion Bündnis 90/Die Grünen**

Die dort vorgesehenen Neuregelungen dürften zur Erreichung der in der Entwurfsbegründung dargelegten Ziele nicht geeignet sein.

Bei der Einführung eines allgemeinen Kriterienkataloges statt eines Anlasstatenkatalogs, wie es § 100a Abs. 2 StPO-E Entwurf der Fraktion Bündnis 90/Die Grünen vorsieht, wären Maßnahmen zur Überwachung der Telekommunikation bei mehr Straftatbeständen als bisher statthaft.

Die weiter nach § 100b Abs. 1 Satz 1-E Entwurf Bündnis 90/Die Grünen vorgesehene Regelung, wonach die Anordnung nach § 100a StPO auf einen zu begründenden Antrag der Staatsanwaltschaft durch einen nach § 10 des Deutschen Richtergesetzes auf Lebenszeit ernannten Richter zu treffen sei, führt zu keiner effektiveren rechtstaatlichen Kontrolle.
Jedenfalls für den Bereich des sehr speziellen Rechts der Telekommunikationsüberwachung gewährleistet ein höheres Dienstalter nicht zugleich eine höhere Kompetenz. Diese wird vielmehr allein dadurch erreicht, dass sich Staatsanwältinnen und Staatsanwälte sowie Richterinnen und Richter mit der Problematik eingehend befassen. Dies kann indes bei einem Richter auf Probe ebenso der Fall sein wie bei einem auf Lebenszeit ernannten Richter.
Zudem wäre die beabsichtigte Zuständigkeitsregelung systemwidrig. Weder nach geltendem noch nach künftigem Recht sind ähnlich schwerwiegende oder gar noch gravierendere Grund-

rechtseingriffe wie die Anordnung eines dauerhaften Freiheitsentzugs auf der Grundlage eines Haftbefehls nach Maßgabe der § 112 StPO ebenfalls auf Lebenszeit ernannten Richtern vorbehalten.

Sachgerecht erscheint die Regelung in § 100b Abs. 4 Satz 3 StPO-E Entwurf Bündnis 90/Die Grünen. Sie entspricht einer bereits vielfach geübten Praxis, ohne dass dadurch die berechtigten Interessen der Kommunikationsdienstleister eine Beeinträchtigung erfahren würden.

4. Zu § 100f StPO-E

Da § 100f Abs. 4 StPO-E auf die Regelung auf die Vorschriften in § 100b Abs. 1 StPO-E verweist, kann auf die obigen Ausführungen zu § 100b Abs. 1 StPO-E verwiesen werden.

5. Zu § 100g StPO-E

a) Nachdrücklich zu unterstützen ist die in § 100g Abs. 1 StPO-E enthaltene sprachliche und inhaltliche Angleichung an die Verkehrsdaten gemäß § 96 Abs. 1 TKG und die Ausgestaltung dieser Vorschrift als Befugnisnorm zur Erhebung von Verkehrsdaten auch in Echtzeit.

b) Soweit § 100g Abs. 2 Satz 1 StPO-E unter anderem auf § 100b Abs. 1 Satz 3 bis 6 StPO-E verweist, wird ebenfalls auf die dortigen Ausführungen Bezug genommen.

c) Die Regelung in § 100g Abs. 4 StPO-E führt, in Verbindung mit den weiter vorgesehenen Berichtspflichten, zu einer weiteren Ressourcenverknappung bei den Strafverfolgungsbehörden; de-

ren personelle und sachliche Mittel sollten vorrangig für eine effektive und geordnete Strafverfolgung eingesetzt werden.

6. Zu § 100i StPO-E

a) § 100i StPO-E sollte dahingehend ergänzt werden, dass er eine Verpflichtung der Telekommunkationsdienstleister erhält, wonach diese den berechtigten Stellen die Standortdaten des lediglich aktiv geschalteten Mobilfunkendgerätes mitzuteilen haben. Diese Forderung basiert auf der Erwägung, dass der Einsatz eines IMSI-Catchers überhaupt nur möglich ist, wenn den Strafverfolgungsbehörden der ungefähre Standort des Betroffenen bereits bekannt ist. Ebenso wenig wie die Regelung des § 100i StPO-E berührt eine entsprechende Mitteilungspflicht der Telekommunikationsdienstleiter das Fernmeldegeheimnis nicht. Auch insoweit kann auf die eingangs zitierte Entscheidung des Bundesverfassungsgerichts verwiesen werden, in der zutreffend darauf hingewiesen wird, dass die technische Eignung eines Gerätes, als Kommunikationsmittel zu dienen, sowie die von dem Gerät ausgehenden technischen Signale zur Gewährleistung der Kommunikationsbereitschaft keine Kommunikation im Sinne von Art. 10 GG darstellen. Sie ermöglichten, so das Bundesverfassungsgericht weiter, anders als Kommunikationsumstände, keinen Rückschluss auf das Kommunikationsverhalten bzw. auf Kommunikationsinhalte. Vielmehr qualifiziere erst die tatsächliche Nutzung zum Austausch von Informationen und Meinungen mit den Telekommunikationseinrichtungen die so übertragenen Daten als dem Schutzbereich des Art. 10 Abs. 1 GG unterfallende Kommunikationsinhalte bzw. -umstände.

b) Soweit § 100i Abs. 2 Satz 2 StPO-E regelt, dass aus technischen Gründen erhobene personenbezogene Daten über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus nicht verwendet werden dürfen und unverzüglich zu lö-

schen sind, dürfte ein Beweiserhebungs- und Beweisverwertungsverbot hinsichtlich dieser Daten jedenfalls dann nicht bestehen, wenn bezüglich des Betroffenen parallel auch Anordnungen gemäß §§ 100a, 100b bzw. 100g, 100h StPO ergangen sind.

Erlaubt eine zeitgleich bestehende Überwachungsanordnung gemäß §§ 100a, 100b StPO die Überwachung der Telekommunikation, dürften auf der Grundlage dieses Beschlusses mittels IMSI-Catcher auch Gesprächsinhalte aufgezeichnet werden.

c) In dem Umfang, in dem § 100i Abs. 3 Satz 1 StPO-E auf § 100b Abs. 1 Satz 3 StPO-E verweist, wird auf die dort gemachten Anmerkungen verwiesen.

7. Zu § 101 StPO-E

a) Die vorgesehenen Benachrichtigungs-, Kennzeichnungs- und Vernichtungsregelungen werden die Strafverfolgungsbehörden insbesondere durch die der Benachrichtigungspflicht regelmäßig vorausgehende Recherche vor einen kaum lösbaren Verwaltungsaufwand stellen.

Die in § 101 Abs. 4 Satz 5 StPO-E enthaltene Regelung, wonach Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person nur vorzunehmen sind, „wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands der Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist“, dürfte nicht geeignet sein, den insgesamt zu erwartenden Verwaltungsaufwand auf ein beherrschbares Maß zu reduzieren.

Verfassungsrechtliche Aspekte, insbesondere die Rechtsprechung des Bundesverfassungsgerichts, gebieten die vorgesehene

extensive und von der Praxis nicht zu bewältigende Benachrichtigungspflicht jedenfalls nicht.

So hat das Bundesverfassungsgericht im Rahmen seiner bereits zitierten Entscheidung vom 22.08.2006 zu § 100i StPO-E ausgeführt, dass es angesichts der geringen Eingriffstiefe nicht unverhältnismäßig sei, auf die Benachrichtigung mitbetroffener Dritter zu verzichten (vgl. Rdnr. 77). Dem wird bei Maßnahmen nach § 100i StPO in § 101 Abs. 4 Satz 1 Nr. 8 StPO-E Rechnung getragen.
Zweifelhaft erscheint jedoch, ob die verfassungsgerichtliche Rechtsprechung die in § 101 Abs. 4 Satz 1 Nr. 3 und 6 StPO-E vorgesehene Benachrichtigung aller Beteiligten der überwachten beziehungsweise betroffenen Telekommunikation zwingend erforderlich erscheinen lässt. Welcher Verwaltungsaufwand insbesondere mit der in § 101 Abs. 4 Satz 1 Nr. 3 StPO-E vorgesehenen Benachrichtigungspflicht verbunden ist, wird besonders in den die Strafverfolgungsbehörden ohnehin schon erheblich belastenden Verfahren der schweren und Organisierten Kriminalität deutlich.

> *In komplexen Ermittlungsverfahren, in denen die Telekommunikation mehrerer Beschuldigter sowie deren Nachrichtenmittler überwacht werden muss, fallen unter Umständen 50.000 bis 80.000 Gesprächsdatensätze an. In einem zzt. vor dem Landgericht Hannover verhandelten Verfahren waren es 82.500 Datensätze.*

In derartigen Verfahren erfordert allein die Vorprüfung, in welchen Fällen Nachforschungen zur Feststellung der Identität der Betroffenen „unter Berücksichtigung der Eingriffsintensität (...) geboten“ sind, einen nicht zu bewältigenden Verwaltungsaufwand.
Auch wenn jedenfalls in Verfahren der schweren Rauschgiftkriminalität die Tatverdächtigen regelmäßig mit der Überwachung ihrer Kommunikation rechnen, ihre Gespräche deshalb „verschlüsseln“

und damit in Gesprächen häufig keine oder aber nur wenige das Persönlichkeitsrecht betreffende Inhalte übermitteln und zahlreiche Gespräche zudem von denselben Personen geführt werden, verbleibt in Umfangsverfahren gleichwohl eine hohe Anzahl von Gesprächen, die nach dem vorstehenden Maßstab zu überprüfen sind. Die Entscheidung der Frage, ob eine Benachrichtigung „unter Berücksichtigung der Eingriffsintensität (…) geboten“ erscheint, erfordert zudem verstärkt eine rechtliche Bewertung. Hinsichtlich zahlreicher Gespräche wird eine solche Bewertung allein von der Staatsanwaltschaft durchgeführt werden und wird deshalb absehbar zu weiteren Mehrbelastungen führen.

Insgesamt dürfte der mit der vorgesehenen Benachrichtigungspflicht verbundene Mehraufwand die Ressourcen namentlich der auf die Verfolgung der schweren und Organisierten Kriminalität sowie des Terrorismus spezialisierten Dienststellen in einem solchen Maße binden, dass diese künftig allein aufgrund der Benachrichtigungspflichten entweder andere bzw. weitere gebotene Ermittlungsmaßnahmen nicht mehr werden durchführen können oder aber auch hier weiterer Personalbedarf entsteht.
Nur selten wird sich darüber hinaus feststellen lassen, ob der Gesprächspartner des Beschuldigten überhaupt mit dem Anschlussinhaber des von diesem angewählten Endgeräts identisch ist, sodass häufig Ungewissheit über die Identität der zu benachrichtigenden Person bestehen wird. Um einen effektiven Rechtsschutz der Beteiligten zu gewährleisten, müssten in die Benachrichtigungsschreiben zudem bestimmte Grundinformationen wie die Person des Beschuldigten, der gegen diesen bestehende Tatverdacht sowie die näheren Umstände der Kommunikation aufgenommen werden, sodass einer Vielzahl von Personen das gegen den Beschuldigten geführte Ermittlungsverfahren bekannt würde.

b) Auch die Regelung des § 101 Abs. 9 StPO-E sollte überdacht werden. Zwar wird in der Begründung (vgl. S. 141) zutreffend

darauf hingewiesen, dass bei tiefgreifenden Grundrechtseingriffen ein Rechtschutzbedürfnis auch nach Beendigung der Maßnahme zu bejahen ist und stellen Maßnahmen zur Überwachung der Telekommunikation grundsätzlich einen tiefgreifenden Grundrechtseingriff dar.

Zu bedenken ist jedoch auch, dass zahlreiche gem. § 101 Abs. 4 Satz 3 Nr. 3 und 6 StPO-E überwachte Personen nur gelegentlich, unter Umständen nur durch ein einziges Telefonat betroffen sind, nach § 101 Abs. 9 Satz 2 StPO-E für die Entscheidung über den nachträglichen Rechtschutz (jedenfalls regelmäßig) der Ermittlungsrichter zuständig ist und eine nach der vorgesehenen Regelung des § 101 Abs. 9 StPO-E jedenfalls mögliche Flut von Beschwerden von diesem nicht bewältigt werden könnte. Angesichts dieser Umstände sollte die Prüfung erwogen werden, ob ein Rechtsschutzbedürfnis nur für diejenigen “sonst überwachten Personen“ vorgesehen werden sollte, bei denen es sich - entsprechend der Regelung in § 101 Abs. 4 Satz 1 Nr. 9b StPO-E – um ebenfalls „erheblich mitbetroffene Personen“ handelt.

8. Zu § 110 Abs. 3 StPO-E

a) Die durch § 110 Abs. 3 Satz 1 StPO-E ermöglichte elektronische Durchsicht solcher räumlich getrennten Speichermedien, zu denen der Betroffene zugangsberechtigt ist, ist ebenso wie die in § 110 Abs. 3 Satz 2 StPO-E enthaltene Befugnis, solche Daten, die für die Untersuchung von Bedeutung sein können, zu speichern, nachdrücklich zu begrüßen.

Von der Regelung nicht erfasst wird hingegen der technisch mögliche, heimliche “Online-Zugriff“ auf zugangsgeschützte Datenbestände. Wohl mehr noch als die von § 110 Abs. 3 Satz 1 StPO-E erfasste offene Durchsicht elektronischer Speichermedien wäre die heimliche (Online-)Durchsuchung derartiger Medien, insbesondere in Fällen der schweren und Organisierten Kriminalität

sowie in Staatsschutzsachen in besonderer Weise geeignet, den Sachverhalt aufzuklären.

Die rechtliche Statthaftigkeit einer solchen Maßnahme war umstritten. So hatte der Ermittlungsrichter beim Bundesgerichtshof in seinem Beschluss vom 21.02.2006 – 3 BGs 31/06 – noch angemerkt, eine Maßnahme, durch die ein hierfür eigens konzipiertes Computerprogramm von außen auf dem Computer des Beschuldigten installiert wird, um die dort abgelegten Daten zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden zu übertragen, sei durch § 102 StPO selbst dann gedeckt, wenn sich der PC des Beschuldigten in der Wohnung eines Dritten befinden sollte. Die Durchsuchung, so der Ermittlungsrichter beim BGH weiter, sei keine Maßnahme, die nach ihrer Rechtsnatur stets und ausnahmslos offen durchgeführt werden müsse. Weder den materiellen noch den formellen Zulässigkeitsvoraussetzungen einer Durchsuchungsanordnung seien Einschränkungen dahingehend zu entnehmen, dass derartige Maßnahmen “stets nur offen möglich sein“ sollten (Seite 6 BA).

Diese Auffassung, die im Schrifttum vereinzelt Zustimmung gefunden hat (Hofmann NStZ 2005, 121 ff.), teile ich aus den oben (vgl. II. 2.) sowie nachfolgend dargelegten Gründen nicht.

b) Demgegenüber hatte der Ermittlungsrichter beim Bundesgerichtshof im Rahmen seines Beschlusses vom 25.11.2006 - 1 BGs 184/06 - einen erneuten, entsprechenden Antrag der Generalbundesanwältin nunmehr mit der Begründung abgelehnt, bei einem heimlichen Zugriff auf die auf dem Computer des Beschuldigten gespeicherten Daten handele es sich um einen schwerwiegenden Eingriff in die persönlichen Freiheitsrechte des Betroffenen. § 102 StPO biete für die heimliche Ausforschung eines Computers keine geeignete Rechtsgrundlage, da diese Maßnahme “eine im Grundsatz auf Offenheit angelegte Maßnahme“ sei. Es könne dahingestellt bleiben, ob die Bestimmung, wonach nach einer Durchsuchung gem. § 105 Abs. 2 StPO Zeugen hinzuzuziehen seien, lediglich eine Ordnungsvorschrift enthalte. Auch bei

solchen Vorschriften stehe “deren Einhaltung nicht zur beliebigen Disposition der Normadressaten“ (Seite 4 BA).

Diese Entscheidung, gegen die Beschwerde eingelegt wurde, ist durch den 3. Strafsenat des Bundesgerichtshofs in seinem Beschluss vom 31.01.2007 – StB 18/06 – bestätigt worden. Der Beschluss verdient Zustimmung, weil eine solche Maßnahme nach geltendem Recht nicht zulässig ist. Dies allerdings nicht, wie in der öffentlichen Diskussion gelegentlich verkannt, wegen der Schwere des mit der Maßnahme verbundenen Eingriffs; unzulässig ist die Maßnahme allein, weil das geltende Recht ihre heimliche Durchführung nicht zulässt. Bei – offenen – Durchsuchungen von Wohnungen werden regelmäßig die elektronischen Datenspeicher von Computern beschlagnahmt und „durchsucht“. Darüber hinaus ist das Merkmal der Heimlichkeit einer Ermittlungsmaßnahme allein nicht geeignet, eine solche als schweren Eingriff zu qualifizieren. Dies gilt beispielsweise für die heimlich durchgeführte kurzfristige wie längerfristige Observation gemäß §§ 161, 163 StPO bzw. gemäß § 163f StPO. Letztere kann sich im Einzelfall jedoch, je nach konkreter Ausgestaltung und Dauer, als ein schwerwiegenderer Eingriff darstellen.

Anzumerken ist indes, dass die verdeckte, sprich heimliche Durchsuchung von Datenspeichern für eine effektive Strafverfolgung zwingend erforderlich ist. Ein Beispiel:

> *In aktuell verdeckt geführten Ermittlungsverfahren nutzen Straftäter den Kommunikationsdienst „Skype“. Mit diesem telefonieren sie kostenlos via Internet bzw. verschicken E-Mails. Diese Art der Kommunikation ist während ihrer paketvermittelten Übertragung nicht zu entschlüsseln*. Die einzige Möglichkeit, die Inhalte der E-Mails, die sich nach anderweitigen, gesicherten Erkenntnissen auf strafbare Handlungen beziehen, verdeckt zur Kenntnis zu nehmen ist eine „Online-Überwachung“.

c) Der Zugriff auf räumlich getrennte Speichermedien wirft indes, im Falle des § 110 Abs. 3 StPO-E ebenso wie im Rahmen einer „Online-Durchsuchung, weitere verfassungsrechtliche Fragen auf.

So die Frage, ob das durch das Urteil des Bundesverfassungsgerichts vom 02.03.2006 – 2 BvR 2099/04 (NStZ 2006, 641 ff.) – konkretisierte Grundrechtsverständnis eine präzise Konturierung des Schutzbereichs von Art. 10 Abs. 1 GG auch in den Fällen solch neuartiger Übertragungstechniken ermöglicht, wie sie in den vorgenannten Beispielsfall zur Anwendung kamen.

Moderne Programme und Provider bieten eine Vielzahl neuartiger und zu zusätzlichen Abgrenzungsproblemen führender Kommunikationsmöglichkeiten an. So kann, um bei den vorgenannten Beispielsfall zu bleiben, im Unterschied zur herkömmlichen E-Mail-Kommunikation, die E-Mail auch direkt im physikalischen Speicher des Mail-Servers im Internet mittels Browser “online“ erstellt werden. Die Übertragung der fertig gestellten Datei vom physikalischen Speicher im Computer des Absenders auf den Mail-Server des Providers entfällt. Die Daten können bis zu ihrer Versendung ebenso wie im eigenen Computer des Kommunizierenden bearbeitet und gelöscht werden. Entsprechendes gilt für versandte und auf den Mail-Server eingegangene E-Mails. Auch sie können dort gelesen und gelöscht werden, ohne dass es eines weiteren Übertragungsvorganges in den Herrschaftsbereich des Telekommunikationsteilnehmers bedarf. In beiden Fällen kann zwar “der Nutzer die Löschung sicher bewirken“, dies ist jedoch nach der vorstehend zitierten Entscheidung des 2. Senats des Bundesverfassungsgerichts “nicht entscheidend“ (vgl. dort Rdnr. 79), wenn zugleich eine “erleichterte Zugriffsmöglichkeit Dritter besteht, in der sich das spezifische Risiko aus der Nutzung einer Fernmeldeeinrichtung“ (vgl. aaO Rn. 81) verwirklicht. Dies ist in den vorgenannten Konstellationen der Fall, weshalb eine Erhebung und

Verwertung der übertragenen und auf dem Server eingegangenen E-Mails zu strafprozessualen Zwecken das Fernmeldegeheimnis berührt.
Bei den Entwürfen, nicht adressierten, jedenfalls noch nicht versandten, zwischengespeicherten E-Mails erscheint dies indes fraglich, weil Art. 10 GG "die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs" (BVerGE aaO Rn. 66) schützt und der eigentliche Übertragungsvorgang hier noch nicht begonnen hat. Hierin dürfte sich diese Form der Zwischenspeicherung auch von derjenigen während des Übertragungsvorganges unterscheiden. Von einem solchen dürfte vielmehr erst dann gesprochen werden können, wenn der Absender diesen dergestalt initiiert hat, dass die Nachricht ohne sein weiteres Zutun bei ungestörtem Fortgang unmittelbar in den Empfangsbereich des Adressaten übermittelt wird.

Zwar besteht auch bei den noch nicht versandten E-Mails die Gefahr eines staatlichen Zugriffs. Der mit den technischen Möglichkeiten einhergehenden gesteigerten Gefährlichkeit kann hier jedoch durch einen Schutz nach Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG, dem Recht auf informationelle Selbstbestimmung, Rechnung getragen werden. Als Eingriffsgrundlage könnte hier auf § 94 StPO zurückgegriffen werden (vgl. Urteil des 2. Senats des BVerfG vom 12.04.2005 – 2 BvR 1027/02, Rdnr. 82).

> *In strafprozessualen Ermittlungsverfahren ist vermehrt festzustellen, dass Straftäter auch diese technischen Gegebenheit zur Kommunikation dergestalt nutzen, dass der „Absender" tatrelevante Informationen lediglich als E-Mail-Entwurf auf dem Server seines E-Mail Providers speichert, diesen Entwurf an seinen Mittäter und Nachrichtenempfänger nicht versendet. Jener teilt diesem vielmehr seine, des Absenders, Zugangberechtigung mit, sodass der Mittäter Zugriff auf den E-Mail Account des „Absen-*

ders“ hat und die dort für ihn hinterlegte Nachricht zur Kenntnis nehmen kann, ohne dass eine Übertragung an diesen im „traditionellen“ Sinne erforderlich wäre.

Wie sich das Bundesverfassungsgericht zu der gesamten Problematik letztlich stellen wird, dürfte derzeit nicht abzusehen sein. Mit der Frage befasst ist es zwischenzeitlich. So hat die III. Kammer des 2. Senats des Bundesverfassungsgerichts in ihrer Entscheidung vom 29.06.2006 gemäß §§ 32 Abs. 1, § 93d Abs. 2 BVerfGG – 2 BvR 902/06 – die betroffene Staatsanwaltschaft angewiesen, “sämtliche Datenträger, auf denen die von dem Provider zur Verfügung gestellten Daten des E-Mail-Accounts des Beschwerdeführers gespeichert sind, sowie sämtliche Schriftstücke, auf denen der Inhalt der Dateien aus dem E-Mail-Account sichtbar gemacht wurde, beim Amtsgericht in Verwahrung zu geben“. Zugegriffen wurde hier durch die Strafverfolgungsbehörde auf der Grundlage der §§ 94, 98 StPO auf ungefähr 2500 E-Mails, die der Beschwerdeführer seit Jahresbeginn 2004 bis zum Tage der Durchsuchung im März 2006 auf einem externen Speicher im Herrschaftsbereich seines Providers abgelegt, sprich archiviert hatte.

Mit einer abschließenden Entscheidung in dieser Sache dürfte zeitnah nicht zu rechnen sein. Deshalb wäre es aus Sicht der Strafverfolgungsbehörden außerordentlich zu begrüßen, wenn der Gesetzgeber den Strafverfolgungsbehörden auch die verfassungsrechtlich zulässige Möglichkeit einer „Online-Durchsuchung“ eröffnen würde.

9. Zu § 162 StPO-E

Die Konzentrationsregelung des § 162 Abs. 1 Satz 1 StPO-E ist nachdrücklich ist sachgerecht. Sie dürfte augenblicklich zu der beabsichtigten Vereinfachung, Beschleunigung und Kompetenzbündelung führen. Bei den Amtsgerichten, in deren Bezirk die

Staatsanwaltschaft ihren Sitz hat, sind die Ermittlungsrichterdezernate aufgrund des Geschäftsanfalls zumeist und überwiegend „volle Dezernate“, so dass die dort tätigen Richterinnen und Richter, gleich ob bereits auf Lebenszeit ernannt oder nicht, aufgrund des Geschäftsanfalls tagtäglich auch mit telekommunikationsrechtlichen Fragestellungen befasst werden. Die sich hier ergebenden Probleme und Fragestellungen sind ihnen regelmäßig geläufiger als den Richterinnen und Richtern der anderen Amtsgerichte.

10. Zu § 163 f StPO-E

Um einen effektiven vorbeugenden Rechtsschutz der von einer längerfristigen Observation betroffenen Person zu gewährleisten, soll durch § 163f Abs. 3 Satz 1 StPO-E auch die Erstanordnung dieser Maßnahme dem Richtervorbehalt unterstellt werden.

Auch wenn die Maßnahme, namentlich dann, wenn sie mit dem Einsatz technischer Mittel gemäß § 100h StPO-E verbunden wird, zu erheblichen Eingriffen in das Recht auf informationelle Selbstbestimmung führen kann, dürfte die Rechtsprechung des Bundesverfassungsgerichts zum „additiven Grundrechtseingriff“ (BVerfG NJW 2005, 1338, 1341), auf den die Begründung u. a. verweist (S. 151), einen Richtervorbehalt nicht erforderlich machen.

Zum einen sind sämtliche mit schwerwiegenden Eingriffen in Grundrechte verbundenen Ermittlungsmaßnahmen einem Richtervorbehalt unterstellt. In den Fällen, in denen es zu einer Kumulierung von Ermittlungsmaßnahmen wie in dem vom Bundesverfassungsgericht entschiedenen Fall käme, wäre eine richterliche Kontrolle bereits durch den Richtervorbehalt bei der Überprüfung dieser eingriffsintensiven Maßnahmen gewährleistet.

Zum anderen ist nach den hier vorliegenden langjährigen Erfahrungen die rechtsstaatliche Kontrolle, die die Staatsanwaltschaft im Rahmen des Ermittlungsverfahrens als ein der dritten Gewalt

zuzurechnendes Organ der Rechtspflege ausübt, der ermittlungsrichterlichen Kontrolle durchweg vergleichbar.

Die Staatsanwaltschaft prüft die regelmäßig von der Polizei initiierten Eingriffsmaßnahmen auf deren Recht- und Zweckmäßigkeit und bescheidet diese Anregungen - ohne dass beides stets einen Niederschlag in den Akten findet – gegebenenfalls abschlägig.
Anträge auf den Erlass richterlicher Anordnungen zur Überwachung der Telekommunikation beziehungsweise ähnlich eingriffsintensiver Maßnahmen stellt sie durchweg nach sorgfältiger Prüfung der Sach- und Rechtslage. Durch keine hier bekannte Studie ist belegt, dass die staatsanwaltschaftliche Sachbearbeitung der richterlichen nachsteht. Gegenteiliges ergibt sich weder aus der Studie des Max-Planck-Instituts zur Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen noch aus der Studie von Backes und Gusy von der Universität Bielefeld.
Vielmehr kommt die Studie des Max-Planck-Instituts zu der Feststellung, dass die Bedarfsträger von dem gesetzlichen Ermittlungsinstrumentarium der §§ 100a, 100b bzw. 100g, 100h StPO durchweg verantwortungsbewusst Gebrauch machen. Die hier beschriebenen Defizite betreffen in erster Linie die Inhalte der richterlichen Anordnungsbeschlüsse sowie die Benachrichtigungspflicht nach § 101 StPO.

11. Zu § 477 Abs. 2 StPO-E

§ 477 Abs. 2 Satz StPO-E regelt die Verwendung personenbezogener Daten für Beweiszwecke in anderen Strafverfahren. Die Vorschrift geht ausweislich der Begründung (vgl. S. 153) u. a. auf das dieses ersetzende „Regelungsvorbild“ des § 100b Abs. 5 StPO (a. F.) zurück. § 477 Abs. 2 StPO-E legt nunmehr fest, dass eine Verwendung der gewonnen Daten „zu Beweiszwecken in anderen Strafverfahren nur zur Aufklärung solcher Straftaten ver-

wendet werden (dürfen), zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz hätte angeordnet werden dürfen.“ Die Beibehaltung der Verwendungsregelung „zu Beweiszwecken“ sowie der Umstand, dass der Neuregelung ausweislich der weiteren Begründung der Gedanke des „hypothetischen Ersatzeingriffs“ zugrunde liegt, machen deutlich, dass solche Zufallserkenntnisse, die eine sich nicht als Katalogtat darstellende andere prozessuale Tat betreffen, in Übereinstimmung mit der bisherigen höchstrichterlichen Rechtsprechung weiterhin nicht unmittelbar zu Beweiszwecken, wohl aber als Spurenansatz zu weiteren Ermittlungen verwendet werden dürfen. So vertritt das BVerfGE (III. Kammer des 2. Senats, Beschluss vom 29.06.2005 – 2 BvR 866/05, NJW 2005, 2766) im Einklang mit der Rechtsprechung des BGH (BGH NStZ 1996, 200, 201; 1998, 426, 427) die Auffassung, dass rechtmäßig gewonnene Zufallserkenntnisse, die nicht Katalogtaten betreffen, zwar nicht unmittelbar zu Beweiszwecken verwertet werden dürfen; sie können aber Anlass zu weiteren Ermittlungen zur Gewinnung neuer Beweismittel sein. Dies sollte in der Begründung des Regierungsentwurfs deutlicher hervorgehoben werden.

Diese Rechtsprechung berücksichtigt einerseits den Schutz des betroffenen Grundrechts, indem weitergehende Ermittlungen nur in den Fällen für zulässig gehalten werden, in denen die Maßnahme nach der jeweiligen Katalogtat rechtmäßig war, berücksichtigt andererseits jedoch auch das Interesse an einer wirksamen Strafrechtspflege. Nach – zutreffender – Auffassung des BGH können auf derartige Zufallserkenntnisse auch Zwangsmaßnahmen gestützt werden. Diese Rechtsprechung ist namentlich für eine Bekämpfung der schweren und Organisierten Kriminalität von gerade herausragender Bedeutung.

12. Zu § 111 TKG-E

a) Zustimmung verdient die Regelung in § 111 Abs. 1 Nr. 5 TKG-E, wonach dann, wenn dem Kunden ein Mobilfunkendgerät überlassen wird, dessen Gerätenummer zu erheben und zu speichern ist. Die Vorschrift korrespondiert mit der des § 100b Abs. 2 Nr. 2 StPO-E, die nunmehr auch eine IMEI-Überwachung vorsieht.

b) Aus Sicht der Strafverfolgungsbehörden sollte darüber hinaus eine Verifikationspflicht der Provider bezüglich derjenigen Daten eingeführt werden, die eine Identifizierung des Kunden ermöglichen. Dies erscheint für eine geordnete, effiziente und damit nachdrückliche Strafverfolgung unumgänglich. So ist den berechtigten Stellen wiederholt als Kundennamen “Dagobert Duck“ mitgeteilt worden.
Soll namentlich die Verpflichtung des § 111 Abs. 1 Nr. 2 bis 4 TKG-E nicht leerlaufen, sollte die – in der Vergangenheit wiederholt diskutierte – Frage der Verifikationspflicht in dem Sinne einer Lösung zugeführt werden, dass diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, sich die Richtigkeit der Personalien anhand eines amtlichen Ausweises bestätigen lassen müssen.

13. Auskunftsersuchen nach § 113 TKG:

In § 113 TKG sollte eine Klarstellung dahingehend erfolgen, dass die Auskunft über den Inhaber einer dynamischen IP-Adresse allein auf ein Auskunftsersuchen nach dieser Vorschrift gestützt werden kann. Zwar wird in der Begründung des Regierungsentwurfs (vgl. Seite 53) die Problematik aufgegriffen, ein Regelungsbedarf jedoch mit der Erwägung verneint, insoweit existiere bereits eine zutreffende und gefestigte Rechtsprechung.

Die zitierte Rechtsprechung, die sich ausschließlich auf Entscheidungen der Landgerichte stützt, wird von einzelnen Telekommunikationsdienstleistern nicht anerkannt.

> *Nach wie vor werden von diesen in deutlich mehr als nur wenigen Einzelfällen Beschlüsse nach §§ 100g, 100h StPO verlangt. Selbst ein Hinweis auf die Erörterung und Bewertung der Problematik in der Begründung des Gesetzentwurfs (Fassung vom 18. April 2007) bewog die betreffenden Telekommunikationsdienstleister nicht dazu, ihre Auffassung aufzugeben.*
>
> *In einem diese Problematik betreffenden Fall hat eine Staatsanwaltschaft nach der wiederholten Weigerung des Telekommunikationsdienstleisters, die Daten auf der Grundlage des § 113 TKG zu beauskunften, einen richterlichen Durchsuchungsbeschluss mit dem Ziel erwirkt, die Geschäftsräume des Telekommunikationsdienstleisters zu durchsuchen und die betreffenden Daten zu beschlagnahmen. Im Rahmen der Vollstreckung blieben die Vertreter des betreffenden Telekommunikationsdienstleisters auch nach Kenntnisnahme von der richterlichen Rechtsauffassung bei ihrer Weigerungshaltung und stellten den die Durchsuchung durchführenden Beamten - das diesen unmögliche Unterfangen - anheim, sich die Daten von den Servern selbst zu kopieren.*

14. Zu § 113a TKG-E

Die in 113a Abs. 1 TKG-E enthaltene Verpflichtung zur Speicherung von Verkehrsdaten für einen Zeitraum von 6 Monaten ist ebenfalls begrüßenswert. Die in Satz 1 enthaltene Regelung, wonach sich diese Speicherpflicht auf solche Verkehrsdaten beschränkt, die bei der Nutzung des Telekommunikationsdienstes erzeugt oder verarbeitet werden, erscheint sachgerecht.

Für die in § 113a Abs. 7 TKG-E vorgesehene Verpflichtung, neben den Funkzellendaten auch die Hauptstrahlrichtung der Funkantennen mitzuteilen, besteht in der strafprozessualen Praxis erheblicher Bedarf. Die Regelung trägt zum einen dem Umstand Rechnung, dass zwischenzeitlich nahezu sämtliche Funkzellen sektoriert und den Telekommunikationsdienstleistern entsprechende Angaben mithin möglich sind. Die ausdrückliche Erwähnung der Hauptstrahlrichtung der Funkantennen ist namentlich auch vor dem Hintergrund von Bedeutung, dass auch § 7 Abs. 1 Nr. 7 TKÜV die Telekommunikationsdienstleister verpflichtet, bezüglich der zu überwachenden Kennung aus Mobilfunknetzen Angaben zum Standort des Mobilfunkgerätes mit der größtmöglichen Genauigkeit mitzuteilen, diese – technisch mögliche – Mitteilung der Hauptstrahlrichtung der Funkantennen in der Vergangenheit jedoch wiederholt verweigert worden war.

Ungenügend erscheint die Regelung in § 113a Abs. 9 TKG-E, wonach die Speicherung der Daten so zu erfolgen hat, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können. Diese Regelung dürfte jedenfalls nicht geeignet sein, den ausweislich der Begründung mit ihr beabsichtigten Zweck zu erreichen, wonach die Daten von dem Verpflichteten in einer Weise gespeichert werden, die eine effektive und schnelle Recherche zulassen soll, so dass erforderliche Auskünfte unverzüglich erteilt werden können.
Namentlich die Erfahrungen im Rahmen der Telekommunikationsüberwachung bzgl. der nach § 7 TKÜV zu übermittelnden Daten streiten nachhaltig dafür, dass auch für den Auskunftsanspruch nach §§ 113a, 113b TKG-E eine entsprechende Verordnung geschaffen werden sollte, die die grundlegenden Anforderungen sowie die organisatorischen Eckpunkte für die Umsetzung dieses Auskunftsanspruchs in einer verbindlichen und eindeutigen Weise regelt.

15. Zu § 3 TKÜV-E

Bedenken bestehen gegen die Regelung in § 3 Abs. 2 Satz 1 Nr. 5 TKÜV-E, durch den der Kreis der Verpflichteten von derzeit 1000 Teilnehmern auf künftig 10.000 Teilnehmer angehoben werden soll. So wird zum einen auch in der Begründung nicht dargelegt, dass die bisher verpflichteten Netzbetreiber mit mehr als 1000, jedoch weniger als 10.000 Teilnehmern übermäßig belastet würden. Zu bedenken ist weiter, dass insbesondere im Zusammenhang mit der Internet-Telefonie verstärkt Netzbetreiber festzustellen sind, die im Falle der beabsichtigten Erhöhung auf 10.000 Teilnehmer nicht mehr verpflichtet wären, Vorkehrungen für eine mögliche Telekommunikationsüberwachung zu treffen.

Auch im übrigen Bereich der paketbasierten Übertragungstechnologien sind verstärkt kleinere Dienstanbieter festzustellen, die im Falle einer Einengung des Kreises der Verpflichteten nach § 3 TKÜV dem Kreis der Verpflichteten ebenfalls nicht mehr unterfallen würden.
Derartige Dienstanbieter könnten künftig von den Beschuldigten gezielt genutzt werden, um einer Überwachung gänzlich zu entgehen.

Ralf Günther