Berlin, im August 2007
Stellungnahme Nr. 41/2007
www.anwaltverein.de

Stellungnahme des Deutschen Anwaltvereins

durch den Strafrechtsausschuss

zum

Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG

Mitglieder des Ausschusses:

Rechtsanwalt Dr. Stefan König, Berlin (Vorsitz und Berichterstatter)
Rechtsanwalt Dr. h.c. Rüdiger Deckers, Düsseldorf
Rechtsanwältin Dr. Gina Greeve, Frankfurt a.M.
Rechtsanwalt Prof. Dr. Rainer Hamm, Frankfurt a.M. (Berichterstatter)
Rechtsanwältin Gabriele Jansen, Köln
Rechtsanwalt Eberhard Kempf, Frankfurt a.M.
Rechtsanwältin Gül Pinar, Hamburg
Rechtsanwalt Michael Rosenthal, Karlsruhe
Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Berichterstatterin)
Rechtsanwalt Dr. Rainer Spatscheck, München (Berichterstatter)

Zuständige DAV-Geschäftsführerin:

Rechtsanwältin Bettina Bachmann, DAV-Berlin

Verteiler:

- Bundesministerium des Innern
- Bundesministerium der Justiz
- Rechtsausschuss, Innenausschuss des Deutschen Bundestages
- Vorsitzender des Rechtsausschusses des Deutschen Bundestages, Andreas Schmidt
- Vorsitzender des Innenausschusses des Deutschen Bundestages, Sebastian Edathy
- Landesjustizverwaltungen
- Bundesgerichtshof
- Bundesanwaltschaft

- Vorstand des Deutschen Anwaltvereins
- Landesverbände des Deutschen Anwaltvereins
- Vorsitzende der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Strafrechtsausschuss des Deutschen Anwaltvereins
- Geschäftsführender Ausschuss der Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins
- Strafrechtsausschuss der Bundesrechtsanwaltskammer
- Vorsitzende des Strafrechtsausschusses des KAV, BAV
- Vorsitzender des Forums Junge Anwaltschaft des DAV

- Deutscher Strafverteidiger e.V., Frau Regina Michalke
- Regionale Strafverteidigervereinigungen
- Organisationsbüro der Strafverteidigervereinigungen und -initiativen

- Arbeitskreise Recht der im Bundestag vertretenen Parteien
- Deutscher Richterbund

- Strafverteidiger-Forum (StraFo)
- Neue Zeitschrift für Strafrecht, NStZ
- Strafverteidiger

- Prof. Dr. Jürgen Wolter, Universität Mannheim
- ÖTV, Abteilung Richterinnen und Richter
- Deutscher Juristentag (Präsident und Generalsekretär)
- Prof. Dr. Schöch, LMU München

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit 64.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

I. Einleitung:

Die Bundesregierung hat mit dem Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (Bundestags-Drucksache 16/5846) das Resultat beachtlicher Anstrengungen vorgelegt, die heimlichen strafprozessualen Ermittlungsmaßnahmen, besonders im Bereich der Telekommunikationsüberwachung, in ein kohärentes, schlüssiges System zu bringen[1].

Die folgende Stellungnahme zu diesem Entwurf widmet sich einzelnen ausgesuchten Aspekten, bei denen uns Anmerkungen aus der Sicht von Strafverteidigerinnen und Strafverteidigern angezeigt scheinen.

Im Wesentlichen geht es um:

- die vom Entwurf vorgeschlagene Regelung des besonderen Schutzes der Kommunikation von **Berufsgeheimnisträgern**. Die hier vorgenommene Differenzierung zwischen verschiedenen Berufsgruppen erscheint dem Ausschuss nicht angemessen. Auch sind die Voraussetzungen, wann Ermittlungsbehörden in diese Sphäre ausnahmsweise eindringen dürfen, nicht eng genug gefasst.

- Die Stellungnahme widmet sich ausführlich dem Vorschlag der GRÜNEN, **anstelle eines Kataloges** von Anlasstaten bei der Telekommunikationsüberwachung (in § 100a Abs.2 StPO i.d.F. des Entwurfs) eine **generalklauselartige Bestimmung** einzuführen, mit der der Kreis der Delikte, zu deren Aufklärung Telekommunikation überwacht werden darf, beschränkt werden soll. Der Strafrechtsausschuss des DAV hat dieses Modell nach ausführlichen Diskussionen **verworfen**, weil er der Auffassung ist, dass damit das Gegenteil des Beabsichtigten erreicht würde. Er ist freilich auch der Auffassung, dass die vorgesehene Ausweitung des Kataloges nicht akzeptabel ist.

- Wir unterstützen das Anliegen des Entwurfs, den **Ermittlungsrichter** bei dem Amtsgericht am Sitz der Staatsanwaltschaft anzusiedeln. Freilich halten wir

[1] Von einem „harmonischen Gesamtsystem“ möchten wir, anders als der Entwurf (vgl. S. 1), allerdings nicht sprechen.

weitergehende Regelungen angesichts der ernüchternden Befunde wissenschaftlicher Untersuchungen zur Praxis ermittlungsrichterlicher Tätigkeit für dringend erforderlich und unterbreiten hierzu konkrete Vorschläge.

- Die vorgesehenen **Berichtspflichten** über Verlauf, Ergebnisse und Umfang von Telekommunikationsüberwachungsmaßnahmen **begrüßen wir** nachhaltig, sehen allerdings auch hier Ergänzungsbedarf.

- Eingehend befasst sich die Stellungnahme mit den im Entwurf vorgesehenen Regeln zur **Durchsicht von Datenträgern** (§ 110 Abs. 3 StPO in der Fassung des Entwurfs). Wir sind der Auffassung, dass das Bemühen, hierdurch dem technischen Fortschritt entsprechende Zugriffsmöglichkeiten auf dislozierte Datenträger zu erhalten, weit über das Notwendige und selbst über das Erträgliche hinausschießt. Die Regelung **schafft** letztlich die **Eingriffsvoraussetzungen für ein – unzulässiges – staatliches „Hacking“**, gegen das der Deutsche Anwaltverein sich grundsätzlich und mit Nachdruck ausspricht.

- Die vorgeschlagenen Vorschriften zur Umsetzung der EU-Richtlinie 2006/24/EG zur so genannten **Vorratsdatenspeicherung lehnen wir ab**. Wir halten die Richtlinie bereits selbst für europarechtswidrig und gehen davon aus, dass der Europäische Gerichtshof dies in dem dort zur Zeit anhängigen Verfahren feststellen wird. Überdies verstößt sie gegen deutsches Verfassungsrecht, wie es für die einschlägigen Problemfelder in der Rechtsprechung des Bundesverfassungsgerichts in mehreren einschlägigen Entscheidungen konturiert wurde.

Insgesamt sind wir der Auffassung, dass der vorliegende Entwurf eine Vielzahl diskussionswürdiger Ansätze enthält, die es verdienen, in einer breiten (nicht nur Fach-) öffentlichen Debatte erwogen und gewürdigt zu werden. Um so mehr bedauern wir es, dass der Entwurf in der gelegentlich von populistischem „Sicherheits“-Wahn überlagerten Debatte der letzten Monate nicht die ihm gebührende Beachtung gefunden hat.

II. Zu den einzelnen Regelungen:

A.

Zur Einführung eines § 53b StPO:

Wir **begrüßen es**, dass die Regelung von Beweiserhebungsverboten bezüglich Ermittlungsmaßnahmen, die sich auf Berufsgeheimnisträger richten, einheitlich, ***„vor die Klammer gezogen“***, erfolgt.

Auch dass der Entwurf im Anschluss an die Vorschläge des Arbeitskreises Strafprozessrecht und Polizeirecht [2] der besonderen Brisanz von Eingriffen der Strafverfolgungsbehörden in das Mandatsverhältnis der Strafverteidiger gerecht werden will, entspricht einer alten Forderung des DAV.

Die Rolle des **Strafverteidigers** in einem rechtsstaatlichen Strafverfahren **verbietet es** ohne wenn und aber**, Informationen, auf die sich sein Zeugnisverweigerungsrecht aus § 53 Abs. 1 Nr. 2 StPO bezieht, zum Objekt von Ermittlungsmaßnahmen zu machen**. Der Beistand dessen, gegen den sich der Verdacht richtet, darf in dieser Funktion unter keinen Umständen ausgerechnet von denen ausgeforscht werden, die gegen den Mandanten ermitteln. Derartiges wäre nicht nur mit dem notwendigen Schutz der Vertraulichkeit der Kommunikation, sondern auch mit der Subjektstellung des Beschuldigten nicht vereinbar, was für den inhaftierten Beschuldigten auch durch § 148 StPO ausdrücklich anerkannt ist. Schon daraus ergibt sich die zwingende Notwendigkeit der in § 53b Abs.1 StPO-E vorgesehenen Regelung für Strafverteidiger.

Bei den übrigen Berufsgeheimnisträgern besteht diese aus der besonderen Konstellation des Strafverfahrens resultierende Situation des Strafverteidigermandats zwar nicht; gleichwohl sprechen **zwingende Gründe** – die bei dem Strafverteidiger zu den genannten hinzutreten – **dagegen, durch eine Differenzierung zwischen den einzelnen Gruppen von Zeugnisverweigerungsberechtigten** aus § 53 Abs.1 StPO, wie der Entwurf sie in § 53b Abs.2 StPO-E vorsieht, eine **Abstufung im Schutzniveau** zwischen den sie betreffenden Vertrauensverhältnissen **vorzunehmen**.

---

[2] Vgl. dazu die von *Wolter* und *Schenke* zusammengestellte Textsammlung „Zeugnisverweigerungsrechte bei (verdeckten) Ermittlungsmaßnahmen“ (2002) in der die vom Arbeitskreis Strafprozessrecht und Polizeirecht (ASP) bei dem Mannheimer Institut für deutsches und europäisches Strafprozessrecht und Polizeirecht erarbeiteten Ergebnisse zu dem vom Bundesministerium der Justiz in Auftrag gegebenen Forschungsprojekt „Informationserhebung und Verwertung durch Vernehmung, Auskunft und heimliche Ermittlungsmaßnahmen“ zusammengestellt sind (vgl. dazu auch die Begründung des Entwurfs, BT-Drs. 16/ 5846, S.56).

Der Gesetzgeber hat durch die Regelung des § 53 Abs.1 zu erkennen gegeben, dass die Beziehung zwischen dem Rat oder Hilfe suchenden Bürger und den Angehörigen der in der Vorschrift aufgezählten Berufe einer besonderen Vertraulichkeit bedarf. Die Leistungen der in § 53 Abs.1 StPO genannten Berufe berühren – und zwar häufiger und stärker als die anderer Berufsgruppen – Bereiche, in denen schutzwürdige Geheimhaltungsinteressen des Einzelnen Beachtung verlangen. Sie sind daher in besonderem Maße davon abhängig, dass demjenigen, der sie in Anspruch nimmt, die Möglichkeit garantiert ist, sich seinem Gegenüber frei, offen und rückhaltlos anzuvertrauen, ohne befürchten zu müssen, dass Tatsachen oder Umstände, die der andere kraft seines Berufes erfährt, offenbart oder sonst ohne die Zustimmung des Betroffenen bekannt werden, insbesondere an die Ohren von Ermittlungsbehörden dringen oder ihnen in die Hände fallen (vgl. BVerfGE 38, 312, 323). Eine Differenzierung zwischen den Zeugnisverweigerungsrechten der einzelnen Berufsgruppen nimmt der Gesetzgeber in § 53 Abs.1 StPO nicht vor. Es geht bei § 53 StPO so wenig wie in § 53b StPO-E um Privilegien für herausgehobene Berufsgruppen. Es geht um die Persönlichkeitsrechte von Bürgern, deren Vertrauen darauf, sich bestimmten Menschen rückhaltlos und unzensiert anvertrauen zu können, geschützt werden muss. Die Gesellschaft und der demokratisch verfasste Rechtsstaat sind auf solche Freiräume angewiesen.

Die Preisgabe von Informationen, auf die sich ein Zeugnisverweigerungsrecht bezieht, ist in den meisten Fällen strafbewehrt (§ 203 Abs. 1 StGB). Zu den tauglichen Tätern nach § 203 StGB gehören allerdings Abgeordnete und Geistliche, die der Entwurf in § 53b Abs. 1 (zusammen mit den Strafverteidigern) vor den übrigen Berufsgeheimnisträgern privilegieren will, nicht.

Die im Entwurf vorgesehene **Differenzierung zwischen verschiedenen Berufsgruppen** führt unweigerlich zu **Wertungswidersprüchen** zwischen einzelnen Regelungen zum Vertraulichkeitsschutz, sei es in § 53 Abs.1 StPO, sei es in § 203 StGB. Sie lässt sich auch nicht aus dem unterschiedlichen Kernbereichsbezug der verschiedenen Berufsgruppen oder aus anderen Grundrechten ableiten, als deren Träger die Berufsausübenden agieren. So ist es nicht plausibel, dass die Informationen, auf die sich das Zeugnisverweigerungsrecht des Geistlichen bezieht, a priori stärkeren Kernbereichsbezug aufweisen sollten, als die seelischen Qualen, die ein Patient seinem Psychiater offenbart. Und das Zeugnisverweigerungsrecht des Journalisten, der das durch Art. 5 GG geschützte Informationsinteresse der Öffentlichkeit bedient, ist nicht weniger verfassungsrechtlich verwurzelt als das des Abgeordneten, das sich unmittelbar aus Art. 47 GG ergibt.

Die Funktion des Verteidigers im rechtsstaatlichen Strafverfahren macht einen besonderen Schutz seiner Beziehung zu derjenigen Person erforderlich, derentwegen dieses Verfahren stattfindet und zu deren Rechtsgewährleistung es geregelt ist. Aus dieser Besonderheit, die einen absoluten Schutz der mandatsinternen Kommunikation gebietet, folgt aber nicht, dass es gerechtfertigt oder gar geboten wäre, die Vertraulichkeitssphäre mit den Angehörigen anderer Berufe, die der Gesetzgeber unter den Schutz des § 53 Abs.1 StPO gestellt hat, für Ermittlungsmaßnahmen auch nur ansatzweise zu öffnen.

Zu begrüßen ist grundsätzlich, dass die das Kommunikationsverhältnis mit den Berufsgeheimnisträgern **schützenden Regelungen künftig nicht mehr bereits dann aufgehoben** sein sollen, wenn ein **bloßer Verdacht** der Beteiligung an der Tat oder der Begünstigung, Strafvereitelung oder Hehlerei besteht (§ 53 b Abs.4 S.1 StPO-E; vgl. auch § 97 Abs.2 S.3 StPO-E). Die Eingriffsschwelle „Einleitung eines Ermittlungsverfahrens“ ist aber bloß eine formale, leicht niederzureißende Barriere. Es ist daher **angemessen,** entsprechend dem geltenden § 138a Abs.1 StPO vorauszusetzen, dass der Berufsgeheimnisträger „**dringend oder in einem die Eröffnung des Hauptverfahrens rechtfertigenden Grade verdächtig** ist, dass er an der Tat, die den Gegenstand der Untersuchung bildet, beteiligt ist oder eine Handlung begangen hat, die für den Fall der Verurteilung des Beschuldigten Begünstigung, Strafvereitelung oder Hehlerei wäre“.

Unbedingt abzulehnen ist der Vorschlag des Bundesrates, auch die Geldwäsche in die Aufzählung der Verstrickungstaten aufzunehmen. Die zahlreichen Auslegungsprobleme des § 261 StGB, die – auch und gerade bei den Strafverteidigerinnen und Strafverteidigern – durch die Rechtsprechung des Bundesverfassungsgerichts (NJW 2004, 1305) keineswegs abschließend geklärt sind, lassen die Vorschrift leicht zum Einfallstor sachfremder Erwägungen zur Überwachung von Berufsgeheimnisträgern, insbesondere von Strafverteidigerinnen und Strafverteidigern werden.

B.

Zu § 100a Abs. 2 StPO-E:

1. Eine Stellungnahme zur vorgeschlagenen Neuregelung des § 100a StPO macht ein Eingehen auf den Vorschlag im Entwurf Bündnis 90/Die Grünen (Drucksache 16/3827) erforderlich, soweit darin vorgeschlagen wird, in § 100a StPO den Anlasstatenkatalog durch die Benennung allgemeiner Kriterien zu ersetzen, welche die Anlasstaten abstrakt und konkret der Schwere nach beschreiben.

Der Strafrechtsausschuss des Deutschen Anwaltvereins hat sich intensiv mit diesem Vorschlag einer grundsätzlichen Neuorientierung in der Regelungssystematik befasst und sich im Ergebnis gegen das Konzept von Bündnis 90/Die Grünen entschieden.

Zutreffend ist der Ausgangsbefund von Bündnis 90/Die Grünen, dass die bisherige Regelungstechnik (Anlasstatenkatalog) unter drei gravierenden Nachteilen leidet:

- Erstens hat die Erfahrung gelehrt, dass der Gesetzgeber tagespolitischen Bedürfnissen zur permanenten Erweiterung des Katalogs wenig Widerstand entgegensetzt, so dass der Katalog immer länger wurde.

- Zweitens wurde bisher auch wenig darauf geachtet, dass der Katalog ein in sich homogenes Konzept von Kriterien erkennen lässt, nach welchen ein Straftatbestand darin enthalten sein soll und nach welchen nicht.

- Drittens hat der äußere Aufbau des geltenden § 100a (Übergewicht des Straftatenkatalogs gegenüber den dagegen kaum wahrnehmbaren einschränkenden Voraussetzungen für die Telekommunikationsüberwachung) offenbar zu dem anwendungspsychologisch nachteiligen Effekt geführt, dass zahlreiche TÜ-Beschlüsse bereits deshalb ergehen, weil die „Aktendeckelnummerierung“ des jeweiligen Ermittlungsgegenstandes sich in dem Katalog wiederfand, ohne dass den weiteren gesetzlichen Eingrenzungsversuchen noch die gebührende Aufmerksamkeit gewidmet wurde.

Für den Systemwechsel, den Bündnis 90/Die Grünen vorschlagen, spricht auch, dass das Freiburger Max-Planck-Institut (Albrecht et al) als Folgerung aus der in beiden Entwürfen wiederholt zitierten Forschungsarbeit zur Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation und anderer verdeckter Ermittlungsmaßnahmen am Ende auch die etwas resignierte Forderung aufgestellt hat, auf den Katalog doch lieber ganz zu verzichten und ihn durch die Formulierung allgemeiner Kriterien zu ersetzen.

Schließlich scheint sich die Kritik an dem Katalogmodell im Hinblick auf die ihm innewohnende Tendenz zur permanenten Verlängerung des Katalogs auch wieder durch den Regierungsentwurf zu bestätigen, der jedenfalls in der Zahl der erwähnten Straftatbestände wiederum umfangreicher ist als im geltenden § 100a StPO.

Gleichwohl konnte sich der Strafrechtsausschuss des Deutschen Anwaltvereins nicht entschließen, den von Bündnis 90/Die Grünen vorgeschlagenen radikalen Schnitt eines völligen Verzichts auf den Katalog zu befürworten.

Bei genauerem Hinsehen besteht nämlich durchaus die Gefahr, dass die Zahl der Überwachungsmaßnahmen bei Geltung des Modells der Grünen eher größer wird als bei Geltung des Modells der Bundesregierung, weil es kaum gelingen kann (und den Verfassern des B90/Die Grünen-Entwurfs auch nicht gelungen ist), durch eine abstrakte Definition diejenigen Gruppen von Anlasstaten, die schon generell (d.h. vor der konkreten Prüfung) den rechtsstaatlichen Kriterien der Erforderlichkeit, Geeignetheit und Verhältnismäßigkeit des schweren Grundrechtseingriffs genügen, so abzugrenzen, dass allein dadurch ein gegenüber der bisherigen Praxis zurückhaltenderer Gebrauch der Maßnahme zu erwarten wäre.

Das sehen offenbar auch die Verfasser des Entwurfs von Bündnis 90/Die Grünen selbst so, denn sie räumen in ihrer Begründung ein, dass im Falle einer Beibehaltung des Katalogmodells auch nach ihren eigenen Vorstellungen letztlich ein längerer Katalog entstanden wäre (S. 11, A, I. der Begründung):

> *„Eine Überarbeitung des bisherigen Katalogs würde zur Streichung weniger und zur Einführung vieler neuer Tatbestände in den Katalog führen.“*

Zu diesem erstaunlichen Zugeständnis sind die Verfasser des Grünen-Entwurfs insbesondere deshalb gekommen, weil sie allein „an der Schwere der Tat orientierte Anordnungsvoraussetzungen“ für richtig halten und folgerichtig dies auch als Hauptmaßstab für ihr Modell der abstrakten Beschreibung nehmen. Wenn aber die Formulierung allgemeiner Kriterien an die Stelle eines (längeren) Katalogs treten soll, ist nahezu zwangsläufig damit zu rechnen, dass die Praxis hinter den abstrakten Umschreibungen im Wege der Auslegung eben jenen („eigentlich gemeinten“) langen Katalog sichtbar macht und anwendet. Die Ermittlungsrichter könnten sich dann sogar mit gewissem Recht auf die Gesetzesmaterialien berufen.

Der Strafrechtsausschuss des Deutschen Anwaltvereins spricht sich ganz entschieden dagegen aus, allein die Schwere der Taten, dessen der Betroffene oder seine Kontaktpersonen verdächtigt sind, für den ersten Prüfungsschritt für Zulässigkeit der Anordnung der Telekommunikationsüberwachung als maßgeblich anzusehen. Es gibt nämlich durchaus eine große Zahl von schweren Straftaten (insbesondere auch individuell begangene Verbrechen), bei denen weder typischerweise die Aufklärung auf eine Kommunikationsüberwachung angewiesen ist, noch typischerweise die Tatbegehung mit konspirativer Kommunikation zwischen Mittätern oder sonstigen Tatbeteiligten den Eingriff rechtfertigen. Der Gesetzgeber würde sich aber der verfassungsrechtlichen Rechtfertigung und Kontrolle weitgehend entziehen, wenn er auf einen Katalog vertypter Ermittlungsgegenstände verzichten wollte, die daraufhin überprüft werden könnten, ob sie neben der Deliktsschwere auch sonstige spezifische Merkmale schon einzelfallunabhängig aufweisen, welche einen Einsatz der sensiblen Ermittlungsmethode als ultima ratio gewährleisten.

Mit der Ersetzung des Katalogs durch den § 100a Abs. 2 in der Fassung des Entwurfs B90/Die Grünen

> *„(2) Straftaten im Sinne des Abs. 1 sind*
>
> *1. Verbrechen und vorsätzliche Vergehen, die mit Freiheitsstrafe von mindestens einem Jahr bedroht sind, wenn nicht bereits auf Grund der äußeren Umstände des Einzelfalls damit zu rechnen ist, dass wegen der Tat eine Strafe von weniger als einem Jahr Freiheitsstrafe verhängt wird, und*
>
> *2. vorsätzliche Vergehen, die im Höchstmaß mit Freiheitsstrafe von mindestens fünf Jahren bedroht sind und bei denen auf Grund der äußeren Umstände der Tat eine Freiheitsstrafe von mindestens einem Jahr zu erwarten ist.“*

wären alle Verdächtigen der so bezeichneten Straftaten und ihre Kontaktpersonen prinzipiell von Überwachungsmaßnahmen bedroht – unabhängig davon, ob dem vorgeworfenen Deliktstyp eine kommunikative, konspirative oder sonst interaktive Begehungsform eigen ist. Offenbar ist dies auch gewollt und soll nur durch die Pflicht zur konkreten Strafmaßprognose ein gewisses Korrektiv erfahren. Aber auch diese Einschränkung soll sich wiederum nur nach dem Parameter „Schwere der Tat“ richten.

2. Demgegenüber ist dem **Versuch des Regierungsentwurfs, den Katalog der Anlasstaten von vorne herein auf solche (auch schwere) Straftaten zu beschränken, bei denen typischerweise die Tataufklärung durch Ausnutzung der Informationen aus den kommunikativen Interaktionen von Verdächtigen Ermittlungserfolge versprechen, der Vorzug zu geben**, auch wenn – was noch zu zeigen sein wird – dieses Prinzip in der vorliegenden Entwurfsfassung nicht konsequent durchgehalten ist. Während die undifferenzierte Aufnahme aller Verbrechen in dem B90/Die Grünen-Entwurf dazu führt, dass auch z.B. alle jene (Verbrechens-)Tatbestände, bei denen es typischerweise nur einen Täter und ein oder überhaupt kein individualisierbares Opfer gibt, erfasst wären, bemühen sich die Verfasser des Regierungsentwurfs darum, solche Delikte auf die Begehensweisen zu beschränken, bei denen typischerweise mehrere Tatbeteiligte vorhanden sind. Das gilt zwar nicht für Mord und Totschlag, die ohne Einschränkung auch bereits im geltenden Recht zu den Katalogtaten gehören, wo man – ähnlich wie bei § 112 Abs. 3 StPO - als Zugeständnis an die Erwartungen des allgemeinen Publikums auf weitere Voraussetzungen für den Grundrechtseingriff verzichten möchte.

Aber bei den Sexualdelikten bemüht sich der Regierungsentwurf im Ansatz darum, die Straftaten gegen die sexuelle Selbstbestimmung auch weiterhin erst unter den Voraussetzungen des § 177 Abs. 2 Nr. 2 und des § 179 Abs. 5 Nr. 2 StGB, also bei gemeinschaftlicher Begehung als Anlasstaten zur Legitimation der Telekommunikationsüberwachung zu belassen.

Andererseits sollen nach dem Regierungsentwurf auch „die minderschweren Fälle des schweren sexuellen Missbrauchs von Kindern nach § 176a Abs. 4 StGB einbezogen werden“, obwohl hier, soweit die Tatmodalitäten des Abs. 1 betroffen sind, für die Wiederholungstat nur ein Strafrahmen von 3 Monaten bis 5 Jahren angedroht wird und bei gleicher Begehungsform im Falle der erstmaligen Tat (§ 176 Abs. 1 StGB) die Telekommunikationsüberwachung nicht vorgesehen werden soll.

Dies wäre dann nachvollziehbar, wenn es gesicherten kriminalistischen Erfahrung entspräche, dass paedophile (Wiederholungs-)Täter, auch soweit sie sich weniger gravierender Praktiken schuldig machen, typischerweise ihre Taten mit Hilfe der Telekommunikation entweder vorbereiten oder begleiten. Derartige Erkenntnisse sind aber nicht ersichtlich und sie wären angesichts der Statistiken über die meist familiären Beziehungen zwischen Tätern und den kindlichen Opfern auch überraschend.

Soweit der Entwurf darauf verweist, eine Ausklammerung dieser Taten erschiene „angesichts der erheblichen Schwere dieser Delikte und der damit verbundenen weit reichenden negativen Folgen für das Opfer nicht zu rechtfertigen“ (S. 91 der Begründung RegE), setzt sich darin die vielfach zu Recht beklagte „Irrationalität der Stimmung“ und „gewisse Hysterisierung“ (Tröndle/Fischer, 54. Auflage § 176 Rnr. 2a) fort, die auch bereits zur Änderung des Sexualstrafrechts im Gesetz vom 27.12.2003 geführt hat.

Bei **Überprüfung** der nach dem Regierungsentwurf **neu einzuführenden Anlasstaten** fällt im Übrigen auch auf, dass es immer noch an einer **konsistenten Durchmusterung aller zu diskutierenden Anlasstaten nach den Kriterien fehlt**, wonach die Telekommunikationsüberwachung generell bezogen auf den jeweiligen Deliktstypus (kumulativ)

- erforderlich,
- geeignet und
- verhältnismäßig

zu sein hat, bevor der Gesetzgeber den schweren Grundrechtseingriff erlaubt.

Hinsichtlich aller drei Kriterien bestehen **auch** bei dem Tatbestand der **Abgeordnetenbestechung (§ 100e StGB) erhebliche Zweifel.** Weil zu erwarten ist, dass sich der einfache Tatverdacht gegen einen Volksvertreter und seine „Klientel“ im Zusammenhang mit völlig legitimen und legalen Formen des Lobbyismus allzu leicht formulieren und zur Grundlage für Ermittlungen (und aus der Sicht der Anzeigeerstatter bis hin zu politische Ausforschungen) nehmen lässt, spricht sich der Strafrechtsausschuss des DAV auch mit Blick auf das Berufsgeheimnis der Abgeordneten gegen diesen Vorschlag aus. Er steht auch im Widerspruch zu den Ausführungen des Regierungsentwurfs bei der Begründung der Einbeziehung des Berufsgeheimnisses der Parlamentarier in den absoluten Schutz (§ 53 Abs. 1 Satz 1 Nr. 1, 2 und 4 StPO):

> „Einbezogen in dieses absolute Erhebungs- und Verwertungsverbot werden auch die Parlamentsabgeordneten. Deren Zeugnisverweigerungsrecht weist zwar nach den Darlegungen des Bundesverfassungsgerichts keinen unmittelbaren Bezug zu dem aus der Menschenwürde resultierenden Kernbereich privater Lebensgestaltung auf. Die Kommunikation mit Abgeordneten unter einen besonderen, Erhebungen ohne Billigung des Abgeordneten ausschließenden Schutz zu stellen, rechtfertigt sich indessen aus Artikel 47 GG, der für diese Berufsgruppe ein Zeugnisverweigerungsrecht und ein dieses flankierendes Beschlagnahmeverbot ausdrücklich vorgibt.

> Sind aber bereits diese offenen Ermittlungsmaßnahmen gegenüber Abgeordneten von deren Einverständnis (Nichtausübung des Zeugnisverweigerungsrechts) abhängig, so spricht der damit vom Grundgesetzgeber intendierte weitreichende Schutz der Abgeordneten dafür, auch andere, insbesondere verdeckte Ermittlungsmaßnahmen zu untersagen, soweit das Zeugnisverweigerungsrecht der Abgeordneten reicht.“ (RegE S. 50)

Wenn aber – was sicherlich zutrifft – die Verfassung bereits unabhängig vom Grundrecht auf freie und ungestörte Kommunikation aller Bürgerinnen und Bürger dem Parlamentarier institutionell einen so weitreichenden Schutz vor verdeckten Ermittlungsmaßnahmen garantiert, muss erst recht die Strafjustiz daran gehindert werden, bereits den einfachen Verdacht einer die Grenze zur „Käuflichkeit“ überschreitenden Wählergruppenbindung zum Anlass für TÜ zu nehmen.

Schließlich wendet sich der Strafrechtsausschuss des DAV auch **gegen die Aufnahme der Geldwäsche** (§ 261 StGB) sowie der **Wettbewerbsverzerrungen in der Privatwirtschaft nach den §§ 298, 299, 300a StGB** in den Katalog des § 100a StPO. Auch hier reichen die Strafrahmen jeweils nur von 3 Monaten bis 5 Jahre, und auch insoweit ist nicht zu erkennen, aus welchen Gründen hier für den schweren Grundrechtseingriff die Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit generell bejaht werden könnte.

Gegen die Aufnahme der **Geldwäsche** in den Katalog spricht, dass es sich um eine vom strafrechtlichen Rechtsgütergedanken abgekoppelte Vor- bzw. Nachfeldkriminalisierung ohne eigenständigen Schutzzweck handelt, dessen kriminalpolische Zielsetzung sich inzwischen als verfehlt herausgestellt hat (dazu im Einzelnen und überzeugend Tröndle/Fischer, StGB 54. Aufl., § 261 Rnr. 4b-d). Zudem hat die Zweistufigkeit im Kataloge des § 100a StPO und des § 261 Abs. 1 StGB zur Folge, dass im Frühstadium von Ermittlungen, allzu leicht der Verdacht der Geldwäsche allein zu dem Zwecke der TÜ-Legitimation begründet werden könnte, ohne dass zum Zeitpunkt der Entscheidung über die Maßnahme eine den schweren Grundrechtseingriff wirklich rechtfertigende Bewertung von zweifelhaften Geldquellen möglich wäre.

Soweit es in der Entwurfsbegründung heißt, die Delikte der **„Privatkorruption“** seien

> *„jeweils dadurch gekennzeichnet, dass sie typischerweise heimlich zwischen den Tatbeteiligten begangen werden und nach außen nicht in Erscheinung treten, so dass regelmäßig auch keine Zeugen vorhanden sind, die das Tatgeschehen beobachten und zur Anzeige bringen können“* und der Einsatz verdeckter Ermittlungsmaßnamen auch in Form der Telekommunikationsüberwachung *„aus der Praxis seit langem gefordert“* werde (RegE S. 89),

verkennt diese Praxis insbesondere die Gefahr, dass gerade auf diesem Kriminalitätsfeld vielfach Strafanzeigen aus dem Wettbewerbsumfeld auch anonym erstattet und von den Staatsanwaltschaften als ausreichend für die Annahme eines einfachen Tatverdachts genommen werden. Die Neigung von unterlegenen Konkurrenten, den Auftragsgewinner ins Blaue hinein anonym anzuzeigen, dürfte erheblich wachsen, wenn damit die Hoffnung verbunden werden könnte, durch heimliche Telekommunikationsüberwachung bloße Vermutungen bestätigt zu bekommen.

Zusammenfassend spricht sich also der Strafrechtsausschuss des DAV dafür aus, die **Gesetzestechnik der katalogmäßigen Auflistung von Anlasstattypen für die TÜ beizubehalten**, den **Katalog** des § 100a Abs. 2 StPO-E aber nach den Kriterien der Erforderlichkeit, Geeignetheit und Verhältnismäßigkeit noch erheblich „**auszudünnen“**.

Das bisherige Gesetzgebungsverfahren gibt allerdings Anlass zu der Besorgnis, dass der Katalog Begehrlichkeiten von verschiedenen Seiten weckt, die nun bedient werden wollen (vgl. die Erweiterungsvorschläge des Bundesrates in Nr.2 und 3 seiner Stellungnahme zum Gesetzentwurf der Bundesregierung um Delikte aus dem Grundstoffüberwachungsgesetz und dem Vereinsgesetz, BT-Drs. 16/5846, S. 199 f.).

C.

Zur Anordnungskompetenz nach den Vorstellungen des Entwurfs:

1. Zuständigkeit des Ermittlungsrichters

Der **Ermittlungsrichter** bleibt auch nach den Vorstellungen des Entwurfs das **Nadelöhr**, durch das die Ermittlungsbehörden von ihnen beabsichtige Eingriffe in Freiheitsrechte der Bürgerinnen und Bürger fädeln müssen. In der Vergangenheit sind allerdings wiederholt Zweifel daran laut geworden, ob er dieser Aufgabe des „Freiheitsrichters" in der Praxis gerecht wird. Die Untersuchungen des MPI zur Praxis der Telekommunikationsüberwachung[3] sowie von *Backes/Gusy*[4] haben gezeigt, dass dieses Nadelöhr in der Praxis nicht selten zum **Scheunentor** wird, weil die von der Staatsanwaltschaft vorgelegten Anträge nur oberflächlich geprüft, eins zu eins übernommen und/oder mit formelhaften Begründungen in Anordnungen umgesetzt werden.

Der Entwurf will an der Zuständigkeit des Ermittlungsrichters im Bereich der betroffenen Vorschriften grundsätzlich nichts ändern (Ausnahme: § 163 f StPO-E). Es ergibt sich folgendes Bild:

Maßnahme	**Anordnung durch**
Überwachung und Aufzeichnung von Telekommunikation nach § 100 a StPO	Ermittlungsrichter (§ 100 b StPO
Akustische Wohnraumüberwachung nach § 100 c StPO	Landgericht (§ 100 d StPO i.V.m. § 74 a Abs. 4 GVG)
Akustische Überwachung außerhalb von Wohnungen nach § 100 f StPO	Ermittlungsrichter (§§ 100 b, 100 f Abs. 4 StPO)
Erhebung von Verkehrsdaten nach § 100 g StPO	Ermittlungsrichter (§§ 100 b, 100 g Abs. 2 StPO)
Observation nach § 100 h StPO	**Neu:** Bei längerfristiger Observation: Ermittlungsrichter nach § 163 f StPO
Imsi-Catcher nach § 100 i StPO	Ermittlungsrichter nach §§ 100 b, 100 i Abs. 5 StPO

[3] *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg i.Brsg. 2003

[4] *Backes/Gusy*, Wirksamkeitsbedingungen von Richtervorbehalten bei Telefonüberwachungen, Bielefeld 2002

Abgesehen davon, dass er gesetzesterminologisch künftig nicht mehr „Richter“ und seine Handlungen nicht mehr „richterlich“ genannt werden sollen, sondern zur „Gewährleistung einer geschlechtsneutralen Gesetzessprache“[5] nur noch vom „Gericht“ die Rede ist, das „gerichtlich“ agiert, schlägt der Entwurf lediglich eine kompetenzrechtliche Änderung vor:

2. Anforderungen an den Ermittlungsrichter

Nach § 162 StPO-E S.1 soll das Amtsgericht zuständig sein, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat, die die gerichtliche Untersuchungshandlung beantragt[6].

Dieser Vorschlag verdient Unterstützung.

Er hilft zu gewährleisten, dass Richterinnen und Richter das Amt bekleiden, die über die notwendigen Erfahrungen bei der Entscheidung über Anträge verfügen, die auf Eingriffe in bürgerliche Freiheitsrechte abzielen. Auch die pragmatischen Vorteile der Regelung – Erleichterung der notwendigen Bereitstellung eines richterlichen Bereitschaftsdienstes[7] - sprechen für sie und helfen, die Bedenken aufzuwiegen, die aus der größeren Nähe zwischen antragstellenden Staatsanwälten und entscheidenden Ermittlungsrichtern resultieren, die nicht allein räumlich, sondern dadurch auch persönlich entsteht.

Der Vorschlag reicht aber nicht aus.

a.
An die berufliche Qualifikation des Ermittlungsrichters sind besondere Anforderungen zu stellen. Der Vorschlag der Bundestagsfraktion von Bündnis 90/Die Grünen in deren „Entwurf eines Gesetzes zur Reform der Telekommunikationsüberwachung (… Gesetzes zur Änderung der Strafprozessordnung)“ ist vorzugswürdig:

Danach sollen Telekommunikationsüberwachungsmaßnahmen allein durch einen nach § 10 des Deutschen Richtergesetzes auf Lebenszeit ernannten Richter[8] angeordnet werden dürfen. Das bedeutet, dass in dieses Amts nur Personen berufen werden dürfen, die über einige richterliche Berufserfahrung verfügen.

---

5 In Ansehung von § 1Abs.2 BGleiG.

6 die Ausnahme hiervon in § 162 S.2 StPO-E kann hier vernachlässigt werden.

7 Vgl. S. 139 der Entwurfsbegründung unter Verweis auf BVerfGE 100, 313, 401; 103, 142, 152; 105, 239, 248; 109, 279, 358; BVerfGE 2, 176, 179

8 Zum Richter auf Lebenszeit kann nach § 10 Abs.1 DRiG (mit in § 10 Abs.2 aufgezählten Ausnahmen) nur ernannt werden, wer nach Erwerb der Befähigung zum Richteramt mindestens drei Jahre im richterlichen Dienst tätig gewesen ist.

Wir meinen, dass die Richterpersönlichkeit, die die „gerichtlichen Untersuchungshandlungen“ nach § 162 StPO vornimmt, *stets* (also nicht nur dann, wenn es um die Anordnung von Telekommunikationsüberwachungs-Maßnahmen geht) die Voraussetzungen des § 10 DRiG erfüllen muss. Über die unter Richtervorbehalt gestellten Eingriffe in Freiheitsrechte der Bürgerinnen und Bürger darf nur von „Gerichten“ entschieden werden, die über genügend Berufserfahrung verfügen, die ihnen ein souveränes Abwägen ermöglicht.

b.

Den ernüchternden Befunden aus den Untersuchungen von *Backes/Gusy* und *Albrecht/Dorsch/Krüpe* muss auf weitere Weise Rechnung getragen werden. Sie ergaben, dass ermittlungsrichterliche Beschlüsse, mit denen TÜ angeordnet wurden, in vielen Fällen nur oberflächlich oder überhaupt nicht begründet werden[9]. An die Begründung ermittlungsrichterlicher Beschlüsse müssen daher besondere Anforderungen gestellt werden, wie es die Bundesregierung in anderem Zusammenhang, nämlich in § 81g Abs.3 S. 5 StPO in der Fassung des Referententwurfs für ein Gesetz zur Novellierung der forensischen DNA-Analyse[10], vorgeschlagen hat. Auch wenn dadurch die Erstellung von Formularen und Textbausteinen sowie die Vorformulierung von Begründungstexten durch Kriminalpolizei und/oder Staatsanwaltschaft[11] nicht ganz auszuschließen ist, zeigt doch die Entwicklung der obergerichtlichen Rechtsprechung im Haftrecht zu § 114 StPO[12], dass Begründungspflichten den besonderen Charakter und die Bedeutung des Eingriffs zur sorgfältigen Reflektion des Entscheidungsträgers stellen.[13]

---

9 Vgl. dazu *Albrecht/Dorsch/Krüpe* a.a.O. S. 446 ff. und *Backes/Gusy* u.a., Kurzfassung des Abschlussberichts, Nr. 4.1., S. 3 f

10 Danach soll § 81g Abs.3 S. 5 StPO folgenden Wortlaut erhalten:
„In der schriftlichen Begründung des Gerichts sind einzelfallbezogen darzulegen
1. die für die Beurteilung der Erheblichkeit der Straftat bestimmenden Tatsachen,
2. die Erkenntnisse, aufgrund derer Grund zu der Annahme besteht, dass gegen den Beschuldigten künftig Strafverfahren zu führen sein werden, sowie
3. die Abwägung der jeweils maßgeblichen Umstände.“

11 Zu dieser Praxis *Backes/Gusy* u.a. a.a.O. (Fn.7)

12 vgl. OLG Düsseldorf, StV 1996, 440 ff. m. Anm. *Weider*; OLG Brandenburg, StV 1997, 140; OLG Köln, StV 1999,156; dazu: L-R-*Hilger*, 25.A., § 114, Rn. 15 ff.

13 Vgl. dazu bereits These 7 in unserer Stellungnahme Nr. 35/2006 von Juni 2006 zum Gutachten der Großen Strafrechtskommission des Deutschen Richterbundes „Die Tätigkeit des Ermittlungsrichters im Ermittlungsverfahren“

Wir schlagen daher vor, hinter § 100b StPO-E in der Fassung des Referentenentwurfs einen neuen Absatz 3 einzufügen, der folgenden Wortlaut hat:

> *(3) In der schriftlichen Begründung des Gerichts sind einzelfallbezogen darzulegen*
> *1. die Tatsachen, die den Verdacht begründen, dass jemand eine in Absatz 2 bezeichnete Straftat begangen oder zu begehen versucht oder durch eine Straftat vorbereitet hat,*
> *2. die Tatsachen, aus denen sich ergibt, dass die Tat schwer wiegt,*
> *3. die Beweismittel, aus denen sich diese Tatsachen ergeben,*
> *4. warum die Erforschung des Sachverhalts oder die Ermittlung des Aufenthalts des Beschuldigten auf andere Weise als durch Überwachung und Aufzeichnung der Telekommunikation erheblich erschwert oder aussichtslos wäre.*

Absätze 3, 4 und 5 in der Fassung des Entwurfes werden dann Absätze 4, 5 und 6.

Auch mit einer solchen Regelung werden die Justizverwaltungen selbstredend nicht von der Pflicht entbunden, dafür zur sorgen, „dass die zur Gewährleistung eines effektiven Rechtsschutzes notwendigen sachlichen und personellen Ressourcen bereitgestellt sind“, was die Entwurfsbegründung[14] unter Verweis auf zahlreiche Entscheidungen des BVerfG als eine von deren „wichtigsten und vornehmsten Aufgaben“ herausstreicht. Das ist angesichts der häufig beklagenswerten Arbeitssituation von Ermittlungsrichtern noch recht euphemistisch formuliert. Sie sind häufig zeitlich überlastet und können daher die erforderlichen gründlichen Prüfungen der Anträge der Staatsanwaltschaft nicht immer gewährleisten. Eine Verbesserung der Ausstattung mit Personal- und Sachkapazitäten ist längst überfällig[15].

Mit ihr allein ist es aber nicht getan, und der Bundesgesetzgeber kann sie auch nicht leisten. Es müssen daher auch – wie von uns vorgeschlagen – konkrete Begründungspflichten kodifiziert werden.

---

14 Entwurfsbegründung S. 51

15 So auch *Albrecht/Dorsch/Krüpe* a.a.O. S. 468

3. Folgen mangelhafter Anordnungen:

Beweisverwertungsverbot

Der Entwurf sieht ein Beweisverwertungsverbot für Erkenntnisse aus Telekommunikations-Überwachungsmaßnahmen in den Fällen vor, in denen eine wegen „Gefahr in Verzug“ angeordnete TKÜ nicht binnen drei Werktagen von dem Gericht bestätigt wird. Die Maßnahme tritt dann außer Kraft. Aufgrund der Anordnung erlangte personenbezogene Daten dürfen nicht zu Beweiszwecken verwertet werden. Das unterstützen wir. Es reicht aber nicht aus.

Die bereits erwähnten Befunde der rechtstatsächlichen Untersuchungen machen es erforderlich, ein Verwertungsverbot auch für die Fälle zu fordern, in denen den Tenorierungs- und Begründungserfordernissen des § 100b Abs.2 und Abs.3 nicht genügt wird, um zu gewährleisten, dass diesen Pflichten auch tatsächlich entsprochen wird.

Wir schlagen vor, einen § 100b Abs.7 StPO-E aufzunehmen, der lautet:

> *„(7) Ist eine wegen Gefahr in Verzug durch die Staatsanwaltschaft getroffene Anordnung nicht binnen drei Werktagen von dem Gericht bestätigt worden, so tritt sie außer Kraft und die aufgrund der Anordnung erlangten personenbezogenen Daten dürfen nicht zu Beweiszwecken zu Lasten des Beschuldigten verwendet werden. Fehlen in der Entscheidungsformel der Anordnung Bestimmungen über Art, Umfang und Dauer der Maßnahme oder in ihrer Begründung einzelne nach § 100 b Abs. 3 StPO erforderliche Bestandteile, so dürfen die aufgrund der Anordnung erlangten personenbezogenen Daten nicht zu Beweiszwecken zu Lasten des Beschuldigten verwendet werden.“*

4. TKÜ-Anordung über sechs Monate hinaus

Eine **Verlängerung der TKÜ über sechs Monate hinaus** darf nur in **extrem gelagerten Ausnahmefällen** zulässig sein. Der Ausnahmecharakter einer solchen Maßnahme sollte durch eine besondere Kompetenzregelung unterstrichen werden. Dieser Überlegung trägt der **Entwurf** durch die Zuweisung der **Anordnungskompetenz** in Fällen, in denen TKÜ-Maßnahmen **über sechs Monate** hinaus erfolgen sollen, an das **im Rechtszug übergeordnete Gericht** (vorbehaltlich § 169 StPO) Rechnung.

Vorzugswürdig erscheint uns hier – parallel zur Regelung in § 122 StPO - der Vorschlag von Bündnis 90/Die Grünen, in § 10 Abs.2 a ihres „Entwurfes eines Gesetzes zur Reform der Telekommunikationsüberwachung (… Gesetzes zur Änderung der Strafprozessordnung)“, die **Entscheidungskompetenz dem Oberlandesgericht zu übertragen**. In § 100b Abs.1 S.6 muss es daher am Ende heißen:

„...so entscheidet über weitere Verlängerungen das Oberlandesgericht.“

D.
Berichtspflichten

1.
Die in § 100 a Abs. 4 StPO-E vorgeschlagene Regelung, wonach das **anordnende Gericht nach Beendigung der Maßnahme über deren Verlauf und Ergebnisse zu unterrichten ist unterstützen wir**. Bislang findet eine solche Erfolgs- bzw. Ergebniskontrolle nicht statt. Auch sie kann dazu führen, die besorgniserregend hohe Anzahl von Telekommunikationsüberwachungsmaßnahmen zu reduzieren. Die Regelung sollte allerdings noch dadurch ergänzt werden, dass das anordnende Gericht von der Staatsanwaltschaft nach Abschluss des Verfahrens darüber unterrichtet wird, ob und inwiefern die Ergebnisse der Maßnahme für die verfahrensabschließende Entscheidung von Bedeutung waren.

2.

Eine **begrüßenswerte Neuerung** sieht der Entwurf in § 100b Abs. 5 und 6 vor (und bei der Erhebung von Verkehrsdaten in § 100g Abs.5 StPO-E, der auf § 100b Abs.5 StPO-E verweist). Danach sollen die **Länder und der Generalbundesanwalt jährlich dem Bundesamt für Justiz über angeordnete Maßnahmen der Telekommunikationsüberwachung berichten**. Die **Berichte** sollen im Internet **veröffentlicht** werden. Nach § 100 a Abs. 6 des Entwurfs sollen sie Angaben über die Anzahl der Verfahren, in denen Telekommunikationsmaßnahmen angeordnet wurden, über die Anzahl der Überwachungsanordnungen, unterschieden nach Erst- und Verlängerungsanordnungen sowie Festnetz-, Mobilfunk- und Internettelekommunikation, über die jeweils zu Grunde liegende Anlassstraftat und über die Anzahl der Beteiligten der überwachten Telekommunikation enthalten.

Erwogen wird auch, in die Berichte Angaben dazu aufzunehmen, ob die Überwachung Ergebnisse erbracht hat, die für das Verfahren relevant sind oder voraussichtlich relevant sein werden und ob die Überwachung Ergebnisse erbracht hat, die für andere Strafverfahren relevant sind oder voraussichtlich relevant sein werden (§ 100b Abs.6 Nr. 5 und 6 StPO-E). Das ist sinnvoll, weil sich daran messen lässt, ob eine vernünftige Mittel-Zweck-Relation bei den Telekommunikationsüberwachungsmaßnahmen besteht. Das rechtfertigt sie für sich genommen zwar noch nicht. Erweist sich eine große Zahl der Maßnahmen aber als bedeutungslos für den Verfahrensausgang, werden sie jedenfalls zweifelhaft.

An die Berichte müssen aber differenziertere Anforderungen gestellt werden. Sie müssen nach den jeweils anordnenden Gerichten unterscheiden. Nur dadurch lässt sich feststellen, **ob bei einzelnen Gerichten in besonderem Umfang Telekommunikationsmaßnahmen angeordnet werden**, so dass Anlass besteht, die Ursachen hierfür zu erforschen und gegebenenfalls Abhilfemaßnahmen zu ergreifen

Die Berichte sollten ferner **Angaben über die Anzahl der Anträge sowie die Anzahl der ihnen stattgebenden bzw. ablehnenden Beschlüsse enthalten**. Schließlich halten wir es für erwägenswert, auch die **Kosten der Telekommunikationsüberwachungsmaßnahmen auszuweisen**, wie es z. B. in den USA geschieht.

Die Bedenken der Entwurfsverfasser, die in § 100b Abs.6 Nr. 5 und 6 StPO-E vorgeschlagene Evaluierungspflicht könne, da sie eine umfassende Kenntnis und Würdigung des Sachstandes voraussetzt, zu einem nicht unerheblichen zusätzlichen Aufwand führen, dürften im Grunde berechtigt sein. Der **Aufwand** ist aber angesichts der Bedeutung des betroffenen Grundrechts und der Besorgnis der Bevölkerung über eine scheinbar unkontrollierte Zunahme von Telekommunikations-überwachungsmaßnahmen **ohne weiteres gerechtfertigt**. Denn entweder wird die Evaluierung erbringen, dass diese Befürchtungen nicht berechtigt sind oder sie wird, wenn das Gegenteil der Fall sein sollte, zu Konsequenzen führen, die diese Entwicklung eindämmen bzw. umkehren wird.

Die Untersuchungen von *Albrecht/Dorsch/Krüpe*[16] haben gezeigt, dass solche Pflichten den Eindruck von planvoller, geheimer und umfassender Überwachung entgegenwirken können. Wenn sie aber – wie von *Albrecht* u. a. hervorgehobenen – geeignet sein sollen, „politische Verantwortlichkeit für die Art und Weise sowie den Umfang der Überwachungstätigkeit einzufordern“, dann ist die von uns vorgeschlagene weitere Ausdifferenzierung der Berichtspflicht unabdingbar.

Wir teilen im Übrigen die Skepsis des Entwurfs gegenüber der Einrichtung eines „Ombudsmannes“ bzw. – nach dänischem Vorbild – der Institutionalisierung eines kontradiktorischen Verfahrens mit einem Anwalt ohne Mandat und ohne Verbindung zum Beschuldigten, demgegenüber er zur Verschwiegenheit verpflichtet werden müsste. Eine solche Rechtsfigur ist unserem Verständnis von den Aufgaben eines Anwaltes, der auf der Grundlage einer Vertrauensbeziehung zu seinem Mandanten (bzw. zu dem Beschuldigten, dem er – in der Regel nach dessen Auswahl – beigeordnet wurde) für dessen Interessen eintritt, nicht vereinbar.

E.
„Durchsicht von Datenträgern“, § 110 Abs. 3 StPO-E

1. Technisches Problem

Der Gesetzgeber ging bei Abfassung der Vorschriften über die Durchsuchung in der StPO (§§ 102 ff.) davon aus, dass im Wesentlichen Räume und die darin vorhandenen Gegenstände das Objekt der Durchsuchung bilden. Eine konkrete Beschreibung war einfach. Mit der technischen Entwicklung von EDV-Anlagen wurden die Durchsuchungs- und Beschlagnahmevorschriften der StPO im Wege des Richterrechts auch auf „elektronische Datenträger und Datenspeicher“ (BGH, NStZ 2003, 670) sowie „Notebooks“ (BVerfG, NJW 2002, 1410) ausgedehnt.

16 a.a.O. S. 441

Nach derzeitiger Rechtssituation besteht somit kein Zweifel daran, dass EDV-Anlagen, Festplatten, CD´s, DVD´s ua., die sich in dem ordentlich konkret beschriebenen Objekt der Durchsuchung befinden, Gegenstand selbiger sind und nach § 110 StPO „durchgesehen“ werden dürfen.

Mit der **flächendeckenden Einführung schneller Internetzugänge** (DSL/UMTS/HSDPA) vollzog sich ein **Quantensprung in der Datenverarbeitung und Speicherung**. Seitdem Hochgeschwindigkeits-DSL-Anschlüsse auch für kleinere Unternehmen zu Flatrates verfügbar sind, sind mehrere Standorte häufig so verbunden, dass die Daten zentral an einem Ort gespeichert werden. Die anderen Niederlassungen verfügen bei sich nur noch über Anwendungsprogramme, während die Daten selbst für jeden Anwendungsfall vom Zentralrechner über einen verschlüsselten VPN-Tunnel angefordert und auf den Rechner des jeweiligen Benutzers übertragen werden. Dies geschieht sowohl deutschlandweit, als auch international. Die Arbeit mit nur einem Datenstamm lässt Probleme bei dem Abgleich der Datensätze verschiedener Standorte sowie Unsicherheiten bei der Datenspeicherung ausgelagerter PC´s entfallen.

Einen weiteren Schritt im Umgang mit vernetzten Computern brachte die **immer besser werdende Leitungskonstanz sowie die Leistungsfähigkeit von Servern** mit sich. So ist es heute auch für kleinere Unternehmen oder Anwaltssozietäten möglich, **zentral** einen **Terminalserver zu betreiben**. Nur auf diesem Terminalserver laufen alle Anwendungsprogramme. Er allein hat Zugriff auf den zentralen Datenspeicher. Die Anwender selbst haben auf ihren Computern und Notebooks keine eigenen Daten mehr gespeichert. Dort laufen auch keine Anwendungsprogramme. Vielmehr werden ausschließlich die Bildschirmdaten vom Terminalserver hin zum Anwender und die Tastatur- bzw. Mausbefehle vom Anwender hin zum Terminalserver übertragen. Diese Anwendungsvariante benötigt nur noch einen Bruchteil der Leitungskapazität, die bei der Übertragung vollständiger Datensätze anfällt. Es ist somit auch völlig unerheblich, ob der jeweilige Anwender im gleichen Gebäude sitzt, in dem sich der Terminalserver befindet oder nur über eine VPN-Anbindung verfügt. Wegen der geringeren Menge übertragener Daten gibt es in der Performance keinen Unterschied.

So ist es beispielsweise problemlos möglich, von unterwegs mit dem Notebook und einer UMTS-Verbindung auf dem Terminalserver zu arbeiten. Dies geht im Zusammenspiel mit Rechnern im In- und Ausland. Das Internet kennt keine Landesgrenzen.

Diese **Anwendungstechnik ist im ASP (Advanced Service Providing) perfektioniert**. Hier kaufen die Anwender keine Programme mehr, sondern bekommen von einem Anbieter die Nutzungsmöglichkeit der auf den Rechnern des Anbieters laufenden Programme lediglich gegen Entgelt eingeräumt. Die DATEV e.G. bietet beispielsweise ihr Programm phantasy für Anwälte als ASP-Lösung an. In diesem Fall laufen alle Programme (phantasy, word, outlook, etc.) auf den Rechenanlagen der DATEV e.G. in Nürnberg, wo auch die Daten gespeichert und gesichert werden. Der Benutzer selbst hat nur noch die Einwahldaten auf seinem Computer.

Ähnliche Anwendungen werden in großer Anzahl im Rahmen von Internetanwendungen realisiert. So werden beispielsweise bei Portalen wie web.de oder gmx E-Mail-Accounts angeboten, deren Bedienung ausschließlich über das Internet erfolgt. Eine Datenspeicherung auf dem Computer des Anwenders wird nicht vorgenommen.

Diese Vorgänge lassen sich **mit der klassischen Vorstellung des Gesetzgebers von einer Durchsuchung und Beschlagnahme nur schwer fassen**. **Die Rechtsprechung stößt an ihre Grenzen**.

2. Lösungsansatz

Die aktuellen gesetzlichen Vorschriften bieten selbst unter Zuhilfenahme des Richterrechts **keine eindeutige Regelung der Ermittlungsmöglichkeiten von dislokal gespeicherten Daten**. **Wegen der Schwere des Eingriffs ist eine eindeutige gesetzliche, einschränkende Regelung grundsätzlich zu begrüßen**.

Im Gesetzesvorschlag wurde darauf verzichtet, eine eigene Ermächtigungsgrundlage im Rahmen der §§ 102 ff. StPO zu schaffen, was sich angeboten hätte.

Vielmehr wurde unter dem Deckmantel der räumlich begrenzten Durchsuchung im Sinne von §§ 102 ff. StPO eine nach der Vorstellung des Gesetzesvorschlags klärende Regelung bei der technischen Beschreibung der Umsetzung einer Durchsuchung, nämlich der „Durchsicht von Papieren“ in § 110 StPO folgender Abs. 3 eingefügt:

> *„(3) Die Durchsicht elektronischer Speichermedien darf auf räumlich getrennte Speichermedien, zu denen der Betroffene zugangsberechtigt ist, erstreckt werden. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gespeichert werden, wenn bis zur Sicherstellung der Datenträger ihr Verlust zu besorgen ist; sie sind zu löschen, sobald sie für die Strafverfolgung nicht mehr erforderlich sind.“*

Folglich gelten **nach dem Entwurf für den Zugriff auf dislokale Speichermedien die gleichen Voraussetzungen, wie für „normale“ räumlich und gegenständlich eng beschränkte Durchsuchungsmaßnahmen**. Eine Annäherung an die Ermächtigungsgrundlage für die Durchführung von Telefonüberwachungen erfolgte nicht.

3. Stellungnahme

§ 110 Abs. 3 StPO-E geht weit über die EU-Vorgaben hinaus, ist hinsichtlich der Eingriffsvoraussetzungen zu unbestimmt, führt zu völkerrechtlich bedenklichen Verletzungen von Hoheitsrechten der Staaten, die keine Ratifizierung der Cybercrime-Convention vorgenommen haben, differenziert nicht, was bedauerlich ist, zwischen dem Umgang mit E-Mails und Daten im Rahmen des Ermittlungsverfahrens, bedeutet letztlich für den „Dritten“, bei dem die Daten erhoben werden, ein unzulässiges staatliches „Hacking“ und ist somit abzulehnen.

Ferner **überrascht** schon die **systematische Stellung** der Norm bei den Regeln zur **„Durchsicht von Papieren“**. Misst man den Entwurf an der aktuellen Praxis im Umgang mit der Beschlagnahme schon von „normalen“ Daten, so **kommt eine „Durchsicht“ quasi nie vor**. Nach derzeitiger Rechtslage erfolgt die Durchsuchung und Beschlagnahme von Computerdaten durch die Beschlagnahme der Datenträger. Seltenst erfolgt eine Vorsichtung vor Ort. Dies ist allein schon vor dem Hintergrund des häufig vorgefundenen Umfangs der Daten ausgeschlossen. Vielmehr werden die Datenträger aus Angst, Daten könnten gelöscht oder verändert werden, **von den Ermittlungsbehörden beim ersten Zugriff umfassend beschlagnahmt oder kopiert**. Da durch die permanente Datenübermittlung bei dislokalem Zugriff eine deutliche Nähe zur Telekommunikation besteht, hätte es nähergelegen, die Vorschrift systematisch dort unterzubringen.

Im Einzelnen:

a. Art. 19 Abs. 2 des Übereinkommens über Computerkriminalität (**Cybercrime-Convention**)

Folgt man der Begründung des Entwurfs, geht die Initiative zur Schaffung der Norm auf Art. 19 Abs. 2 der Cybercrime-Convention des Europarats zurück. Dieser hat folgenden Wortlaut:

> *„Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon nach Abs. 1 a durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon im Hoheitsgebiet der betreffenden Vertragspartei gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugängig oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können."*

In einigen Punkten geht **§ 110 Abs. 3 StPO-E über die EU-Vorlagen weit hinaus**. Dort ist der Zugriff auf dislokal gespeicherte Daten nur im Hinblick auf die „gesuchten Daten" zu gewähren. Eingriffsvoraussetzung nach der Cybercrime-Convention ist also, dass bestimmte Daten bereits als die Daten, die im Rahmen der Ermittlungsmaßnahme gesucht werden, identifiziert wurden. Im deutschen Entwurf hingegen ist eine unbestimmte, allgemeine Durchsicht der Daten möglich, selbst wenn noch nicht feststehen sollte, dass sich gesuchte Daten auf dem nicht ortsanwesenden Datenträger befinden. Eine „Durchsicht ins Blaue hinein" wird folglich von § 110 Abs. 3 StPO-E unberechtigterweise ermöglicht. Ferner spricht die Cybercrime-Convention nur davon, dass die „Vertragspartei", also die an der Cybercrime-Convention beteiligten Staaten, diese Voraussetzung schaffen sollen und im Gegenseitigkeitsverhältnis durchgeführte Ermittlungsmaßnahmen bei den eigenen Landesbürgern dulden müssen. Eine solche Einschränkung auf die Vertragsparteien kennt der StPO-Entwurf ebenfalls nicht. Der Entwurf des Abs. 3 bezieht vielmehr auch Drittstaaten, die nicht der Cybercrime-Convention verpflichtet sind, mit in den Regelungsbereich ein (zu den Konsequenzen, siehe unten Punkt 4.). Bis heute wurde die Cybercrime-Convention des Europarats nur von 19 Staaten ratifiziert. Bislang noch nicht beigetreten sind wichtige Länder, wie z.B. die Schweiz, Großbritannien oder Kanada.

Der Entwurf lässt sich folglich nicht auf das Argument einer notwendigen Umsetzung der Cybercrime-Convention stützen.

b. Eingriffsintensität

Der Gesetzesentwurf wird **zu Unrecht** auf die Begründung gestützt, die **„Durchsicht" von körperlich nicht unmittelbar vorhandenen Datenträgern über VPN oder andere Zugriffsmöglichkeiten sei weniger eingriffsintensiv als deren Beschlagnahme**. Hierbei handelt es sich um ein **Scheinargument**.

Gerade nach dem Verhältnismäßigkeitsgrundsatz ist eine **offene, „ehrliche" Beschlagnahme für alle Betroffenen insofern ein geringerer Eingriff, als gerade durch die Kenntnis eine Anfechtung mit Rechtsmitteln möglich ist.** Ferner wird es nach der Struktur der vorgeschlagenen Eingriffsnorm regelmäßig nicht bei der „Ferndurchsicht" von Daten bleiben. Vielmehr ist zu befürchten, dass allein schon aus Beweissicherungsgründen eine Datenkopie durch die Ermittlungsbehörden angelegt werden wird. Eine Kopie der Datenträger ist aber – ebenfalls nach dem Verhältnismäßigkeitsgrundsatz – auch nur zu befürchten, wenn eine körperliche Beschlagnahme der Datenträger erfolgt. In der Praxis werden diese heute nicht mehr beschlagnahmt und mitgenommen. Vielmehr fertigen die EDV-Spezialisten der Ermittlungsbehörden regelmäßig Kopien der zu beschlagnahmenden Datenträger, um den Unternehmen und Privatpersonen eine Weiterarbeit zu ermöglichen.

Qualitativ stellt der Entwurf somit kein „weniger" gegenüber der aktuellen Regelung dar.

c. Bestimmtheit

§ 110 Abs. 3 StPO-E **genügt nicht den Bestimmtheitsanforderungen** für Eingriffsnormen.

§ 110 Abs. 3 Satz 1 StPO-E erlaubt die Durchsicht von Speichermedien, zu denen der Betroffene „zugangsberechtigt" ist. Unklar bleibt, wer „Betroffener" ist. Handelt es sich nur um den Beschuldigten oder auch um Dritte? Muss die „Zugangsberechtigung" eine rechtmäßige sein? Ab welchem Stadium darf von der „Durchsicht" zum „Speichern" übergangen werden? In der Praxis ist zu befürchten, dass immer gespeichert werden wird. Allein die Kenntnis der Ermittlungsbehörden von Daten ist in einer eventuellen späteren Hauptverhandlung nur schwer verwertbar, weshalb der Versuch, Beweismittel zu sichern, nachvollziehbar ist.

Ferner bleibt **völlig offen, auf welche Dateien zugegriffen werden darf**. Muss es sich um bereits vorher bekannte Dateien handeln, die lediglich auf dem externen Datenspeicher „gesucht“ werden? Oder darf – wie der Gesetzestext vermuten lässt – der dislokale Datenträger auch auf bislang unbekannte Dateien systematisch „durchkämmt“ werden? Letzteres ist jedenfalls **von Art. 19 Abs. 2 der Cybercrime-Convention nicht gedeckt**. Dort wird als im Entwurf des § 110 Abs. 3 StPO fehlende Eingriffsvoraussetzung lediglich die Schaffung des Zugriffs auf „gesuchte Daten“, also Daten deren Existenz bereits vorher bekannt ist, gefordert.

Insbesondere vor dem Hintergrund, dass es sich bei modernen Datenbeständen regelmäßig um „Verbunddaten“ handelt, ist zur **Verhinderung eines grenzenlosen Durchsuchens eine konkrete Bezeichnung der gesuchten Dateninformationen erforderlich**. Die Speicherung als „Verbunddaten“ z.B. in einem Anwaltsbüro bedeutet, dass es nicht für jeden Mandant einen Ordner gibt in dem – für Ermittler nachvollziehbar – alle Mandantendaten gespeichert sind. Vielmehr verfügen die Anwaltsprogramme über Adressspeicher, in denen die Kontaktdaten aller Mandanten gespeichert sind. Ferner werden die geschriebenen Schriftstücke ebenso in einem allgemeinen Korrespondenzordner gespeichert, wie Abrechnungsdaten zentral abgelegt werden. Beim Aufrufen eines konkreten Mandanten „verbindet“ das Anwaltsprogramm alle im Zusammenhang mit diesem verknüpften Daten (gleich von welchem Speicherort) und stellt sie in einer Maske auf dem Bildschirm zusammen. Würde, wie von § 110 Abs. 3 StPO-E vorgesehen, der unbeschränkte Zugriff auf alle vom Betroffenen dislokal erreichbaren Speichermedien eröffnet, stünde z.B. im Korrespondenzordner auch die nicht von den Ermittlungen betroffene Mandantenkommunikation den Ermittlern zur Verfügung. Deshalb ist eine konkrete Bezeichnung der gesuchten Dateien im richterlichen Durchsuchungsbeschluss unverzichtbar. Im Rahmen des Berechtigungskonzepts des EDV-Programms ist der Online-Zugriff hierauf, also z.B. alle Daten betreffend Mandant X, gleich technisch zu beschränken.

Neben einer Unbestimmtheit auf Seiten der Eingriffsvoraussetzungen ist die Regelung über die Löschung der Daten in § 110 Abs. 3 Satz 2, 2. Halbsatz StPO-E ungenügend. Es fehlt an jeglicher Überwachungs- und Überprüfungsmöglichkeit. Das ist insofern äußerst bedenklich, als nach der Entwurfsregelung die Information des Datenberechtigten, d.h. jedenfalls auch desjenigen auf dessen Datenträger die Daten eingesehen und abgezogen werden, über den „Datenklau“ nicht zwingend erfolgen muss. Häufig ist der Eigentümer des dislokalen Datenträgers nicht der „Betroffene“ im Sinne von § 110 Abs. 3 Satz 1 StPO-E. Nimmt beispielsweise ein Rechtsanwalt das oben beschriebene ASP-Angebot der DATEV e.G. wahr, ist Eigentümerin aller Speichermedien die DATEV e.G.

Die Rechner, auf denen die Anwendungsprogramme laufen, sind ebenso wie alle Datenspeichermedien körperlich im Datenzentrum in Nürnberg aufgestellt.

Schließlich ist vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts zur informationellen Selbstbestimmung eine Verpflichtung zur Information des „Betroffenen“ bzw. des Eigentümers oder Berechtigten des dislokalen Datenträgers zwingende, hier jedoch nicht erfüllte Voraussetzung für die Rechtmäßigkeit einer Eingriffsnorm.

d. Unzulässige Auslandsermittlungen

Die Tätigkeit der Ermittlungsbehörden ist grundsätzlich auf das eigene Hoheitsgebiet beschränkt. Soll eine nationenübergreifende Tätigkeit erfolgen, sind die Ermittlungsbehörden auf die Rechtshilfe angewiesen, die in einer europäischen Konvention oder einzelvertraglich zwischen den Staaten vereinbart sein kann. Die **Gewährung von Rechtshilfe** außerhalb solcher Vertragswerke ist möglich, bedarf jedoch einer gesonderten Anfrage und Genehmigung.

Jeglicher Verstoß sei es durch Ermittlungsmaßnahmen von Beamten vor Ort oder auch nur per Post (schriftliche Zeugenbefragungen) sowie der Datenübergriff stellen einen rechtswidrigen Eingriff in die Hoheitsrechte des anderen Staates dar.

§ 110 Abs. 3 StPO-E ist in seiner unbeschränkten Weite der Zugriffsmöglichkeiten insofern abzulehnen, als er auch den **unbeschränkten Zugriff auf dislokale Datenträger im Drittland** erlaubt. Nach der Cybercrime-Convention ist zwar die „Durchsuchung“ dislokaler Datenträger auch über die Landesgrenzen hinaus zu gewähren bzw. zu dulden. Diese Preisgabe hoheitlicher Rechte kann jedoch nur die Staaten, die sich der Cybercrime-Convention angeschlossen haben, betreffen. „Drittländer“, wie z.B. der für Ermittler interessante Bankenstandort Schweiz sind hiervon nicht betroffen.

Nach der Entwurfsregelung sollen sich die Ermittler keine Gedanken darüber machen müssen, wo sich der Datenträger, auf den via Datenleitung zugegriffen wird, tatsächlich körperlich befindet. Vor diesem Hintergrund ist mit rechtswidrigen Eingriffen in fremde Hoheitsrechte permanent zu rechnen. Eine Norm sollte nicht bereits zum Zeitpunkt ihrer Entstehung gravierende Rechtsverletzungen akzeptieren.

Folge einer unzulässigen Auslandsermittlung kann schon nach aktueller Gesetzeslage ein **Verwertungsverbot** der gewonnenen Informationen in Deutschland sein. Jedenfalls ist in eine eventuelle Regelung des Zugriffs auf dislokale Datenträger ein Verwertungsverbot für rechtswidrig erhobene Informationen zwingend aufzunehmen.

f. Differenzierung Daten und E-Mail

§ 110 Abs. 3 StPO-E differenziert die Eingriffsmöglichkeiten nicht zwischen den verschiedenen, auf dem dislokalen Datenträger gespeicherten Informationen. So kann der Zugriff hierauf materiell die „Durchsicht“ von reinen Daten, also beispielsweise Word-, PDF-, Excel- oder sonstige Files betreffen. Denkbar und in der Praxis sehr wahrscheinlich ist aber auch, dass der „Betroffene“ via Datenleitung den Zugriff auf dislokale E-Mail-Systeme hat. Nicht nur im Unternehmens-, sondern auch im Privatbereich ist der Onlinezugriff via Internet auf E-Mail-Provider wie zB web.de, gmx oder andere, heute üblich. Das Bundesverfassungsgericht hat in einer Reihe von Urteilen begonnen, den Umgang mit „normalen“ Daten, die allgemeinen Beschlagnahmegrundsätzen unterliegen, und mit E-Mails, die als Teil der Telekommunikation dem Schutzbereich des Art. 10 GG unterliegen, herauszuarbeiten (BVerfG 2 BvR 1027/02 vom 12.4.2005; 2 BvR 2099/04 vom 2.3.2006; 2 BvR 902/06 vom 29.6.2006). So ist gerade die Frage, wann ein Übertragungsvorgang bei E-Mails, die an einen von dem Betroffenen gehaltenen Online-Account gehen, abgeschlossen ist und ein Zugriff nicht mehr den Voraussetzungen des § 100 a StPO unterliegt in der Rechtsprechung der Landgerichte und der Literatur umstritten (vgl. LG Ravensburg, 2 Qs 153/02 vom 9.12.2002, NStZ 2003, 325; SPATSCHECK/SCHMID, PStR 2005, 288).

Vor diesem Hintergrund ist eine deutliche Differenzierung zwischen E-Mail-Verkehr als Telekommunikation und den „ruhenden“ Daten für jede neue Ermächtigungsnorm zwingende Voraussetzung. Eine Regelung, die gerade auf dieses drängende Praxisproblem der Abgrenzung nicht eingeht, ist nicht nur unsensibel und rechtswidrig, sondern auch praxisuntauglich.

g. Unzulässiges „staatliches“ Hacking

§ 110 Abs. 3 StPO-E **ermöglicht das unzulässige staatliche Online-Hacking.**

Der Bundesgerichtshof (StB 18/06 vom 31.1.2007) hat die **verdeckte staatliche Online-Durchsuchung** für unzulässig erklärt. Eine solche würde bei Einführung der Entwurfsvorschrift im Rahmen der „Durchsicht von Papieren“ **quasi faktisch unter Umgehung der Eingriffsermächtigung der §§ 102 ff. StPO eingeführt**.

Die Daten, auf die sich die Durchsicht nach § 110 Abs. 3 Satz 1 StPO-E erstrecken soll, werden regelmäßig nicht nur dem „Betroffenen“ zustehen. Vielmehr ist denkbar und wahrscheinlich, dass beispielsweise im Rahmen der Durchsuchung einer Anwaltssozietät wegen eines Ermittlungsverfahrens gegen einen der Sozien, weitere Datenberechtigte existieren. Für Letztere sowie für den Eigentümer bzw. „Betreiber“ der dislozierten Datenträger, der von dem Eingriff jedenfalls nichts weiß, stellt die Durchsicht sowie das Kopieren der Daten im Rahmen der Entwurfsnorm eine verdeckte Online-Durchsuchung dar. Diese ist nicht einmal an Voraussetzungen geknüpft, wie z.B. einen vorangehenden vergeblichen Versuch, die Daten vor Ort im Wege der Beschlagnahme des Datenträgers zu sichern.

h. **Fazit**

Das Bedürfnis der Ermittlungsbehörden dem technischen Fortschritt entsprechend Zugriffsmöglichkeiten auf dislozierte Datenträger zu erhalten, ist anzuerkennen und zu respektieren. Eine solche Zugriffsmöglichkeit wird nicht grundsätzlich abgelehnt. Doch ist gerade im Hinblick auf die Eingriffsintensität eines solchen Vorgehens eine s**orgfältig ausgearbeitete, bestimmte Ermächtigungsgrundlage zu fordern**, die folgende Voraussetzungen erfüllen sollte:

- Zugriff auf dislokale Datenträger nur, wenn bereits bekannt ist, dass dort für das Ermittlungsverfahren bedeutsame Daten gespeichert sind,

- die Daten müssen im richterlichen Durchsuchungsbeschluss jedenfalls konkret bezeichnet sein,

- der zwingend vorausgehende Versuch, die Daten auf klassische Weise, also durch Beschlagnahme der Datenträger, zu sichern, muss nachgewiesen werden,

  ein Verwertungsverbot für rechtswidrig online-kopierte Daten, die z.B. von Servern in „Drittländern“ abgezogen wurden, wird im Gesetz aufgenommen,

- wer „Betroffener“ ist, muss ebenso eindeutig geklärt sein, wobei hier nur der „Beschuldigte“ in Betracht kommen kann,

- gleiches gilt für die Art des Zugriffsrechts auf dislokale Datenträger, das dem Betroffenen zusteht, wobei alle möglichen technischen Einschränkungen z.B. Nur-Lesezugriff auf konkrete Daten, wahrgenommen werden müssen,

- es ist eine Differenzierung zwischen E-Mails und sonstigen Daten vorzunehmen,

- eine systematische Aufnahme der Regelung für die „bloßen“ Daten (keine E-Mails) unmittelbar bei den Durchsuchungsvorschriften, §§ 102 ff. StPO, bringt die erforderliche Klarheit über deren Inhalt.

Der aktuelle § 110 Abs. 3 StPO-E erfüllt diese Voraussetzungen nicht.

F.

Gesetz (...) zur Umsetzung der Richtlinie 2006/24/EG

Die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die **Vorratsspeicherung von Daten**, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG – im folgenden Richtlinie genannt – verletzt europäisches Vertragsrecht und Art. 8 EMRK. Beim EuGH sind Klagen anhängig, mit denen die Nichtigerklärung der Richtlinie beantragt ist. Sollte der EuGH den Klagen stattgeben, die Richtlinie für nichtig erklären und erkennen, dass die Vorratsdatenspeicherung vertragskonform nur im Unionsrecht (3. Säule) – und nicht wie hier im Gemeinschaftsrecht (1. Säule) – geregelt werden kann, entfällt die Umsetzungspflicht der Bundesrepublik Deutschland.

Im Einzelnen:

1. Inhalt der Richtlinie

a.
Art. 3 i.V.m. Art. 5 der Richtlinie verpflichtet die Mitgliedsstaaten, sicherzustellen, dass solche Daten auf Vorrat gespeichert werden, die bei den Anbietern elektronischer Kommunikationsdienste oder Kommunikationsnetze betriebsbedingt anfallen – wie etwa Rufnummer, Rufum-, und -weiterleitung, Namen und Anschriften der Teilnehmer oder der registrierten Benutzer, Protokolladresse (IP-Adresse), Benutzerkennung, Kalenderdaten, Uhrzeit und Dauer der Kommunikation sowie Daten zur Standorterkennung.

b.
Die **Speicherung** setzt weder einen Tatverdacht noch eine Katalogstraftat voraus. Es handelt sich um eine „**verdachtslose Maßnahme**“. Nach Art. 1 Abs. 1 der Richtlinie erfolgt die Vorratsdatenspeicherung, „*um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedsstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen*“.

c.
Art. 8 der Richtlinie verpflichtet die Mitgliedsstaaten, die Daten so zu speichern, dass sie *„unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können“*. Nach Art. 10 der Richtlinie sollen die Mitgliedsstaaten dafür sorgen, dass der Kommission jährlich eine Statistik über die Vorratsspeicherung übermittelt wird, aus der hervorgeht, *„in welchen Fällen im Einklang mit dem innerstaatlichen Recht Daten an die zuständigen Behörden weitergegeben worden sind“*, *„wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefordert wurden, vergangen ist“* und *„in welchen Fällen die Anfragen nach Daten ergebnislos geblieben sind“*. Spätestens am 15. September 2010 soll die Kommission dem Europäischen Parlament und dem Rat *„eine Bewertung der Anwendung dieser Richtlinie sowie ihre Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher vorlegen, um festzustellen, ob die Bestimmungen dieser Richtlinie (...) geändert werden müssen“* (Art. 14 Abs. 1 der Richtlinie).

d.
Gemäß Art. 15 Abs. 1 der *Richtlinie* sind die Mitgliedsstaaten verpflichtet, die Richtlinie spätestens bis 15. September 2007 umzusetzen. Nach Abs. 3 S. 1 dieser Vorschrift kann jeder Mitgliedsstaat bis 15. März 2009 die Anwendung dieser Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonieren, Internet-E-Mail aufschieben. Hiervon hat die Bundesrepublik Deutschland Gebrauch gemacht und erklärt, dass sie sich das Recht vorbehält, die Anwendung der Richtlinie insoweit für einen Zeitraum von 18 Monaten ab dem in Art. 15 Abs. 1 S. 1 genannten Zeitpunkt (15. September 2007), mithin bis zum 15. Januar 2009, zurückzustellen.

2. **Unvereinbarkeit** der Richtlinie mit europäischem Recht

Das Europäische Parlament und der Rat der Europäischen Union stützen die Richtlinie auf Art. 95 des Vertrages zur Gründung der Europäischen Gemeinschaft (EGV). Diese Norm ermächtigt den Rat, Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedsstaaten, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben, zu erlassen. Während Richtlinien nach Art. 95 EGV (Gemeinschaftsrecht, 1. Säule) mit qualifizierter Mehrheit beschlossen werden können, setzt der Erlass eines Rahmenbeschlusses gemäß Art. 34 des Vertrages über die Europäische Union (EUV) (Unionsrecht, 3. Säule) Einstimmigkeit voraus.

Die Mitgliedsstaaten **Irland**[17] **und Slowakei** halten die Verfahrensweise von Europäischem Parlament und Rat der Europäischen Union für **vertragsrechtswidrig** und haben bei dem ***EuGH*** beantragt, die **Richtlinie für nichtig zu erklären**. Sie sind der Auffassung, dass die Vorratsdatenspeicherung ihre **Rechtsgrundlage im Unionsrecht (3. Säule)** findet, also nur mit einem aufgrund Art. 34 EUV **einstimmig erlassenen Rahmenbeschluss geregelt** werden kann und **nicht** mit einer auf Art. 95 EGV gestützten **Richtlinie**. Sollte der *EuGH* den Klagen stattgeben und die Richtlinie für nichtig erklären, entfällt für die Bundesrepublik Deutschland die Pflicht, die Richtlinie umzusetzen.

[17] Rechtssache C-301/06: Irland gegen den Rat der Europäischen Union und das Europäische Parlament (OJ L 105, S. 54).

Die **Klagen werden erfolgreich sein**. Dies ergibt sich aus Folgendem:

a.

Mit **Urteil vom 30. Mai 2006** hat der ***EuGH*** zum *Abkommen zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security (CBP)* erklärt, dass Art. 95 EGV die Zuständigkeit der Gemeinschaft für den Abschluss des Abkommens nicht begründen könne, da die Übermittlung der Fluggastdatensätze an CBP eine Verarbeitung darstelle, die die öffentliche Sicherheit und die Tätigkeiten des Staates im strafrechtlichen Bereich betreffe[18]. Zwar treffe es aus Sicht des *EuGH* zu, dass die Fluggastdatensätze von den Fluggesellschaften ursprünglich im Rahmen einer unter das Gemeinschaftsrecht fallenden Tätigkeit erhoben worden seien, nämlich im Rahmen des Verkaufs eines Flugscheins, der zu einer Dienstleistung berechtige; die Datenverarbeitung, die in der Angemessenheitsentscheidung Berücksichtigung finde, sei jedoch von anderer Art. Denn diese Entscheidung beziehe sich – so der *EuGH* – auf eine Datenverarbeitung, die nicht für die Erbringung einer Dienstleistung erforderlich sei, sondern zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken als erforderlich angesehen werde[19]. Interpretiert wird diese Entscheidung so, dass in den Fällen, in denen ein Rechtsakt eine dem Strafrecht zugehörige Maßnahme legalisiere, die nicht der Durchsetzung gemeinschaftlich geregelter Bereiche diene, die Ermächtigungsgrundlage für diesen Rechtsakt auch nicht dem Gemeinschaftsrecht, sondern **nur dem Unionsrecht (3. Säule) entnommen werden könne[20]**.

b.

Geht man hiernach, steht fest, dass die Vorratsdatenspeicherung nicht der Durchsetzung gemeinschaftlich geregelter Bereiche dient und demnach die Ermächtigungsgrundlage für diesen Rechtsakt nicht dem Gemeinschaftsrecht, sondern nur dem Unionsrecht entnommen werden kann. Denn die in Art. 6 der Richtlinie geregelten Speicherungsfristen *„für einen Zeitraum von mindestens sechs Monaten und höchsten zwei Jahren ab dem Zeitpunkt der Kommunikation“* stehen einer europarechtlichen Harmonisierung der nationalen Vorschriften zur Vorratsdatenspeicherung entgegen.

---

18 *EuGH*, NJW 2006, 2029, 2032 f., Rdn. 67, 56.

19 *EuGH*, NJW 2006, 2029, 2032 Rdn. 57.

20 So *Leutheusser-Schnarrenberger*, ZRP 9, 12, die – gestützt auf das Urteil des EuGH v. 13.09.2005 – von Gemeinschaftsrecht ausgehen will, wenn „die Harmonisierung strafrechtlicher Normen der Mitgliedsstaaten zum Zwecke der Durchsetzung gemeinschaftsrechtlich festgeschriebener Ziele (wie der Verstärkung des Umweltschutzes) dienen“.

Die Richtlinie würde nur dann einen Beitrag zur primären Binnenmarktorientierung leisten, wenn für alle Mitgliedsstaaten einheitliche Speicherfristen gelten. Dies ist aber nicht der Fall. Der Zustand ist unharmonisch[21], wenn die Mitgliedsstaaten die Daten uneinheitlich, das heißt sechs, acht, 16 oder 20 Monate speichern. Hinzukommt, dass die Vorratsdatenspeicherung der Ermittlung, Feststellung und Verfolgung von schweren Straftaten dienen soll (Art. 1 Abs. 1 der Richtlinie). Der Richtlinie liegen also vornehmlich sicherheitspolitische – und nicht binnenmarktpolitische – Erwägungen zugrunde.

3. **Unvereinbarkeit** der Richtlinie mit **Art. 8 EMRK**

Prüfungsmaßstab für das sekundäre Gemeinschaftsrecht, mithin für die hier in Rede stehende Richtlinie, ist das **primäre Gemeinschaftsrecht**. Hierzu zählen nicht nur die Gründungsverträge der Gemeinschaft (wie etwa EGV), sondern **auch** und insbesondere die **Gemeinschaftsgrundrechte als allgemeine Rechtsgrundsätze des Gemeinschaftsrechts** (vgl. Art. 6 Abs. 2 EUV). Die Gemeinschaftsgrundrechte hat der *EuGH* aus den Verfassungen der Mitgliedsstaaten entwickelt; die **europäische Menschenrechtskonvention (EMRK)** wendet der *EuGH* in der Regel in ihrer Auslegung durch den Europäischen Gerichtshof für Menschenrechte an[22].

Die **Richtlinie verstößt gegen Art. 8 Abs. 1 EMRK**. Nach Abs. 1 dieser Norm hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. In die Ausübung dieses Rechtes darf nur unter den Voraussetzungen des Art. 8 Abs. 2 EMRK eingegriffen werden. Danach muss der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sein *für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer*. Der Verhältnismäßigkeitsgrundsatz ist zu beachten[23]. Von einer Verhältnismäßigkeit der Maßnahme aber kann nicht ausgegangen werden. Es steht bereits nicht fest, dass eine Vorratsdatenspeicherung rechtstatsächlich überhaupt geeignet und erforderlich ist. Zudem fehlt es an der Verhältnismäßigkeit im engeren Sinne. Denn von der Vorratsdatenspeicherung werden Millionen von Menschen betroffen sein, von denen weder ein Anfangsverdacht oder gar der Verdacht einer schweren Straftat ausgeht. Die Daten, die die Strafverfolgungsbehörde aller Voraussicht nach verwerten werden, werden nach nur einen Bruchteil der insgesamt gespeicherten Daten ausmachen. Bereits dieses Missverhältnis macht deutlich, dass die Maßnahme unverhältnismäßig ist.

---

21 vgl. *Leutheusser-Schnarrenberger*, ZRP 2007, 9, 12.

22 *EuGH*, Urteil vom 20.05.2003, Az: C-465/00, EuGRZ 2003, 232, 238, 69 und 73 ff.

23 *EGMR*, NJW 1993, 718; StraFo 2005, 371.

Dieses Ergebnis stellt sich ebenfalls ein, wenn man die Richtlinie an Art. 8 der Charta der Grundrechte der Europäischen Union misst. Dieser verlangt in Abs. 2 eine Einwilligung oder eine gesetzlich geregelte legitimierte Grundlage. Die Charta ist zwar noch nicht förmlich in Kraft getreten, mithin kein bindendes Rechtsinstrument. Die Grundrechte aber sieht der *EuGH* als integraler Bestandteil der allgemeinen Rechtsgrundsätze an[24].

4. **Unvereinbarkeit** des Gesetzes (...) zur Umsetzung der Richtline **mit dem Grundgesetz**

Werden die Klagen der Mitgliedsstaaten Irland und Slowakei erfolgreich sein und der *EuGH* die Richtlinie für nichtig erklären, entfällt für die Bundesrepublik Deutschland die Pflicht, die Richtlinie umzusetzen. Konsequenz wäre, dass das nationale Gesetz, mit welchem die Richtlinie voreilig umgesetzt wird, im Wege der abstrakten Normkontrolle und der Verfassungsbeschwerde vom Bundesverfassungsgericht zur Prüfung angenommen werden könnte. Denn in diesem Fall ginge es nicht mehr um die Umsetzung von sekundärem Gemeinschaftsrecht mit der Folge, dass die *Solange II* – Entscheidung[25] das Bundesverfassungsgericht nicht hindern würde, die Verfassungsmäßigkeit des nationalen Gesetzes am Grundgesetz zu prüfen. Aus der *Solange II* – Entscheidung und den nachfolgenden Entscheidungen zum Maastrichtvertrag[26] und zur Bananenmarktordnung[27] folgt „lediglich“, dass die nationalen Rechtsakte, die sekundäres Gemeinschaftsrecht umsetzen, dass dem nationalen Gesetzgeber keinen Spielraum lässt, nicht verfassungsrechtlich überprüft und entsprechende Verfassungsbeschwerden vom Bundesverfassungsgericht für unzulässig erklärt werden. In der Verfassungsgerichtsentscheidung zur Europäischen Bananenordnung erklärt das Bundesverfassungsgericht hierzu:

> „Verfassungsbeschwerden (...), die eine Verletzung von Grundrechten des Grundgesetzes durch sekundäres Gemeinschaftsrecht geltend machen, sind von vornherein unzulässig, wenn ihre Begründung nicht darlegt, dass die europäische Rechtsentwicklung einschließlich der Rechtsprechung des *EuGH* nach Ergehen der *Solange II* – Entscheidung unter dem erforderlichen Grundrechtstandard abgesunken ist“[28].

---

24 *EuGH*, Urteil vom 27.06.2006, Rechtssache C 540/03 Europäisches Parlament ./. Rat der EU.
25 *BVerfG* NJW 1987, 577.
26 *BVerfG* NJW 1993, 3047.
27 *BVerfG* NJW 2000, 3124.
28 *BVerfG* NJW 2000, 3124.

In dem Fall aber, in dem der *EuGH* die Richtlinie für nichtig erklärt, geht es nicht mehr um die Verletzung von Grundrechten des Grundgesetzes durch sekundäres Gemeinschaftsrecht, sondern um die Verletzung von Grundrechten des Grundgesetzes durch das nationale Gesetz, mit dem die Richtlinie voreilig umgesetzt worden ist.

Dass das Gesetz zur Umsetzung der Richtlinie gegen das Grundgesetz verstößt und daher abstrakte Normkontrolle und Verfassungsbeschwerde Aussicht auf Erfolg hätten, liegt auf der Hand. Denn das **Gesetz zur Umsetzung der Richtlinie verstößt gegen das strikte – nationale – Verbot der Sammlung personenbezogener Daten auf Vorrat.** Bereits in den 80er Jahren hat das ***BVerfG*** **klargestellt**, dass der Zwang zur Angabe personenbezogener Daten voraussetze,

> „dass der Gesetzgeber den Verwendungszweckbereich spezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren“ (*BVerfGE* 65, 1, 47 = NJW 1984, 419).

In der sogenannten **Rasterfahndungsentscheidung** hat das ***BVerfG*** dies noch einmal **bestätigt** und erklärt, dass die Frage, ob ein Grundrechtseingriff zur Abwehr künftig drohender Rechtsgutbeeinträchtigung auch im Vorfeld konkreter Gefahren verhältnismäßig sein kann, auch davon abhänge,

> „welche Anforderungen die Eingriffsnorm hinsichtlich der Nähe der betroffenen Person zur fraglichen Rechtsgutbedrohung vorsieht (...). Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht“ (*BVerfG* NJW 2006, 1936, 1946).

Zwar spricht der Entwurf der Bundesregierung diese Entscheidung des *BVerfG* ausdrücklich an und führt aus, dass sich das strikte Verbot der *Vorratsdatensammlung* auf die Sammlung von Personendaten „auf Vorrat“ zu unbestimmten oder noch nicht bestimmbaren Zwecken beziehe, dies aber nicht Gegenstand des Entwurfes sei, sondern mit der Einführung von Speicherungspflichten für Verkehrsdaten lediglich sichergestellt werden solle, dass „diese Daten für Zwecke der Strafverfolgung zur Verfügung stehen“ (Entwurf der Bundesregierung, Stand 27.6.2007, BT-Drs. 16/5846, S.74).

Dies jedoch überzeugt nicht. Die **allgemeine Zweckbestimmung „Strafverfolgung“ genügt verfassungsrechtlichen Anforderungen nicht.** Die in § 110 a TKÜ-E geregelte Pflicht der Telekommunikationsdiensteanbieter, Verkehrsdaten für die Zwecke der Strafverfolgung sechs Monate im Inland zu speichern, ist mit dem Grundrecht auf Fernmeldegeheimnis (Art. 10 Abs. 1 GG) und mit dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) unvereinbar. Der Zweck – „Strafverfolgung“ – trägt den Anforderungen an das besondere Gewicht des zu verfolgenden Rechtsgutes nicht Rechnung. In seiner Entscheidung zum *NdsSOG* hat das ***BVerfG*** **erklärt, dass Strafverfolgung an den Verdacht einer schon verwirklichten Straftat anknüpft und ein solcher Bezug fehlt, soweit die Aufgabe darin besteht, im Vorfeld der Strafverfolgung Vorsorge im Hinblick auf in der Zukunft eventuell zu erwartende Straftaten zu treffen.** Das *BVerfG* stellt klar, dass deshalb die Bestimmtheitsanforderungen spezifisch an die Vorfeldsituation ausgerichtet werden müssen – dergestalt, dass der Gesetzgeber

> „die den Anlass bildenden Straftaten sowie die Anforderungen an Tatsachen, die auf die künftige Begehung hindeuten, so bestimmt zu umschreiben hat, dass das im Bereich der Vorfeldermittlung besonders hohe Risiko einer Fehlprognose gleichwohl verfassungsrechtlich noch hinnehmbar ist. Die Norm muss handlungsbegrenzende Tatbestandsmerkmale enthalten, die ein Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten ist“ (*BVerfG*, NJW 2005, 2603, 2608).

Diesen Anforderungen genügt § 110 a TKÜ-E nicht. Die Vorschrift verlangt keine konkreten, in der Entwicklung begriffenen – strafrechtlichen – Vorgang oder dessen Planung. Sie will anlasslos sämtliche Daten gespeichert wissen, die bei der Kommunikation mittels Festnetz, Mobilfunk und Internet anfallen. Das ist zu unbestimmt und unverhältnismäßig.

5. **Fazit:**

Der Gesetzgeber ist aufgefordert, **von einer Umsetzung der Richtlinie abzusehen**. Zumindest sollte er die Entscheidung des *EuGH* über die Klagen der Mitgliedsstaaten Irland und Slowakei abwarten. Denn es ist davon auszugehen, dass die Klagen Aussicht auf Erfolg haben und der *EuGH* die Richtlinie für nichtig erklären wird.

Sollte der *EuGH* dies tun, entfällt für die Bundesrepublik Deutschland die Umsetzungspflicht mit der Folge, dass ein bereits verabschiedetes „Umsetzungsgesetz“ im Wege der abstrakten Normenkontrolle und der Verfassungsbeschwerde vom Bundesverfassungsgericht zur Prüfung angenommen werden könnte. Da es nicht mehr um die Umsetzung von sekundärem Gemeinschaftsrecht ginge, stünde die sogenannte „Solange II – Entscheidung“ des *BVerfG* nicht im Wege.

Selbst wenn der *EuGH* die Nichtigkeitsklagen abweisen und die Richtlinie – wider Erwarten – im Einklang mit europäischem Vertragsrecht und Gemeinschaftsgrundrechten sehen sollte, ist der **Bundesgesetzgeber ebenso aufgefordert, von einer Umsetzung abzusehen**. Dies **folgt** nicht zuletzt aus der **Entscheidung des *BVerfG* über das Europäische Haftbefehlsgesetz**[29]. Das *BVerfG* hat erklärt, dass der Gesetzgeber verpflichtet sei, die Umsetzungsspielräume, die der Rahmenbeschluss den Mitgliedsstaaten belässt, in einer **grundrechtsschonenden Weise auszufüllen**. Deutlich gemacht hat diese Entscheidung, dass das *BVerfG* nicht bereit ist, *„es hinzunehmen, wenn der deutsche Gesetzgeber Vorgaben aus Brüssel ohne Rücksicht auf elementare Grundsätze des deutschen Verfassungsrechts in nationales Recht umsetzt“*[30]. Dies bedeutet, dass die verfassungsrechtliche Gewährleistung der Grundrechte nicht dadurch eingeschränkt werden kann, dass Staaten sich gegenseitig anerkennen[31]. Zwar ist zuzugeben, dass der Gesetzgeber nach Art. 10 EGV verpflichtet ist, sekundäres Gemeinschaftsrecht in nationales Recht umzusetzen. Eine **Umsetzung contra Verfassungsrecht** ist aber – gemessen an der Entscheidung des *BVerfG* zum Gesetz über das Europäische Haftbefehlsgesetz – **nicht ohne weiteres möglich**. Ist der Grundrechtsverstoß – wie hier – offensichtlich, ist davon auszugehen, dass das *BVerfG* reagieren und seine Rechtsprechung zum Gesetz über das Europäische Haftbefehlsgesetz in einer **„Solange III – Entscheidung“** konsequent fortschreiben wird.

---

29 *BVerfG*, NJW 2005, 2289.

30 *Glauben*, DRiZ 2007, 34.

31 vgl. *Bosbach*, NStZ 2006, 104, 105.