

01.03.19

**Empfehlungen**  
der Ausschüsse

R - In

zu **Punkt ...** der 975. Sitzung des Bundesrates am 15. März 2019**Entwurf eines Strafrechtsänderungsgesetzes - Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen****- Antrag der Länder Nordrhein-Westfalen und Hessen -****A.**

Der **federführende Rechtsausschuss (R)** und  
der **Ausschuss für Innere Angelegenheiten (In)**

empfehlen dem Bundesrat,

den Gesetzentwurf gemäß Artikel 76 Absatz 1 des Grundgesetzes nach Maßgabe folgender Änderungen beim Deutschen Bundestag einzubringen:

- R,  
In  
  
(bei  
Annahme  
entfällt  
Ziffer 3)
1. Zu Artikel 1 Nummer 2 (§ 126a Überschrift,  
Absatz 1 Satz 1,  
Satz 2,  
Absatz 2,  
Absatz 3,  
Absatz 4 – neu – StGB)

In Artikel 1 Nummer 2 ist § 126a wie folgt zu ändern:

- a) In der Überschrift ist das Wort „Anbieten“ durch das Wort „Zugänglichmachen“ und das Wort „Ermöglichung“ durch das Wort „Begehung“ zu ersetzen.

- b) Absatz 1 ist wie folgt zu ändern:
- aa) Satz 1 ist wie folgt zu ändern:
- aaa) Das Wort „anbietet“ ist durch das Wort „zugänglich macht“ zu ersetzen.
- bbb) Die Wörter „deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und“ sind zu streichen.
- ccc) Die Wörter „im Sinne von Satz 2“ sind zu streichen.
- ddd) Die Wörter „ermöglichen oder zu fördern“ sind durch die Wörter „ermöglichen, zu fördern oder zu erleichtern“ zu ersetzen.
- eee) Das Wort „drei“ ist durch das Wort „fünf“ zu ersetzen.
- bb) Satz 2 ist zu streichen.
- c) In Absatz 2 ist die Angabe „Satz 2“ zu streichen.
- d) In Absatz 3 ist das Wort „gewerbsmäßig“ durch die Wörter „gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten im Sinne dieser Vorschrift verbunden hat,“ zu ersetzen.
- e) Folgender Absatz 4 ist anzufügen:
- „(4) Absatz 1 gilt nicht für Handlungen,
1. wenn die Begehung von Straftaten nur einen Zweck oder eine Tätigkeit von untergeordneter Bedeutung darstellt, oder
  2. die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen.“

#### Folgeänderungen:

- a) In Artikel 1 Nummer 1 ist in der Inhaltsübersicht die Angabe zu § 126a wie folgt zu fassen:
- „§ 126a Zugänglichmachen von Leistungen zur Begehung von Straftaten“
- b) Das Vorblatt ist wie folgt zu ändern:
- aa) Der Abschnitt „A. Problem und Ziel“ ist wie folgt zu ändern:
- aaa) Dem Absatz 1 ist folgender Absatz voranzustellen:

„Der – nicht selten anonyme und mittels Krypto-Währungen abgewickelte – Handel mit illegalen Waren und Dienstleistungen – insbesondere mit Betäubungsmitteln, Kinderpornographie, Schadsoftware, Falschgeld, Ausweispapieren oder Waffen – über das Internet hat aufgrund der Möglichkeit der Anonymisierung, die das Internet bietet, erheblich zugenommen. Entsprechende Handelsplattformen finden sich im für jedermann ohne Weiteres zugänglichen Bereich des Internets (sogenanntes Surface-Web), vermehrt aber auch im sogenannten Darknet.“

bbb) Absatz 1 ist wie folgt zu fassen:

„Der Zugang zum Darknet erfolgt insbesondere über das „The Onion Router“ (Tor)-Netzwerk, das aus einer Vielzahl von weltweit verteilten Servern besteht, über die Datenpakete in ständig wechselnder Form geleitet werden. Beim Verbindungsaufbau wird durch das Programm eine zufällige Route über einen Teil der Server festgelegt, ohne dass Herkunft oder Ziel der Daten protokolliert werden. Durch die Verschlüsselung der Nutzerdaten und die dynamische Routenwahl wird die Feststellung von Anfangs- und Endpunkten eines Datentransfers erheblich erschwert. Zugang und Erreichbarkeit der Darknet-Angebote sind durch das Erfordernis besonderer Programme, wie des Tor-Browsers, beschränkt.“

ccc) Absatz 5 ist wie folgt zu fassen:

„Weil der Zugang zu den einschlägigen Angeboten in der Regel keinen besonderen technischen Anforderungen unterliegt und die Erreichbarkeit teilweise zwar beschränkt, aber ohne erheblichen technischen Aufwand möglich ist, bieten die Handelsplattformen somit einen niedrigschwelligen Zugriff auf logistische Infrastrukturen für die Begehung von Straftaten auch für Personen, die herkömmliche Beschaffungswege für Waffen, Betäubungsmittel oder kriminelle Dienstleistungen nicht beschreiten. Auf diese Weise wird einer unbestimmten Vielzahl von Personen die Möglichkeit verschafft, eine unbestimmte Vielzahl von Straftaten zu begehen. Diese Angebote stellen eine erhebliche Gefahr für die öffentliche Sicherheit dar, ohne dass die geltende

Rechtslage ausreichende Möglichkeiten für eine angemessene strafrechtliche Verfolgung bietet.“

bb) Der Abschnitt „B. Lösung“ ist wie folgt zu fassen:

**„B. Lösung**

Der Gesetzentwurf führt einen neuen Straftatbestand des Zugänglichmachens von Leistungen zur Begehung von Straftaten ein. Der Tatbestand erfasst die internetbasierte Zugänglichmachung und setzt die Ausrichtung der Leistung auf die Ermöglichung, Förderung oder Erleichterung von rechtswidrigen Taten voraus. Ergänzt wird der Grundtatbestand durch Qualifikationen im Falle der gewerbsmäßigen oder bandenmäßigen Tatbegehung sowie einen Tatbestandsausschluss unter anderem für Handlungen von Personen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Die Qualifikation soll Anknüpfungstat für die cyberspezifische Ermittlungsmaßnahme der Telefonüberwachung sein.“

c) Die Begründung ist wie folgt zu ändern:

aa) Der Abschnitt „A. Allgemeines, I. Zielsetzung und wesentlicher Inhalt des Gesetzesentwurfs“ ist wie folgt zu ändern:

aaa) Dem Absatz 1 ist folgender Absatz 0 voranzustellen:

„Der – nicht selten anonyme und mittels Krypto-Währungen abgewickelte – Handel mit illegalen Waren und Dienstleistungen (insbesondere mit Betäubungsmitteln, Kinderpornographie, Schadsoftware, Falschgeld, Ausweispapieren oder Waffen) über das Internet hat aufgrund der Möglichkeit der Anonymisierung, die das Internet bietet, erheblich zugenommen. Entsprechende Handelsplattformen finden sich im für jedermann ohne Weiteres zugänglichen Bereich des Internets (sogenanntes Surface-Web), vermehrt aber auch im sogenannten Darknet.“

bbb) Absatz 1 ist wie folgt zu fassen:

„Der Zugang zum Darknet erfolgt insbesondere über das „The Onion Router“ (Tor)-Netzwerk, das aus einer Vielzahl von weltweit verteilten Servern besteht, über die Datenpakete in ständig wechselnder Form geleitet werden. Beim Verbindungsaufbau wird durch das Programm eine zufällige Route über ei-

nen Teil der Server festgelegt, ohne dass Herkunft oder Ziel der Daten protokolliert werden. Durch die Verschlüsselung der Nutzerdaten und die dynamische Routenwahl wird die Feststellung von Anfangs- und Endpunkten eines Datentransfers erheblich erschwert. Zugang und Erreichbarkeit der Darknet-Angebote sind durch das Erfordernis besonderer Programme, wie des Tor-Browsers, beschränkt.'

ccc) Absatz 8 ist wie folgt zu fassen:

„Weil der Zugang zu den einschlägigen Angeboten in der Regel keinen besonderen technischen Anforderungen unterliegt und die Erreichbarkeit teilweise zwar beschränkt, aber ohne erheblichen technischen Aufwand möglich ist, bieten die Handelsplattformen somit einen niedrighschwelligen Zugriff auf logistische Infrastrukturen für die Begehung von Straftaten auch für Personen, die herkömmliche Beschaffungswege für Waffen, Betäubungsmittel oder kriminelle Dienstleistungen nicht beschreiten. Auf diese Weise wird einer unbestimmten Vielzahl von Personen die Möglichkeit verschafft, eine unbestimmte Vielzahl von Straftaten zu begehen. Diese Angebote stellen eine erhebliche Gefahr für die öffentliche Sicherheit dar, ohne dass die geltende Rechtslage ausreichende Möglichkeiten für eine angemessene strafrechtliche Verfolgung bietet.“

ddd) Absatz 9 ist wie folgt zu fassen:

„Diese Lücken sollen durch die Einführung der neuen Vorschrift geschlossen werden. Der Entwurf zielt darauf, das Betreiben von auf die Förderung, Ermöglichung oder Erleichterung illegaler Zwecke ausgerichteten Plattformen unabhängig von dem Nachweis der Beteiligung an einzelnen konkreten Handelsgeschäften unter Strafe zu stellen. Die Vorschrift soll die öffentliche Sicherheit und die staatliche Ordnung schützen, daher erfolgt die Aufnahme in den sechsten Abschnitt. Die Aufnahme eines Tatbestands in das Strafgesetzbuch fördert eine einheitliche Rechtsanwendung und erscheint daher gegenüber spezialgesetzlichen Einzelregelungen vorzugswürdig. Soweit vereinzelt bereits Strafvorschriften das Verschaffen einer Gelegenheit zur Bege-

hung von Straftaten erfassen, zum Beispiel § 29 Absatz 1 Nummer 10 BtMG, regelt § 126a StGB-E den Sonderfall der internetbasierten Tatbegehung. Dem Konkurrenzverhältnis wird insoweit durch eine Subsidiaritätsklausel in § 126a Absatz 1 StGB-E Rechnung getragen.“

eee) Absatz 10 ist wie folgt zu fassen:

„Eine Einschränkung auf nur bestimmte, für das geschützte Rechtsgut besonders gefährlich einzustufende szenetypische Delikte ist aus Gründen der Verhältnismäßigkeit nicht erforderlich und nicht sachgerecht. Ein solcher Katalog liefe – ähnlich einer Neuregelung in einzelnen Spezialgesetzen – Gefahr, unvollständig zu bleiben. Zum anderen ist die Zugänglichmachung jedes internetbasierten Angebots, das auf die Begehung jeglicher Straftaten gerichtet ist, gleichermaßen strafwürdig. Dies gilt zum Beispiel auch für Plattformen, welche auf die Begehung von Äußerungsdelikten gerichtet sind. Dem Verhältnismäßigkeitsgrundsatz wird durch die ausdrückliche Beschränkung des Absatzes 2 Rechnung getragen, die sicherstellt, dass die Strafe nicht schwerer sein darf als die für die ermöglichten rechtswidrigen Taten angedrohte Strafe. Die Gefährlichkeit der Delikte wird durch die internetbasierte Begehung erheblich erhöht, da die Leistungen quasi ohne Beschränkung zugänglich sind. Der potentielle Adressatenkreis ist damit praktisch unbegrenzt. Die Täter des § 126a StGB-E eröffnen durch die Handelsplattformen einen örtlich, zeitlich und sachlich unbegrenzten Zugang zu illegalen Waren und Dienstleistungen, der in der analogen Welt auch nicht annähernd vergleichbar besteht oder möglich wäre und Grundlage weiterer digitaler oder analoger Handelsketten sein kann.“

fff) Absatz 11 ist wie folgt zu fassen:

„Die Vorschrift ist hinsichtlich ihres sachlichen Anwendungsbereichs auch zur Ermöglichung der Berücksichtigung der weiteren technischen Entwicklung weit gefasst und erfasst jegliche internetbasierte Zugänglichmachung von Leistungen. Der Begriff „internetbasiert“ ist hierbei technikbezogen auszulegen und erfasst

alle Dienste, die auf der Netzwerkschicht des OSI-Referenzmodells über das Internet-Protokoll (IP) vermittelt werden. Über den allgemeinen Sprachgebrauch zum Begriff „Internet“ hinaus fallen damit nicht nur solche Dienste in den Anwendungsbereich der Norm, die zum Beispiel über das World Wide Web oder per E-Mail erbracht werden, sondern auch per Voice-over-IP Dienste. Eine Beschränkung des Anwendungsbereichs auf auf technische Weise zugangsbeschränkte Internetplattformen wäre demgegenüber nicht sachgerecht, würde doch gerade derjenige, der solche Dienste offen und für jeden zugänglich feilbietet, insoweit straflos bleiben. Die Dreistigkeit des unverdeckt Handelnden würde damit belohnt werden. Das für die Öffentlichkeit bestehende Gefährdungspotential ist zudem deutlich größer, wenn jedermann unabhängig von seinem technischen Know-how auf eine internetbasierte Zugänglichmachung illegaler Leistungen zugreifen könnte. Zur Abgrenzung der durch den Tatbestand erfassten Angebote von legalen Handelsplattformen, die ohne den Willen der Betreiber für strafrechtlich relevante Zwecke genutzt werden, wird – in Anlehnung an die Formulierung des § 129 StGB – überdies auf den Zweck und die Ausrichtung der Tätigkeit abgestellt. Damit sind Betreiber, deren Angebote ohne entsprechende Zielrichtung zur Förderung von Straftaten genutzt werden, vom Tatbestand ausgenommen. Dies gewährleistet eine Beschränkung schon des Tatbestands auf strafwürdige Online-Angebote. Die Prüfung der Ausrichtung der Plattform hat anhand des konkreten Einzelfalls zu erfolgen und ist allgemein verbindlichen Kriterien nicht zugänglich. Auf Grundlage der bisherigen praktischen Erfahrungen dürften indizielle Bedeutung in diesem Zusammenhang erlangen zum Beispiel das tatsächliche Angebot einer Online-Plattform, der Umgang mit Hinweisen auf Handel mit illegalen Waren und Dienstleistungen und auch die etwa in Allgemeinen Geschäftsbedingungen (AGB) enthaltenen Vorgaben. Schon im Rahmen der Prüfung eines Anfangsverdachts dürften diese Umstände ohne erheblichen Aufwand feststellbar sein.“

ggg) Absatz 13 wie folgt zu fassen:

„Der Grundtatbestand des § 126a Absatz 1 StGB-E ist aufgrund der potentiell erheblichen Gefährdung des Rechtsfriedens mit Geldstrafe oder Freiheitsstrafe von bis zu fünf Jahren bedroht. Der Täter des § 126a StGB-E schafft durch den Betrieb der Plattform Aktionsraum und niedrigschwelligen Zugriff auf Infrastruktur für die Begehung auch schwerer Straftaten durch eine unbestimmte Vielzahl anderer Straftäter und dadurch eine andauernde und ganz erhebliche Gefahr für die öffentliche Sicherheit und Ordnung. Bei erhöhten Strafdrohungen in anderen Tatbeständen, zum Beispiel § 29 Absatz 1 Nummer 10 BtMG, greift die Subsidiaritätsklausel des § 126a Absatz 1 StGB-E. Aus Gründen der Verhältnismäßigkeit begrenzt § 126a Absatz 2 StGB-E die Strafdrohung auf die für die Straftat im Sinne von § 126a Absatz 1 StGB-E angedrohte Strafe. Neben dem Grundtatbestand sieht § 126a Absatz 3 StGB-E bei gewerbsmäßiger oder bandenmäßiger Begehung aufgrund der erhöhten kriminellen Energie eine mit im Mindestmaß erhöhter Strafdrohung bewehrte Qualifikation vor. Die Erfahrungen der Praxis zeigen, dass nicht jede Tathandlung im Sinne des § 126a StGB-E gewerbsmäßig begangen wird, Anbieter stellen Handelsmöglichkeiten auch oft kostenfrei aus ideellen Gründen oder zur Mehrung des eigenen Ansehens in der Szene bereit. Auch bei Tauschbörsen für Schriften mit kinderpornographischen Inhalten fehlt es ferner regelmäßig an einem gewerbsmäßigen Handeln. Das Kriterium der Gewerbsmäßigkeit rechtfertigt daher die in der Qualifikation vorgesehene höhere Strafdrohung.“

- bb) Der Abschnitt „B. Zu den einzelnen Vorschriften“, zu Artikel 1 Nummer 2 ist wie folgt zu fassen:

**„Zu Nummer 2**

Zu § 126a Absatz 1 StGB-E

Die Vorschrift trägt der besonderen Gefährlichkeit des Zugänglichmachens internetbasierter Leistungen Rechnung, die sich ohne zeitliche, sachliche oder räumliche Grenzen an Personen jeden Alters richten. Die Vorschrift ist hinsichtlich ihres sachlichen Anwendungsbereichs weit gefasst, um künftige technische Entwicklungen berücksichtigen zu können,

und erfasst jegliche internetbasierte Zugänglichmachung von Leistungen. Der Begriff „internetbasiert“ ist hierbei technikbezogenen auszulegen und erfasst alle Dienste, die auf der Netzwerkschicht des OSI-Referenzmodells über das Internet-Protokoll (IP) vermittelt werden. Über den allgemeinen Sprachgebrauch zum Begriff „Internet“ hinausgehend fallen damit nicht nur solche Dienste in den Anwendungsbereich der Norm, die zum Beispiel über das World Wide Web oder per E-Mail erbracht werden, sondern beispielsweise auch Voice-over-IP Dienste. Eine Beschränkung des Anwendungsbereichs auf Internetplattformen, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt ist, wäre demgegenüber nicht sachgerecht, würde doch gerade derjenige, der solche Dienste offen und für jeden zugänglich feilbietet, insoweit straflos bleiben. Die Dreistigkeit des unverdeckt Handelnden würde damit belohnt werden. Unter dem Aspekt der Strafwürdigkeit ist die Einschränkung auf das Darknet nicht geboten, da eine etwaige Verschleierung der Täteridentität nichts über das durch die Tat begangene Unrecht aussagt. Das für die Öffentlichkeit bestehende Gefährdungspotential ist zudem deutlich größer, wenn jedermann von überall unabhängig von seinem technischen Know-how auf eine internetbasierte illegale Leistung zugreifen könnte.

Der Begriff der Leistung beschreibt alle Angebote, die sich an einen oder mehrere Nutzer richten, ohne stets auf Dauer und wiederholte Nutzung abzielen. Ein Zugänglichmachen liegt entsprechend der zu § 184 Absatz 1 Nummer 1 StGB entwickelten Grundsätze dann vor, wenn den Nutzern die Möglichkeit der Wahrnehmung der Leistung eröffnet wird. So stellt zum Beispiel der Betrieb eines sogenannten „bulletproof hosters“, der keine eigenen Angebote online stellt, sondern lediglich den Speicherplatz und das Routing für (kriminelle) Dritter anbietet, ein Fall des „Zugänglichmachens“ dar. Zur Abgrenzung der vom Tatbestand erfassten von den nicht strafwürdigen Angeboten ist auf die Ausrichtung des Zwecks oder der Tätigkeit abzustellen. So soll sichergestellt werden, dass ordnungsgemäß eingerichtete Online-Angebote, die entgegen ihrer Zielsetzung auch für den Handel mit illegalen Waren oder Dienstleistungen genutzt werden, nicht der Gefahr strafrechtlicher Verfolgung ausgesetzt werden. Ziel der Zugänglichmachung im Sinne des § 126a Absatz 1 StGB-E muss das Ermöglichen, Fördern oder Erleichtern von rechtswid-

rigen Straftaten sein. Dem steht nicht entgegen, dass auch legale Aktivitäten abgewickelt werden sollen, soweit dies lediglich dem Verschleiern der tatsächlichen Zielrichtung dient. Die Prüfung der Ausrichtung einer Online-Plattform hat anhand des konkreten Einzelfalls zu erfolgen und ist allgemein verbindlichen Kriterien nicht zugänglich. Hierbei kann auf die zu § 202c Absatz 1 Nummer 2 StGB entwickelten Maßstäbe abgestellt werden. Auf Grundlage der bisherigen praktischen Erfahrungen dürften indizielle Bedeutung in diesem Zusammenhang erlangen zum Beispiel das tatsächliche Angebot einer Online-Plattform, der Umgang mit Hinweisen auf Handel mit illegalen Waren und Dienstleistungen und auch die etwa in Allgemeinen Geschäftsbedingungen (AGB) enthaltenen Vorgaben. Schon im Rahmen der Prüfung eines Anfangsverdachts dürften diese Umstände ohne erheblichen Aufwand aufzuklären sein. Stellt die Begehung von Straftaten nur einen Zweck untergeordneter Bedeutung dar, so findet der Tatbestandsausschluss des § 126a Absatz 4 StGB-E Anwendung.

§ 126a StGB-E soll sämtliche rechtswidrige Taten (§ 11 Absatz 1 Nummer 5 StGB) erfassen. Eine Beschränkung auf einzelne Tatbestände birgt die Gefahr der Unvollständigkeit und trägt ferner nicht der Strafwürdigkeit der Zugänglichmachung jedes internetbasierten Angebots Rechnung, das auf die Begehung jeglicher Straftaten gerichtet ist. Die Erfahrungen in der Praxis zeigen, dass Schwerpunkte des illegalen Online-Handels die Bereiche Betäubungsmittel, Waffen, Falschgeld beziehungsweise gefälschte Urkunden, Kinderpornographie und Cyberwerkzeuge, insbesondere Hacker-Programme, sind. Daneben können aber auch Plattformen nicht außen vor bleiben, die zum Beispiel auf die Begehung von Äußerungsdelikten gerichtet sind oder als Dienstleistungen die Begehung von Straftaten gegen die körperliche Unversehrtheit und gegen das Leben vermitteln.

Der größte Anteil der Handelsaktivitäten fällt nach den praktischen Erfahrungen im Bereich der Betäubungsmittel an. Im Bereich gefälschter Urkunden sind besonders Identitätsnachweise zu nennen, die vor allem für betrügerische Bestellungen und die Anlage finanztransaktionsverschleiender Tarnkonten genutzt werden. Abgeschottete Plattformen im Netz sind zudem einer der vorherrschenden Absatz- und Verteilmechanismen kinderpornographischer Schriften, deren Verbreitungsgrad ohne

die dahinterstehenden technischen Infrastrukturen kaum denkbar wäre. Im Bereich der Cyberwerkzeuge werden über Online-Plattformen zum Beispiel Schadsoftwareprogramme angeboten, mit denen Schwachstellen von IT-Systemen ausgenutzt und Sicherungen überwunden werden können. Ebenso wird sogenannte Ransomware, das heißt Software, die Nutzdaten verschlüsselt, um von den Nutzern Zahlungen zur Aufhebung der Verschlüsselung zu erlangen, angeboten. Des Weiteren wird die unmittelbare Durchführung von Cyberangriffen als Dienstleistung offeriert. Hier stehen die sogenannten Botnetze im Fokus, das heißt eine Vielzahl gekaperteter Drittrechner, die unter Täterkontrolle koordinierte Überlastangriffe auf legitime Webseiten und -services durchführen.

Eine Abgrenzung zu den nicht dem Tatbestand unterfallenden legalen Handelsplattformen gelingt über das Tatbestandsmerkmal der Ausrichtung des Zwecks oder der Tätigkeit unter Heranziehung der entwickelten Kriterien zu § 202c Absatz 1 Nummer 2 StGB sowie ferner über eine Anwendung des Tatbestandsausschlusses nach § 126a Absatz 4 Nummer 1 StGB-E. Etwaigen Abgrenzungsproblemen im Bereich der beruflichen Handlungen, insbesondere der in § 53 Absatz 1 Satz 1 Nummer 5 StPO genannten Personen, wird durch die Schutzklausel des § 126a Absatz 4 Nummer 2 StGB-E begegnet.

Zu § 126a Absatz 2 StGB StGB-E

Aus Gründen der Verhältnismäßigkeit begrenzt § 126a Absatz 2 StGB-E die Strafdrohung auf die für die rechtswidrige Tat im Sinne von § 126a Absatz 1 StGB-E angedrohte Strafe. Dieses Vorgehen orientiert sich an den Regelungen in vergleichbaren Vorschriften, zum Beispiel §§ 202d Absatz 2, 257 Absatz 2, 258 Absatz 3 StGB.

Zu § 126a Absatz 3 StGB StGB-E

Neben dem Grundtatbestand sieht § 126a Absatz 3 StGB-E für Täter, welche die Tat nach § 126a Absatz 1 StGB-E gewerbsmäßig oder als Mitglied einer Bande begehen, die sich zur fortgesetzten Begehung von Straftaten im Sinne von § 126a Absatz 1 StGB-E verbunden hat, aufgrund der erhöhten kriminellen Energie eine mit im Mindestmaß erhöhter Strafdrohung bewehrte Qualifikation vor. Aufgrund des bestehenden Organisationsaufwands der Betreiber wird die Intention der Betreiber nicht selten auf eine Gewinnerzielung ausgerichtet sein. Die Erfahrung

gen der Praxis zeigen, dass nicht jede Tathandlung im Sinne des § 126a StGB-E gewerbsmäßig begangen wird, Anbieter stellen Handelsmöglichkeiten auch oft kostenfrei aus ideellen Gründen oder zur Mehrung des eigenen Ansehens in der Szene bereit. Auch bei Tauschbörsen für Schriften mit kinderpornographischen Inhalten fehlt es ferner regelmäßig an einem gewerbsmäßigen Handeln. Das Kriterium der Gewerbsmäßigkeit rechtfertigt daher die vorgesehene höhere Strafdrohung, die zudem verdeutlicht, dass die Qualifikation des § 126a Absatz 3 StGB-E dem Bereich der besonders schweren Kriminalität zuzurechnen ist.

Der Strafraum orientiert sich auf Grundlage der erhöhten kriminellen Energie von auf Dauer angelegten, gewinnorientierten Strukturen an denen für vergleichbare Delikte bei gewerbsmäßiger oder bandenmäßiger Begehungsweise, zum Beispiel § 260 Absatz 1 Nummer 1 und 2 StGB (Hehlerei), § 263 Absatz 3 Satz 2 Nummer 1 StGB (Betrug) – auch in Verbindung mit § 263a Absatz 2 StGB (Computerbetrug) –, § 267 Absatz 3 Satz 2 Nummer 1 StGB (Urkundenfälschung) und § 303b Absatz 4 Satz 2 Nummer 2 StGB (Computersabotage). Das Delikt ist, anders als einige der vorgenannten Beispiele, als Qualifikation ausgestaltet, um dem Umstand Rechnung zu tragen, dass Online-Plattformen für illegale Waren und Dienstleistungen den Nährboden weiter Bereiche des Cybercrime darstellen. Die Bedeutung der Plattformen entspricht dabei der vergleichbarer Einrichtungen im legalen Bereich. Der Unternehmensgegenstand zahlreicher, auch international erfolgreicher Unternehmen besteht im Unterhalt einer Infrastruktur für den örtlich und zeitlich ungebundenen Austausch von Waren und Dienstleistungen. Ebenso stellen sich Funktion und Bedeutung der illegalen Plattformen dar, denen eine erhebliche Ausstrahlung im Bereich des Cybercrime zukommt.

Zu § 126a Absatz 4 StGB StGB-E

§ 126a Absatz 4 Nummer 1 StGB-E sieht einen Tatbestandsausschluss für die Fälle vor, in denen die Begehung von Straftaten nur einen Zweck oder eine Tätigkeit von untergeordneter Bedeutung darstellt. Die Vorschrift stellt damit klar, dass insbesondere Leistungen von legalen Handelsplattformen, die von Dritten für strafrechtlich relevante Zwecke genutzt werden, nicht unter § 126a Absatz 1 StGB-E fallen. Im Übrigen können die in der Rechtsprechung zu § 129 Absatz 3 Nummer 2 StGB entwickelten Abgrenzungskriterien herangezogen werden. § 126a Absatz 4 Nummer 2

StGB-E nimmt entsprechend zu § 202d Absatz 3 Satz 2 Nummer 2 StGB aus Gründen der Verhältnismäßigkeit und zum Schutze bestimmter Berufsgruppen solche Handlungen von der Strafbarkeit aus, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Hierzu zählen insbesondere berufliche Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 StPO genannten Personen.“

Begründung (nur gegenüber dem Plenum):

a) Die Problemanalyse des Gesetzentwurfs ist weitestgehend zutreffend und die Forderung nach einem eigenen Straftatbestand für den Betrieb krimineller Infrastrukturen zu unterstützen. Zu befürworten ist insbesondere, dass ein Straftatbestand im Kernstrafrecht geschaffen werden soll. Dies ist einer Lösung über Anpassungen spezialgesetzlicher Regelungen unter anderem im Waffen-, Betäubungsmittel- und Sprengstoffrecht vorzuziehen, da die Waren- und insbesondere auch Dienstleistungsangebote, die auf kriminellen Internetplattformen gehandelt werden, oft so breitgefächert sind, dass eine Regelung in den entsprechenden Spezialgesetzen immer Gefahr läuft, unübersichtlich zu geraten und unvollständig zu bleiben.

b) Zu § 126a Absatz 1 StGB-E:

aa) Zu Buchstabe a und b Doppelbuchstabe aa Dreifachbuchstabe aaa (Zugänglichmachen)

Der Begriff des „Anbietens“ im ersten Satz des § 126a StGB-E soll durch die weitergehende, bereits in § 184 Absatz 1 Nummer 1 StGB bewährte Formulierung des „Zugänglichmachens“ ersetzt werden. Im Gegensatz zum Begriff des „Anbietens“ erfasst die Tatbestandshandlung des „Zugänglichmachens“ strafwürdige Leistungen technischer Dienstleister in der Underground Economy umfassender. So stellt zum Beispiel der Betrieb eines sogenannten „bulletproof hosters“, der keine eigenen Angebote online stellt, sondern lediglich den Speicherplatz und das Routing für (kriminelle) Dritter zur Verfügung stellt, ein Fall des „Zugänglichmachens“ dar.

bb) Zu Buchstabe b Doppelbuchstabe aa Dreifachbuchstabe ddd (Erleichtern von Straftaten)

Eine Beschränkung der Vorschrift auf die „Ermöglichung oder Förderung“ von rechtswidrigen Taten überzeugt nicht. Zu bedenken ist, dass die ständige Rechtsprechung im Rahmen der Beihilfe als „Hilfeleistung“ im Sinne des § 27 StGB grundsätzlich jede Handlung ausreichen lässt, die die Herbeiführung des Taterfolges „objektiv fördert oder erleichtert“. „Die Ermöglichung des Taterfolgs“ dürfte restriktiver zu verstehen sein als ein „Erleichtern des Taterfolgs“. Um an dieser Stelle unnötige Abgrenzungsschwierigkeiten für die Praxis zu vermeiden, sollte das „Erleichtern von Straftaten“ als weitere Tathandlungsalternative eingefügt werden.

cc) Zu Buchstabe b Doppelbuchstabe aa Dreifachbuchstabe ccc, Doppelbuchstabe bb und Buchstabe c  
(Straftatenkatalog)

Die bisher in § 126a Absatz 1 Satz 2 StGB-E vorgesehene Einschränkung der Anwendbarkeit durch einen Strafkatalog sollte gestrichen werden. Zum einen läuft dieser Gefahr, unvollständig zu bleiben. So umfasst dieser vorliegend weder die Urkundendelikte noch Dienstleistungen in Form von Straftaten gegen die körperliche Unversehrtheit oder gegen das Leben. Ferner ist auch die Auswahl der Katalogtaten nicht sachgerecht. Insbesondere erfolgt eine Aufnahme von § 263a StGB, nicht jedoch von § 263 StGB. Zum anderen ist die Zugänglichmachung jedes internetbasierten Angebots, das auf die Begehung jeglicher Straftaten gerichtet ist, strafwürdig. Dies gilt zum Beispiel auch für Plattformen, welche auf die Begehung von Äußerungsdelikten oder Volksverhetzung gerichtet sind. Gegen die Einfügung eines Straftatenkatalogs spricht schließlich auch in systematischer Hinsicht ein Vergleich mit § 111 StGB, der das öffentliche Auffordern zu jeglicher rechtswidriger Tat als strafbar erklärt.

dd) Zu Buchstabe b Doppelbuchstabe aa Dreifachbuchstabe bbb  
(Zugangsbeschränkung)

Ferner erscheint die Einschränkung, wonach der Betrieb krimineller Cyberstrukturen nur dann strafbar sein soll, wenn der Zugang zu diesen Leistungen „durch besondere technische Vorkehrungen beschränkt ist“, nicht sachgerecht. Zwar ist es zutreffend, dass das damit umschriebene Darknet ein attraktiver Ort für Anbieter krimineller Internetplattformen sein wird. Nichts desto trotz erscheint es nicht sachgerecht, wenn sich ausschließlich nur derjenige strafbar macht, der kriminelle Dienste auf zugangsbeschränkten Internetplattformen anbietet und demgegenüber derjenige, der solche Dienste offen und für jeden zugänglich feilbietet, insoweit straflos bliebe. Im letztgenannten Fall würde dies zum einen die Dreistigkeit des unverdeckt Handelnden belohnen. Zum anderen ist das Gefährdungspotenzial für die Öffentlichkeit größer, wenn jedermann unabhängig von seinem technischen Know-how auf eine derartige internetbasierte Zugänglichmachung illegaler Leistungen zugreifen könnte.

Schließlich ist das Tatbestandsmerkmal der „Beschränkung durch besondere technische Vorrichtungen“ in erheblichem Umfang auslegungsbedürftig, so dass eine Vorhersehbarkeit strafbaren Verhaltens für den Normadressaten kaum gegeben ist. Dies zeigt sich schon daran, dass ein Teil der in der Entwurfsbegründung aufgeführten Plattformen, wie etwa „crimenetwork.biz“, nicht im Darknet, sondern im sogenannten Surface Web betrieben wurden und nur dann von § 126a StGB-E erfasst wären, wenn bereits handelsübliche Webbrowser (zum Beispiel Firefox, Internet Explorer) als „besondere technische Vorkehrungen“ aufzufassen wären. Ausweislich der Gesetzesbegründung, die auf Darknet-Angebote abstellt, soll dies nicht intendiert sein.

ee) Zu Buchstabe b Doppelbuchstabe aa Dreifachbuchstabe eee (Strafrahmen)

Anstelle der Beschränkung des Strafrahmens des Grundtatbestandes auf Freiheitsstrafe bis zu drei Jahren oder Geldstrafe ist ein Strafrahmen von Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe sachgerecht. Der Täter des § 126a StGB-E schafft durch den Betrieb der Plattform Aktionsraum und niedrigschwelligen Zugriff auf Infrastruktur für die Begehung auch schwerer Straftaten durch eine unbestimmte Vielzahl anderer Straftäter und dadurch eine andauernde und ganz erhebliche Gefahr für die öffentliche Sicherheit und Ordnung. Dem Grundsatz der Verhältnismäßigkeit trägt bereits jetzt die Beschränkung in § 126a Absatz 2 StGB-E Rechnung.

c) Zu Buchstabe d (§ 126a Absatz 3 StGB-E)

Die Qualifikation des § 126a Absatz 3 StGB-E ist um den Fall der bandenmäßigen Tatbegehung zu erweitern. Auch bei einer bandenmäßigen Begehung sollte wegen der ihr innewohnenden Dynamik und des zusätzlichen Organisationsunrechts, die eine erhöhte Gefährlichkeit begründen, der Strafrahmen eine Freiheitsstrafe von sechs Monaten bis zu zehn Jahren vorsehen. Trotz der amorphen Organisationsstruktur in der einschlägigen Szene erscheint eine Begehungsweise, die das Tatbestandsmerkmal der bandenmäßigen Begehung erfüllt, nicht ausgeschlossen, weshalb die Qualifikation auch dies erfassen soll.

d) Zu Buchstabe e (§ 126a Absatz 4 StGB-E)

§ 126a StGB-E ist aus Gründen der Verhältnismäßigkeit um einen neuen Absatz 4 zu ergänzen, der einen Tatbestandsausschluss erstens für diejenigen Fälle vorsieht, in denen die Begehung von Straftaten nur einen Zweck oder eine Tätigkeit von untergeordneter Bedeutung darstellt. Hiermit soll in Anlehnung an § 129 Absatz 3 Nummer 2 StGB klargestellt werden, dass grundsätzlich legale Internetportale von § 126a Absatz 1 StGB-E nicht erfasst sind. Zweitens normiert Absatz 4 in Anlehnung an § 202d Absatz 3 Satz 2 Nummer 2 StGB zum Schutz bestimmter Berufsgruppen einen Tatbestandsausschluss für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen.

R,  
In

2. Zu Artikel 1 Nummer 1a – neu – (§ 5 Nummer 10b – neu – StGB)

In Artikel 1 ist nach Nummer 1 folgende Nummer 1a einzufügen:

(setzt  
Annahme  
von  
Ziffer 1  
voraus)

,1a. In § 5 wird nach Nummer 10a folgende Nummer 10b eingefügt:

„10b. Zugänglichmachen von Leistungen zur Begehung von Straftaten (§ 126a StGB), wenn sich die zugänglich gemachte internetbasierte Leistung auf die Ermöglichung, Förderung oder Erleichterung von rechtswidrigen Taten im Inland bezieht.“ ‘

Folgeänderungen:

- a) Im Vorblatt ist dem Abschnitt „B. Lösung“ folgender Satz anzufügen:

„Daneben erfolgt eine Aufnahme des Straftatbestands in § 5 StGB, um auch Handlungen aus dem Ausland zu erfassen, die einen besonderen Inlandsbezug dadurch aufweisen, dass sie sich auf die Ermöglichung, Förderung oder Erleichterung von rechtswidrigen Taten im Inland beziehen.“

- b) Die Begründung ist wie folgt zu ändern:

- aa) Im Abschnitt „A. Allgemeines“ ist im Abschnitt „I. Zielsetzung und wesentlicher Inhalt des Gesetzesentwurfs“ nach Absatz 8 folgender Absatz 8a einzufügen:

„Da eine Vielzahl von Tätern ferner aus dem Ausland agiert, um ihr Entdeckungs- und Ergreifungsrisiko zusätzlich zu minimieren und um rechtswidrige Taten im Inland zu ermöglichen, lassen sich die Ermittlungen zumeist nicht auf das Inland begrenzen. So wurden beispielsweise ausweislich des Berichts der Bundesregierung über die im Jahr 2017 ergriffenen Maßnahmen zum Zweck der Löschung von Telemedizinangeboten mit kinderpornografischen Inhalten im Sinne des § 184b StGB 84 Prozent der dem Bundeskriminalamt im Jahr 2017 gemeldeten Internetseiten mit kinderpornographischen Inhalten im Ausland gehostet.“

- bb) Im Abschnitt „B. Zu den einzelnen Vorschriften“ ist nach dem Abschnitt zu Artikel 1 Nummer 1 folgender Text einzufügen:

**„Zu Nummer 1a (§ 5 Nummer 10b StGB-E)**

Die Erweiterung des Straftatenkatalogs des § 5 StGB soll den Schutz der öffentlichen Sicherheit und Ordnung vor internetbasierten Leistungsangeboten in den Fällen gewährleisten, in denen die Leistung des Portalbetreibers zwar im Ausland angeboten wird, diese aber einen besonderen Inlandsbezug dadurch aufweist, dass sie sich auf die Ermöglichung, Förderung oder Erleichterung von rechtswidrigen Taten im Inland bezieht. Denn nach der neueren Rechtsprechung des Bundesgerichtshofes zu § 86 StGB und § 130 Absatz 1 bis 3 StGB findet das deutsche Strafrecht nicht gemäß § 3 StGB in Verbindung mit § 9 Absatz 1 StGB auf Handlungen eines Täters im Ausland Anwendung, wenn es sich – wie bei § 126a StGB-E – um ein abstraktes Gefähr-

dungsdelikt handelt, das keinen zum Tatbestand gehörenden Erfolg beschreibt (vgl. BGH, Beschluss vom 19. August 2014, 3 StR 88/14; Beschluss vom 3. Mai 2016, 3 StR 449/15).

Es verdichtet sich bei § 126a StGB-E die Gefahr einer Verletzung des Schutzes der öffentlichen Sicherheit und Ordnung bei internetbezogenen Angeboten, die sich auf die Ermöglichung, Förderung oder Erleichterung von rechtswidrigen Taten im Inland beziehen. § 126a StGB-E findet demnach beispielsweise über § 5 StGB dann Anwendung, wenn sich die Server eines Internetplattformbetreibers zwar im Ausland befinden, mittels der Plattform jedoch – zum Beispiel durch an Inländer gerichtete Angebote von Betäubungsmitteln, Waffen oder Kinderpornographie – die Begehung von Straftaten im Inland ermöglicht wird. Ohne Erweiterung des § 5 StGB bestünde die Gefahr, dass derartige im Ausland begangene Handlungen trotz ihres Bezugs zur öffentlichen Sicherheit und Ordnung im Inland nicht vom deutschen Strafrecht erfasst würden – insbesondere wenn sie im Ausland nicht strafbar sind – und daher möglicherweise bewusst im Ausland vorgenommen würden – beispielsweise durch das gezielte Betreiben von Servern im Ausland -, um einer Strafbarkeit nach deutschem Recht zu entgehen. Die Regelung dient daher vor allem dazu, entsprechenden, im Cyberbereich durch technische Möglichkeiten besonders erleichterten Umgehungsversuchen von vornherein entgegenzuwirken.

Begründung (nur gegenüber dem Plenum):

Die Problemanalyse des Gesetzentwurfs ist weitestgehend zutreffend, lässt jedoch außer Betracht, dass sich der Serverstandort einer nicht unerheblichen Anzahl an Internetportalen, über die rechtswidrige Taten im Inland ermöglicht werden, im Ausland befindet. So wurden beispielsweise ausweislich des Berichts der Bundesregierung über die im Jahr 2017 ergriffenen Maßnahmen zum Zweck der Löschung von Telemedienangeboten mit kinderpornografischen Inhalten im Sinne des § 184b StGB 84 Prozent der dem Bundeskriminalamt im Jahr 2017 gemeldeten Internetseiten mit kinderpornografischen Inhalten im Ausland gehostet.

Da nach der Rechtsprechung des Bundesgerichtshofes zu § 86 StGB und § 130 Absatz 1 bis 3 StGB das deutsche Strafrecht nicht gemäß § 3 in Verbindung mit § 9 Absatz 1 StGB auf Handlungen eines Täters im Ausland Anwendung findet, wenn es sich – wie bei § 126a StGB-E – um ein abstraktes Gefährdungsdelikt handelt, das keinen zum Tatbestand gehörenden Erfolg beschreibt (vgl. BGH, Beschluss vom 19. August 2014, 3 StR 88/14; Beschluss vom

3. Mai 2016, 3 StR 449/15), ist eine Aufnahme des § 126a StGB-E in § 5 StGB zwingend notwendig, um – im Cyberbereich durch technische Möglichkeiten besonders erleichterten – Umgehungsversuchen von vornherein entgegenzuwirken. Die Erweiterung des Straftatenkatalog des § 5 StGB soll den Schutz der öffentlichen Sicherheit und Ordnung vor internetbasierten Leistungsangeboten in den Fällen gewährleisten, in denen die Leistung des Portalbetreibers zwar im Ausland angeboten wird, diese aber einen besonderen Inlandsbezug dadurch aufweist, dass sie sich auf die Ermöglichung, Förderung oder Erleichterung von rechtswidrigen Taten im Inland bezieht. Es verdichtet sich bei § 126a StGB-E die Gefahr einer Verletzung des Schutzes der öffentlichen Sicherheit und Ordnung in den Fällen, in denen die Leistung des Portalbetreibers zwar im Ausland angeboten wird, diese aber einen besonderen Inlandsbezug dadurch aufweist, dass sie sich auf die Ermöglichung, Förderung oder Erleichterung von rechtswidrigen Taten im Inland bezieht.

- R 3. Zu Artikel 1 Nummer 1a – neu – (§ 5 Nummer 10b – neu – StGB)<sup>\*</sup>  
 (entfällt bei Annahme von Ziffer 1)  
 In Artikel 1 ist nach Nummer 1 folgende Nummer 1a einzufügen:  
 ,1a. In § 5 wird nach Nummer 10a folgende Nummer 10b eingefügt:  
 „10b. Anbieten von Leistungen zur Ermöglichung von Straftaten (§ 126a StGB), wenn sich die angebotene internetbasierte Leistung auf die Ermöglichung von rechtswidrigen Taten im Inland bezieht;“ ‘

Folgeänderungen:

- a) Im Vorblatt ist dem Abschnitt „B. Lösung“ folgender Satz anzufügen:  
 „Daneben erfolgt eine Aufnahme des Straftatbestands in § 5 StGB, um auch Handlungen aus dem Ausland zu erfassen, die einen besonderen Inlandsbezug dadurch aufweisen, dass sie sich auf die Ermöglichung von rechtswidrigen Taten im Inland beziehen.“
- b) Die Begründung ist wie folgt zu ändern:  
 aa) Im Abschnitt „A. Allgemeines“ ist im Abschnitt „I. Zielsetzung und wesentlicher Inhalt des Gesetzesentwurfs“ nach Absatz 8 folgender Absatz 8a einzufügen:  
 „Da eine Vielzahl von Tätern ferner aus dem Ausland agiert, um ihr

---

\* Im Rechtsausschuss als Hilfsempfehlung zu Ziffer 1 beschlossen.

Entdeckungs- und Ergreifungsrisiko zusätzlich zu minimieren und um rechtswidrige Taten im Inland zu ermöglichen, lassen sich die Ermittlungen zumeist nicht auf das Inland begrenzen. So wurden beispielsweise ausweislich des Berichts der Bundesregierung über die im Jahr 2017 ergriffenen Maßnahmen zum Zweck der Löschung von Telemedizinangeboten mit kinderpornografischen Inhalten im Sinne des § 184b StGB 84 Prozent der dem Bundeskriminalamt im Jahr 2017 gemeldeten Internetseiten mit kinderpornographischen Inhalten im Ausland gehostet.“

bb) Im Abschnitt „B. Zu den einzelnen Vorschriften“ ist nach dem Abschnitt zu Artikel 1 Nummer 1 folgender Text einzufügen:

**„Zu Nummer 1a ( § 5 Nummer 10b StGB-E)**

Die Erweiterung des Straftatenkatalogs des § 5 StGB soll den Schutz der öffentlichen Sicherheit und Ordnung vor internetbasierten Leistungsangeboten in den Fällen gewährleisten, in denen die Leistung des Portalbetreibers zwar im Ausland angeboten wird, diese aber einen besonderen Inlandsbezug dadurch aufweist, dass sie sich auf die Ermöglichung von rechtswidrigen Taten im Inland bezieht. Denn nach der neueren Rechtsprechung des Bundesgerichtshofes zu § 86 StGB und § 130 Absatz 1 bis 3 StGB findet das deutsche Strafrecht nicht gemäß § 3 StGB in Verbindung mit § 9 Absatz 1 StGB auf Handlungen eines Täters im Ausland Anwendung, wenn es sich – wie bei § 126a StGB-E – um ein abstraktes Gefährdungsdelikt handelt, das keinen zum Tatbestand gehörenden Erfolg beschreibt (vgl. BGH, Beschluss vom 19. August 2014, 3 StR 88/14; Beschluss vom 3. Mai 2016, 3 StR 449/15).

Es verdichtet sich bei § 126a StGB-E die Gefahr einer Verletzung des Schutzes der öffentlichen Sicherheit und Ordnung bei internetbezogenen Angeboten, die sich auf die Ermöglichung von rechtswidrigen Taten im Inland beziehen. § 126a StGB-E findet demnach beispielsweise über § 5 StGB dann Anwendung, wenn sich die Server eines Internetplattformbetreibers zwar im Ausland befinden, mittels der Plattform jedoch – zum Beispiel durch an Inländer gerichtete Angebote von Betäubungsmitteln, Waffen oder Kinderpornographie – die Begehung von Straftaten im Inland ermöglicht wird. Ohne Erweiterung des § 5 StGB

bestünde die Gefahr, dass derartige im Ausland begangene Handlungen trotz ihres Bezugs zur öffentlichen Sicherheit und Ordnung im Inland nicht vom deutschen Strafrecht erfasst würden – insbesondere wenn sie im Ausland nicht strafbar sind – und daher möglicherweise bewusst im Ausland vorgenommen würden – beispielsweise durch das gezielte Betreiben von Servern im Ausland –, um einer Strafbarkeit nach deutschem Recht zu entgehen. Die Regelung dient daher vor allem dazu, entsprechenden, im Cyberbereich durch technische Möglichkeiten besonders erleichterten Umgehungsversuchen von vornherein entgegenzuwirken.“

Begründung (nur gegenüber dem Plenum):

Die Problemanalyse des Gesetzentwurfs ist weitestgehend zutreffend, lässt jedoch außer Betracht, dass sich der Serverstandort einer nicht unerheblichen Anzahl an Internetportalen, über die rechtswidrige Taten im Inland ermöglicht werden, im Ausland befindet. So wurden beispielsweise ausweislich des Berichts der Bundesregierung über die im Jahr 2017 ergriffenen Maßnahmen zum Zweck der Löschung von Telemedienangeboten mit kinderpornografischen Inhalten im Sinne des § 184b StGB 84 Prozent der dem Bundeskriminalamt im Jahr 2017 gemeldeten Internetseiten mit kinderpornografischen Inhalten im Ausland gehostet.

Da nach der Rechtsprechung des Bundesgerichtshofes zu § 86 StGB und § 130 Absatz 1 bis 3 StGB das deutsche Strafrecht nicht gemäß § 3 in Verbindung mit § 9 Absatz 1 StGB auf Handlungen eines Täters im Ausland Anwendung findet, wenn es sich – wie bei § 126a StGB-E – um ein abstraktes Gefährdungsdelikt handelt, das keinen zum Tatbestand gehörenden Erfolg beschreibt (BGH, Beschluss vom 19. August 2014, 3 StR 88/14; Beschluss vom 3. Mai 2016, 3 StR 449/15), ist eine Aufnahme des § 126a StGB-E in § 5 StGB zwingend notwendig, um – im Cyberbereich durch technische Möglichkeiten besonders erleichterten – Umgehungsversuchen von vornherein entgegenzuwirken. Die Erweiterung des Straftatenkatalog des § 5 StGB soll den Schutz der öffentlichen Sicherheit und Ordnung vor internetbasierten Leistungsangeboten in den Fällen gewährleisten, in denen die Leistung des Portalbetreibers zwar im Ausland angeboten wird, diese aber einen besonderen Inlandsbezug dadurch aufweist, dass sie sich auf die Ermöglichung von rechtswidrigen Taten im Inland bezieht. Es verdichtet sich bei § 126a StGB-E die Gefahr einer Verletzung des Schutzes der öffentlichen Sicherheit und Ordnung in den Fällen, in denen die Leistung des Portalbetreibers zwar im Ausland angeboten wird, diese aber einen besonderen Inlandsbezug dadurch aufweist, dass sie sich auf die Ermöglichung von rechtswidrigen Taten im Inland bezieht.

- In 4. Zu Artikel 2 Nummer 1 (§ 99 Absatz 2 – neu – StPO),  
(bei Nummer 2 (§ 100a Absatz 2 Nummer 1 Buchstabe d StPO),  
Annahme Nummer 3 (§ 100b Absatz 2 Nummer 1 Buchstabe b StPO),  
entfällt Nummer 4 (§ 100g Absatz 2 Satz 2 Nummer 1 Buchstabe b StPO)  
Ziffer 5)

Artikel 2 ist wie folgt zu fassen:

## **,Artikel 2**

### **Änderung der Strafprozessordnung**

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. § 99 wird wie folgt geändert:
  - a) Dem bisherigen Wortlaut wird die Absatzbezeichnung „(1)“ vorangestellt.
  - b) Folgender Absatz wird angefügt:

„(2) Statt einer Beschlagnahme kann der Richter, unter den Voraussetzungen des § 100 auch der Staatsanwalt, von Personen oder Unternehmen, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen, Auskunft über die in Absatz 1 genannten Sendungen verlangen, die vom Beschuldigten herrühren oder für ihn bestimmt sind. Die Auskunft wird auch über solche Sendungen erteilt, die sich bei Eingang des Ersuchens nicht mehr oder noch nicht im Machtbereich der Person oder des Unternehmens befinden.“
2. § 100a Absatz 2 Nummer 1 Buchstabe d wird wie folgt gefasst:

„d) Straftaten gegen die öffentliche Ordnung nach § 126a Absatz 1, soweit die rechtswidrige Tat eine Katalogtat im Sinne dieser Vorschrift darstellt, und nach §§ 126a Absatz 3, 129 bis 130,“.
3. § 100b Absatz 2 Nummer 1 Buchstabe b wird wie folgt gefasst:

„b) Straftaten gegen die öffentliche Ordnung nach § 126a Absatz 1, soweit die rechtswidrige Tat eine Katalogtat im Sinne dieser Vorschrift darstellt, und nach § 126a Absatz 3, § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und § 129a Absatz 1, 2, 4, 5 Satz 1 Alternative 1, jeweils auch in Verbindung mit § 129b Absatz 1,“.

4. § 100g Absatz 2 Satz 2 Nummer 1 Buchstabe b wird wie folgt gefasst:

„b) besonders schwerer Fall des Landfriedensbruchs nach § 125a sowie Straftaten gegen die öffentliche Ordnung nach § 126a Absatz 1, soweit die rechtswidrige Tat eine Katalogtat im Sinne dieser Vorschrift darstellt, und nach § 126a Absatz 3, § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und § 129a Absatz 1, 2, 4, 5 Satz 1 Alternative 1, jeweils auch in Verbindung mit § 129b Absatz 1,“ ‘

Folgeänderungen:

a) Das Vorblatt ist wie folgt zu ändern:

aa) Der Abschnitt „A. Problem und Ziel“ ist wie folgt zu ändern:

aaa) Nach Absatz 5 sind folgende Absätze einzufügen:

„Die strafrechtliche Bekämpfung des Handels mit illegalen Gütern im Internet steht ferner vor dem Problem, dass die Betreiber und Nutzer der Handelsplattformen zunehmend die Möglichkeiten der Anonymisierung nutzen, die ihnen das Internet bietet, und daher oftmals nicht oder nur schwer identifiziert werden können. Zwar gibt es durchaus erfolgsversprechende Ermittlungsansätze zur Identifizierung der Tatverdächtigen, namentlich die Daten, die bei der internetbasierten Kommunikation der Tatverdächtigen anfallen oder auf den von den ihnen genutzten informationstechnischen Systemen gespeichert sind. Jedoch können die Strafverfolgungsbehörden auf diese Daten häufig trotz Bestehens eines Anfangsverdachts mangels entsprechender Befugnisnormen nicht zugreifen.

Zur Identifizierung der Tatverdächtigen, die über die entsprechenden Plattformen ihre kriminellen Geschäfte abwickeln, ergeben sich am Übergang von der digitalen in die analoge Welt erfolgsversprechende Ermittlungsansätze, nämlich aus den Daten, die bei der Aufgabe und Annahme entsprechender Warensendungen von den Postdienstleistern festgehalten werden. Jedoch können die Strafverfolgungsbehörden nach dem Beschluss eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) mangels Rechtsgrundlage dann keine Auskunft über diese Daten von den Postdienstleistern ver-

langen, wenn die Sendung bereits ausgeliefert ist und sich damit nicht mehr im Gewahrsam des Postdienstleisters befindet (sogenannte retrograde Auskunftsverlangen). Ähnliches dürfte – wie der Ermittlungsrichter in dem vorgenannten Beschluss anmerkt – auch für Postsendungen gelten, die sich noch nicht im Gewahrsam des Postdienstleisters befinden. Die entsprechende Gesetzeslücke zu schließen, sei Aufgabe des Gesetzgebers.“

bbb) Absatz 6 ist wie folgt zu ändern:

aaaa) In Satz 1 sind die Wörter „mit der Effektivität strafrechtlicher Ermittlungen im Darknet“ durch die Wörter „und am 21. und 22. Juni 2017 in Deidesheim mit den geschilderten Problemlagen“ zu ersetzen.

bbbb) Folgender Satz ist anzufügen:

„Ferner haben sie die Bundesregierung gebeten, sich für eine klarstellende gesetzliche Regelung einzusetzen, die es den Strafverfolgungsbehörden ausdrücklich ermöglicht, von Postdienstleistern Auskünfte auch über noch nicht ein- sowie bereits ausgelieferte Sendungen zu verlangen.“

bb) Der Abschnitt „B. Lösung“ ist wie folgt zu ändern:

aaa) Satz 4 ist wie folgt zu fassen:

„Ferner sollen für die Qualifikation sowie diejenigen Fälle des Grundtatbestandes, in denen es sich bei der rechtswidrigen Tat um eine "schwere" beziehungsweise "besonders schwere" Straftat handelt, die Ermittlungsmaßnahmen gemäß §§ 100a, 100b und 100g StPO eröffnet sein.“

bbb) Folgender Satz ist anzufügen:

„Schließlich schafft der Gesetzentwurf zur Klarstellung eine gesetzliche Regelung, die es Strafverfolgungsbehörden ausdrücklich ermöglicht, von Postdienstleistern Auskünfte auch über noch nicht ein- sowie bereits ausgelieferte Sendungen zu verlangen.“

cc) Der Unterabschnitt „E.2 Erfüllungsaufwand für die Wirtschaft“ ist wie folgt zu fassen:

„E.2 Erfüllungsaufwand für die Wirtschaft

Der Aufwand, der für die Postunternehmen durch die Auskunftsverlangen über noch nicht ein- sowie bereits ausgelieferte Sendungen zu erwarten ist, kann nicht beziffert werden.“

b) Die Begründung ist wie folgt zu ändern:

aa) Im Abschnitt „A. Allgemeines“ ist Abschnitt I wie folgt zu ändern:

aaa) Nach Absatz 8 sind folgende Absätze 8a und 8b einzufügen:

„Die strafrechtliche Bekämpfung des Handels mit illegalen Gütern im Internet steht ferner vor dem Problem, dass die Betreiber und Nutzer der Handelsplattformen zunehmend die Möglichkeiten der Anonymisierung nutzen, die ihnen das Internet bietet, und daher oftmals nicht oder nur schwer identifiziert werden können. Zwar gibt es durchaus erfolgversprechende Ermittlungsansätze zur Identifizierung der Tatverdächtigen, namentlich die Daten, die bei der internetbasierten Kommunikation der Tatverdächtigen anfallen oder auf den von ihnen genutzten informationstechnischen Systemen gespeichert sind. Jedoch können die Strafverfolgungsbehörden auf diese Daten häufig trotz Bestehens eines Anfangsverdachts mangels entsprechender Befugnisnormen nicht zugreifen.

Zur Identifizierung der Tatverdächtigen, die über die entsprechenden Plattformen ihre kriminellen Geschäfte abwickeln, ergeben sich am Übergang von der digitalen in die analoge Welt erfolgversprechende Ermittlungsansätze, nämlich aus den Daten, die bei der Aufgabe und Annahme entsprechender Warensendungen von den Postdienstleistern festgehalten werden. Jedoch können die Strafverfolgungsbehörden nach dem Beschluss eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) mangels Rechtsgrundlage dann keine Auskunft über diese Daten von den Postdienstleistern verlangen, wenn die Sendung bereits ausgeliefert ist und sich damit nicht mehr im Gewahrsam des Postdienstleisters befindet (so genannte

retrograde Auskunftsverlangen). Ähnliches dürfte – wie der Ermittlungsrichter in dem vorgenannten Beschluss anmerkt – auch für Postsendungen gelten, die sich noch nicht im Gewahrsam des Postdienstleisters befinden. Die entsprechende Gesetzeslücke zu schließen, sei Aufgabe des Gesetzgebers.“

bbb) Absatz 14 ist durch folgende Absätze zu ersetzen:

„Die erhöhte Strafandrohung verdeutlicht überdies, dass die Qualifikation des § 126a Absatz 3 StGB-E dem Bereich der besonders schweren Kriminalität zuzurechnen sind. Dies begründet in Verbindung mit den Besonderheiten der Tatbegehung mittels internetbasierter Leistung die Aufnahme des Qualifikationstatbestands in den Katalog der Ermittlungsmaßnahmen der §§ 100a Absatz 2 Nummer 1 Buchstabe d, 100b Absatz 2 Nummer 1 Buchstabe b, 100g Absatz 2 Satz 2 Nummer 1 Buchstabe b StPO. Diese Ermittlungsmaßnahmen sind zur effektiven Verfolgung der Straftaten gemäß § 126a StGB-E zwingend erforderlich. Den von § 126a StGB-E erfassten Lebenssachverhalten ist es immanent, dass die Begehung der Tat in den allermeisten Fällen ausschließlich in der digitalen Welt erfolgt – mit der Folge, dass der Täter nahezu ausschließlich Spuren in dieser digitalen Welt hinterlässt, die als Ermittlungsansätze und Tatnachweis dienen können. Diesen Gegebenheiten müssen die Ermittlungsbefugnisse Rechnung tragen. § 126a Absatz 3 StGB-E fügt sich hinsichtlich seines Schweregrades nicht nur in den Straftatenkatalog des § 100a Absatz 2 Nummer 1 StPO, sondern auch in die Straftatenkataloge der §§ 100b Absatz 2, 100g Absatz 2 StPO ein, die Straftaten gegen die öffentliche Ordnung mit Freiheitsstrafe von mehr als fünf Jahren im Höchstmaß in Nummer 1 Buchstabe b bereits jeweils erfassen.

Daneben ist auch eine Aufnahme des Grundtatbestands des § 126a Absatz 1 StGB-E in den Katalog der Ermittlungsmaßnahmen der §§ 100a Absatz 2 Nummer 1 Buchstabe d, 100b Absatz 2 Nummer 1 Buchstabe b, 100g Absatz 2 Satz 2 Nummer 1 Buchstabe b StPO angezeigt, soweit die rechtswidrige Tat ihrerseits der schweren beziehungsweise besonders schweren Kriminalität zuzurechnen ist. Hiermit wird dem Umstand Rechnung getragen, dass die Nachweisbarkeit einer Beihilfestrafbarkeit zu den Katalogtaten

der §§ 100a Absatz 2, 100b Absatz 2, 100g Absatz 2 StPO im Cyberbereich erheblich erschwert ist. Da § 126a StGB-E die sich hieraus ergebenden Strafbarkeitslücke zu schließen bezweckt und strukturell an eine Teilnahmestrafbarkeit anknüpft, ist eine entsprechende Anpassung der Ermittlungsmaßnahmen erforderlich. In einem digitalen Umfeld müssen auch digitale Ermittlungsmaßnahmen möglich sein. Indem die Anordnung der oben genannten Ermittlungsmaßnahmen auf die Fälle beschränkt wird, in denen die rechtswidrige Straftat im Sinne des § 126a Absatz 1 StGB-E ihrerseits eine Katalogtat im Sinne der Ermittlungsmaßnahme darstellt, wird dem Verhältnismäßigkeitsgrundsatz genügt und ein Gleichlauf zur Beihilfestrafbarkeit gewährleistet.

Schließlich schafft der Gesetzentwurf mit § 99 Absatz 2 StPO-E eine klarstellende gesetzliche Regelung, die es den Strafverfolgungsbehörden ausdrücklich ermöglicht, von Postdienstleistern Auskünfte auch über noch nicht ein- sowie bereits ausgelieferte Sendungen zu verlangen. Diese Regelung trägt dem Beschluss eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) Rechnung, in dem in ausdrücklichem Widerspruch zu einer früheren Entscheidung eines anderen Ermittlungsrichters des Bundesgerichtshofs vom 11. Juli 2012 (3 BGs 211/12, BeckRS 2014, 05922) entschieden wurde, dass für retrograde Auskunftsverlangen keine Rechtsgrundlage existiere und auch für Auskunftsverlangen über noch nicht im Gewahrsam des Postdienstleisters befindliche Postsendungen keine Rechtsgrundlage existieren dürfte. Auch wenn offen ist, ob andere Ermittlungsrichter beim Bundesgerichtshof sich dieser Auffassung anschließen werden, ist jedenfalls zur Vermeidung von Rechtsunsicherheiten eine gesetzliche Klarstellung notwendig. Die Auskünfte von Postdienstleistern liefern einen effektiven Ermittlungsansatz zur Identifizierung von Verdächtigen, insbesondere in den Fällen des Handels mit illegalen Waren im Internet, aber auch im Bereich anderer Kriminalitätsphänomene wie etwa beim Betrug im Versandhandel oder in Staatsschutz- und Terrorismusverfahren. Die praktische Bedeutung retrograder Auskunftsverlangen auch in Staatsschutz- und Terrorismusverfah-

ren wird dabei durch den Umstand belegt, dass dem vorgenannten Beschluss eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 ein Antrag des Generalbundesanwalts zugrunde lag, der in einem Ermittlungsverfahren wegen des Verdachts der Beihilfe zur Vorbereitung einer schweren staatsgefährdenden Gewalttat gemäß §§ 89a, 27 StGB unter anderem zum Ziel hatte, Name und Anschrift der jeweiligen Absender von Sendungen an einen bestimmten Adressaten innerhalb eines bestimmten Zeitraums zu ermitteln.“

bb) Im Abschnitt „B. Zu den Einzelnen Vorschriften“ ist die Begründung zu Artikel 2 wie folgt zu fassen:

**„Zu Artikel 2 (Änderung der Strafprozessordnung)**

**Zu Nummer 1 (§ 99 Absatz 2 – neu –StPO)**

Mit § 99 Absatz 2 StPO-E wird eine klarstellende gesetzliche Regelung geschaffen, die es den Strafverfolgungsbehörden ausdrücklich ermöglicht, von Postdienstleistern Auskünfte über Sendungen zu verlangen und zwar unabhängig davon, ob sich die jeweilige Sendung in deren Gewahrsamsbereich befindet oder nicht.

§ 99 Absatz 2 Satz 1 StPO-E regelt hierzu, dass der Richter, unter den Voraussetzungen des § 100 StPO auch der Staatsanwalt, von Personen oder Unternehmen, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen, statt einer Beschlagnahme Auskunft über Postsendungen und Telegramme verlangen kann, die vom Beschuldigten herrühren oder für ihn bestimmt sind. Damit wird die bereits bisher weitgehend anerkannte Möglichkeit, unter den Voraussetzungen des § 99 StPO an Stelle einer Beschlagnahme als Minus von den Postdienstleistern Auskunft über Postsendungen zu verlangen, im Gesetz ausdrücklich klargestellt.

§ 99 Absatz 2 Satz 2 StPO-E stellt klar, dass Auskunft auch über solche Sendungen verlangt werden kann, die sich bei Eingang des Ersuchens nicht mehr oder noch nicht im Machtbereich des Postdienstleisters befinden. Damit wird dem Umstand Rechnung getragen, dass bislang sowohl in der Rechtsprechung als auch in der Literatur unterschiedliche Auffassungen dazu vertreten wurden, ob Auskünfte auch über noch nicht ein- und bereits ausgelieferte Sendungen zu erteilen sind. Wäh-

rend einige Stimmen dies bejahten und sich dabei auf eine analoge Anwendung von § 99 StPO stützen oder die Vorschriften der §§ 94, 95 und 98 StPO heranzogen, lehnten andere die Zulässigkeit solcher Auskunftsverlangen mangels einschlägiger Rechtsgrundlage ab. Der zuletzt genannten Auffassung hat sich auch ein Ermittlungsrichter beim Bundesgerichtshof mit Beschluss vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) in ausdrücklichem Widerspruch zur früheren Entscheidung eines anderen Ermittlungsrichter des Bundesgerichtshofs vom 11. Juli 2012 (3 BGs 211/12, BeckRS 2014, 05922) für Auskunftsverlangen über bereits ausgelieferte Sendungen (retrograde Auskunftsverlangen) angeschlossen und angemerkt, dass ähnliches auch für noch nicht eingelieferte Sendungen gelten dürfte. Auch wenn offen ist, ob sich auch andere Ermittlungsrichter beim Bundesgerichtshof dieser Auffassung anschließen werden, ist zur Vermeidung von Rechtsunsicherheiten eine gesetzliche Klarstellung erforderlich, die mit dem Satz 2 des § 99 Absatz 2 StPO-E umgesetzt wird.

Im Ergebnis wird damit für die Ermittlungsbehörden die Möglichkeit geschaffen, Auskünfte über Postsendungen und Telegramme zu verlangen, die sich im Gewahrsam des Postdienstleisters befinden, befunden haben oder zur dortigen Einlieferung (etwa aufgrund einer online Frankierung) ankündigt sind.

#### **Zu Nummer 2 (§ 100a Absatz 2 Nummer 1 Buchstabe d StPO)**

Für eine effektive Verfolgung von mittels internetbasierter Kommunikation begangener Taten ist es regelmäßig erforderlich, die Kommunikationswege der Beteiligten nachzuvollziehen. Andere Ermittlungsmethoden führen nicht zur Aufklärung der Tatstrukturen, die sich ohne reelle Kontakte mit etwaigen Beteiligten in der analogen Welt gestalten. Diese Notwendigkeit rechtfertigt indes nicht die Eröffnung eingriffintensiver Ermittlungsmaßnahmen für alle Fälle der Informations- und Kommunikationskriminalität. Mit Blick auf das durch Maßnahmen gemäß § 100a StPO betroffene Grundrecht aus Artikel 10 GG gebietet der Grundsatz der Verhältnismäßigkeit eine Abwägung im Einzelfall, ob bestimmte Straftaten durch den Gesetzgeber im Rahmen seines Beurteilungsspielraums als derart schwer eingestuft werden, dass ein entsprechender Tatverdacht Grundrechtseingriffe rechtfertigen kann (vergleiche BVerfG NJW 2012, 833 – Rn. 203 ff.). Dabei sind insbesondere

das geschützte Rechtsgut und dessen Bedeutung für die Rechtsgemeinschaft in den Blick zu nehmen.

Die in § 126a Absatz 3 StGB-E geregelte Qualifikation weist einen deutlich gesteigerten Unrechtsgehalt auf und stellt daher eine schwere Straftat im Sinne des § 100a Absatz 1 StPO dar. Die auch in anderen Deliktsbereichen, zum Beispiel § 263 Absatz 3 Satz 2 Nummer 1 StGB, zu einer erhöhten Strafdrohung führende Begehungsweise erhöht die Gefahren für die bereits durch den Grundtatbestand und die Haupttaten geschützten Rechtsgüter weiter und dauerhaft. In diesen Fällen, in denen ein Täter nicht nur alleine und gelegentlich oder ohne eigennütziges finanzielles Interesse gezielt Strukturen der kriminellen Infrastruktur sowie gleichzeitig eine besondere Organisationsgefahr schafft, handelt es sich daher um schwere Straftaten im Sinne des § 100a Absatz 1 StPO. Dies bestätigt auch der Vergleich mit den weiteren in § 100a Absatz 2 StPO genannten Straftatbeständen.

Daneben ist auch eine Aufnahme des Grundtatbestandes des § 126a Absatz 1 StGB-E in den Katalog der Ermittlungsmaßnahmen des § 100a Absatz 2 Nummer 1 Buchstabe d StPO angezeigt, soweit die rechtswidrige Tat ihrerseits der schweren Kriminalität zuzurechnen ist. Hiermit wird den besonderen Strukturen im Cyberbereich Rechnung getragen, in deren Rahmen analoge Ermittlungsmaßnahmen versagen. In einem digitalen Umfeld müssen auch digitale Ermittlungsmaßnahmen möglich sein. Da § 126a StGB-E die sich hieraus ergebenden Strafbarkeitslücke zu schließen bezweckt, ist eine entsprechende Anpassung der Ermittlungsmaßnahmen erforderlich. Dem Betrieb einer kriminellen Infrastruktur kann ein zumindest den jeweiligen Beihilfehandlungen in ihrer Summe gleichwertiger Unrechtsgehalt zugemessen werden. Indem die Anordnung der oben genannten Ermittlungsmaßnahmen auf die Fälle beschränkt wird, in denen die rechtswidrige Tat im Sinne des § 126a Absatz 1 StGB-E ihrerseits eine Katalogtat im Sinne der Ermittlungsmaßnahme darstellt, wird ein Wertungswiderspruch zur Beihilfestrafbarkeit verhindert. Verhältnismäßigkeitserwägungen stehen einer Aufnahme des Grundtatbestandes des § 126a Absatz 1 StGB-E, zumal mit der gewählten Beschränkung, nicht entgegen. Die von § 100a StPO erfassten Ermittlungsmaßnahmen (Überwachung von E-Mails, Nachrichten in sozialen Netzwerken einschließlich ge-

schlossener Benutzergruppen et cetera) sind für Ermittlungen in der digitalen Welt zwingend erforderlich, weil analoge Spuren/Ermittlungsansätze meist nicht zur Verfügung stehen. Die mit Überwachungsmaßnahmen gemäß § 100a StPO einhergehenden Grundrechtseingriffe sind dadurch zu rechtfertigen, dass durch die Begehung von § 126a StGB-E eine Gefahr geschaffen wird, die über das bloße Anbieten einer bestimmten Infrastruktur hinausgeht, indem nämlich besonders gefährliche Straftaten Vorschub geleistet wird, die aus diesem Grund ihrerseits Katalogtaten im Sinne des § 100a Absatz 2 StPO darstellen.

**Zu Nummer 3** (§ 100b Absatz 2 Nummer 1 Buchstabe b StPO)

Für eine effektive Verfolgung von mittels internetbasierter Kommunikation begangener Taten wird vielfach ferner der verdeckte Zugriff der Ermittlungsbehörden auf ein von dem Betroffenen genutztes informationstechnisches Systems notwendig sein. § 100a Absatz 1 Satz 2 und 3 StPO erfasst nur laufende und hinzukommende Kommunikationsinhalte, wohingegen § 100b StPO den Zugriff auf alle im System bereits gespeicherten Daten ermöglicht. Aufgrund der Eingriffsintensität in das Grundrecht auf informationelle Selbstbestimmung setzt § 100b StPO den Verdacht des Vorliegens einer besonders schweren Straftat voraus, wobei die Tat auch im konkreten Einzelfall und nicht nur abstrakt besonders schwer wiegen und die Ermittlungen auf andere Weise wesentlich erschwert oder aussichtslos sein müssen.

Die erhöhte Strafdrohung des § 126a Absatz 3 StGB-E verdeutlicht, dass der Tatbestand aufgrund des erhöhten Unrechtsgehalts dem Bereich der besonders schweren Kriminalität zuzurechnen ist. Daher erfolgt die Aufnahme des Qualifikationstatbestands in den Katalog des § 100b Absatz 2 Nummer 1 Buchstabe b StPO. § 126a Absatz 3 StGB-E fügt sich damit hinsichtlich seines Schweregrades in den Straftatenkatalog des § 100b Absatz 2 StPO ein, der Straftaten gegen die öffentliche Ordnung mit Freiheitsstrafe von mehr als fünf Jahren im Höchstmaß in Nummer 1 Buchstabe b bereits erfasst.

Soweit durch die Begehung des § 126a Absatz 1 StGB-E eine Katalogtat im Sinne des § 100b Absatz 2 StPO ermöglicht oder gefördert wird, handelt es sich auch bei dem Grundtatbestand gemäß § 126a Absatz 1

StGB-E um eine besonders schwere Straftat. Auch hier besteht die Parallele zur Beihilfestrafbarkeit. Im Übrigen, auch bezüglich der Ausführungen zur Verhältnismäßigkeit, wird auf die Begründung zu § 100a Absatz 2 Nummer 1 Buchstabe d StPO Bezug genommen.

**Zu Nummer 4** (§ 100g Absatz 2 Satz 2 Nummer 1 Buchstabe b StPO)

Die Erhebung von Verkehrsdaten im Sinne von §§ 96 Absatz 1, 113b TKG kann in vielen Fällen die einzig erfolgversprechende Ermittlungsmaßnahme für die Auswertung internetbasierter Kommunikation darstellen, die wiederum in den Fällen des § 126a StGB-E meist die einzigen Ermittlungsansätze bietet. Über § 100g StPO können zum Beispiel Erkenntnisse über die Identität von Kommunikationspartnern, IP-Adressen und Standortdaten gewonnen werden. Sowohl beim Qualifikationstatbestand des § 126a Absatz 3 StGB-E handelt es sich um schwere Straftaten als auch bei § 126a Absatz 1 StGB-E, wenn durch die internetbasierte Leistung eine Katalogtat im Sinne des § 100g Absatz 2 StPO unterstützt wird. Im Übrigen, auch bezüglich der Ausführungen zur Verhältnismäßigkeit, wird auf die Begründung zu § 100b Absatz 2 Nummer 1 Buchstabe b StPO Bezug genommen.“

Begründung (nur gegenüber dem Plenum):

Die Problemanalyse des Gesetzesantrags ist zutreffend und die Forderung nach einem eigenen Straftatbestand für den Betrieb krimineller Infrastrukturen, dessen Qualifikationstatbestand in den Katalog der Ermittlungsmaßnahme der Telefonüberwachung aufgenommen wird, grundsätzlich zu unterstützen.

Zu Artikel 2 Nummer 1 (§ 99 StPO):

In Ergänzung zum Straftatbestand für den Betrieb krimineller Infrastrukturen müssen auch die Ermittlungsbefugnisse der Strafverfolgungsbehörden ausgebaut werden. Der im Gesetzesantrag vorgesehene Ausbau dieser Ermittlungsbefugnisse geht allerdings nicht weit genug. Erfolgsversprechende Ermittlungsansätze ergeben sich auch am Übergang von der digitalen in die analoge Welt, nämlich bei der Aufgabe und Annahme entsprechender Warensendungen.

Die Befugnis der Strafverfolgungsbehörden, Auskunft auch über solche Warensendungen zu verlangen, die sich noch nicht oder nicht mehr im Machtbereich der Postdienstleister befinden, ist jedoch aufgrund der Entscheidung eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) zweifelhaft geworden. Denn in dieser Entscheidung wurde in ausdrücklichem Widerspruch zu einer früheren Entscheidung eines anderen Ermittlungsrichters des Bundesgerichtshofs vom 11. Juli 2012 (3 BGs

211/12, BeckRS 2014, 05922) festgestellt, dass für Auskunftsverlangen über bereits ausgelieferte Sendungen (sogenannte retrograde Auskunftsverlangen) keine Eingriffsnorm existiere und dass Ähnliches auch für noch nicht eingelieferte Sendungen gelten dürfte. Die entsprechende Gesetzeslücke zu schließen, sei Aufgabe des Gesetzgebers. Auch wenn offen ist, ob sich andere Ermittlungsrichter beim Bundesgerichtshof dieser Auffassung anschließen werden, sollte – entsprechend dem einstimmig gefassten Beschluss der Justizministerinnen und Justizminister im Rahmen ihrer Frühjahrskonferenz am 21. und 22. Juni 2017 – zur Vermeidung von Rechtsunsicherheiten umgehend eine gesetzliche Klarstellung erfolgen. Eine entsprechende Empfehlung hat auch die Länder-Arbeitsgruppe „Digitale Agenda für das Straf- und Strafprozessrecht“ in ihrem Abschlussbericht 2018 ausgesprochen.

Zu Artikel 2 Nummer 2 bis 4 (§ 100a Absatz 2 Nummer 1 Buchstabe d StPO, § 100b Absatz 2 Nummer 1 Buchstabe b StPO und § 100g Absatz 2 Satz 2 Nummer 1 Buchstabe b StPO)

Die Aufnahme des neuen § 126a Absatz 3 StGB-E in § 100a Absatz 2 StPO ist zu befürworten, greift im Ergebnis jedoch zu kurz.

Dies gilt zum einen für die Aufnahme lediglich des Qualifikationstatbestandes in den Katalog des § 100a Absatz 2 StPO, zum anderen sind für die effektive Durchführung von Ermittlungen auch die Befugnisse zur Online-Durchsuchung (§ 100b StPO) und zur Verkehrsdatenerhebung (§ 100g StPO) unerlässlich.

- a) Der Gesetzentwurf verkennt, dass es sich bei § 126a Absatz 3 StGB-E um "schwere" beziehungsweise "besonders schwere Kriminalität" im Sinne der §§ 100b Absatz 2 Nummer 1 Buchstabe b, 100g Absatz 2 Satz 2 Nummer 1 Buchstabe b StPO handelt und diese Ermittlungsmaßnahmen zur effektiven Verfolgung der Straftaten vor dem Hintergrund der Besonderheiten der Tatbegehung mittels internetbasierter Leistung gemäß § 126a StGB-E zwingend erforderlich sind. In einem digitalen Umfeld müssen auch digitale Ermittlungsmaßnahmen möglich sein. Es reicht nicht aus, auf die Telekommunikation des zunächst anonym agierenden Täters im Sinne des § 126a StGB-E zugreifen zu können, sondern den Ermittlungsbehörden muss auch die Möglichkeit offen stehen, seinen Standort zu ermitteln, ihn zu identifizieren, herauszufinden, mit welchen anderen Telekommunikationspartnern Kontakt bestand (§ 100g StPO) und die von ihm betreffend die von ihm zugänglich gemachte Leistung gespeicherten Daten zu erheben (§ 100b StPO). Besonders augenscheinlich wird das für die Ermittlungsbefugnisse gemäß § 100b StPO: Ohne diese könnte beispielsweise auf den Systemen eines Beschuldigten, der verdächtig ist, eine Plattform für illegalen Waffen- oder Betäubungsmittelhandel zu betreiben, nicht einmal nach Erkenntnissen zu dieser Plattform gesucht und mittels des dort vorhandenen Zugangs zu der Plattform weiter ermittelt werden. Die Beschlagnahme der Geräte des Beschuldigten kann vielfach nicht weiterführen, da die Software, mit der die Plattform betrieben wird, auf externen Servern liegt.

Nur, wenn den Strafverfolgungsbehörden das gesamte Ermittlungsportfolio für die digitale Welt zur Verfügung steht, können Straftaten gemäß

- § 126a StGB-E, die in der digitalen Welt stattfinden, aufgeklärt werden.
- b) Zum anderen ist durch Aufnahme des § 126a Absatz 1 StGB-E in den Katalog der Ermittlungsmaßnahmen, soweit die rechtswidrige Tat ihrerseits eine Katalogtat im Sinne der Ermittlungsmaßnahmen darstellt, dem Umstand Rechnung zu tragen, dass eine Bestrafung wegen Beihilfe zu den Katalogtaten der §§ 100a Absatz 2, 100b Absatz 2, 100g Absatz 2 StPO aufgrund der durch den Cyberbereich bedingten Nachweisschwierigkeiten in der Regel ausscheidet. § 126a StGB-E bezweckt jedoch gerade, die sich hieraus ergebenden Strafbarkeitslücke zu schließen. Dem Betrieb einer kriminellen Infrastruktur kann ein zumindest den jeweiligen Beihilfehandlungen in ihrer Summe gleichwertiger Unrechtsgehalt zugemessen werden. Zur Vermeidung von Wertungswidersprüchen ist eine Aufnahme des § 126a StGB-E in den Katalog der Ermittlungsmaßnahmen daher zwingend angezeigt. Verhältnismäßigkeitserwägungen stehen einer Aufnahme des Grundtatbestands des § 126a Absatz 1 StGB-E, zumal mit der gewählten Beschränkung, in die Kataloge der §§ 100a Absatz 2, 100b Absatz 2, 100g Absatz 2 StPO nicht entgegen. Die von § 100a StPO erfassten Ermittlungsmaßnahmen (Überwachung von E-Mails, Nachrichten in sozialen Netzwerken einschließlich geschlossener Benutzergruppen etcetera) sind für Ermittlungen in der digitalen Welt zwingend erforderlich, weil "analoge" Spuren/Ermittlungsansätze meist nicht zur Verfügung stehen. Die mit den Ermittlungen einher gehenden Grundrechtseingriffe sind dadurch gerechtfertigt, dass durch die Begehung von § 126a StGB-E eine Gefahr geschaffen wird, die über die bloße Zurverfügungstellung einer bestimmten Infrastruktur hinausgehen, indem nämlich besonders gefährliche Straftaten ermöglicht oder gefördert werden, die aus diesem Grund ihrerseits Katalogtaten im Sinne der §§ 100a Absatz 2, 100b Absatz 2, 100g Absatz 2 StPO darstellen.

R 5. Zu Artikel 2 Nummer 1 – neu – (§ 99 Absatz 2 – neu – StPO)

(entfällt  
bei  
Annahme  
von  
Ziffer 4)

Artikel 2 ist wie folgt zu fassen:

**,Artikel 2**

**Änderung der Strafprozessordnung**

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. § 99 wird wie folgt geändert:

a) Der bisherige Wortlaut wird Absatz 1.

b) Folgender Absatz 2 wird angefügt:

„(2) Statt einer Beschlagnahme kann der Richter, unter den Voraussetzungen des § 100 auch der Staatsanwalt, von Personen oder Unternehmen, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen, Auskunft über die in Absatz 1 genannten Sendungen verlangen, die vom Beschuldigten herrühren oder für ihn bestimmt sind. Die Auskunft wird auch über solche Sendungen erteilt, die sich bei Eingang des Ersuchens nicht mehr oder noch nicht im Machtbereich der Person oder des Unternehmens befinden.“

2. § 100a Absatz 2 Nummer 1 Buchstabe d ... <weiter wie Vorlage>

#### Folgeänderungen:

a) Das Vorblatt ist wie folgt zu ändern:

aa) Der Abschnitt „A. Problem und Ziel“ ist wie folgt zu ändern:

aaa) Nach Absatz 5 ist folgender Absatz 5a einzufügen:

Zur Identifizierung der Tatverdächtigen, die über die entsprechenden Plattformen ihre kriminellen Geschäfte abwickeln, ergeben sich am Übergang von der digitalen in die analoge Welt erfolgversprechende Ermittlungsansätze, nämlich aus den Daten, die bei der Aufgabe und Annahme entsprechender Warensendungen von den Postdienstleistern festgehalten werden. Jedoch können die Strafverfolgungsbehörden nach dem Beschluss eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) mangels Rechtsgrundlage dann keine Auskunft über diese Daten von den Postdienstleistern verlangen, wenn die Sendung bereits ausgeliefert ist und sich damit nicht mehr im Gewahrsam des Postdienstleisters befindet (sogenanntes retrograde Auskunftsverlangen). Ähnliches dürfte – wie der Ermittlungsrichter in dem vorgenannten Beschluss anmerkt – auch für Postsendungen gelten, die sich noch nicht im Gewahrsam des Postdienstleisters befinden. Die entsprechende Gesetzeslücke zu schließen, sei Aufgabe des Gesetzgebers.“

bbb) Absatz 6 ist wie folgt zu fassen:

„Vor diesem Hintergrund haben sich die Justizministerinnen und Justizminister der Länder bereits anlässlich ihrer Konferenzen am 17. November 2016 in Berlin und am 21. und 22. Juni 2017 in Deidesheim mit den geschilderten Problemlagen befasst. Die Justizministerinnen und Justizminister halten für erforderlich, das öffentliche Feilbieten von Gegenständen und Dienstleistungen zur Vorbereitung von Straftaten im Internet zu unterbinden. Sie haben daher die Bundesregierung um Prüfung gebeten, inwieweit dies durch Anpassungen des materiellen Strafrechts, namentlich des Waffengesetzes, besser als bisher erreicht werden kann. Ferner haben sie die Bundesregierung gebeten, sich für eine klarstellende gesetzliche Regelung einzusetzen, die es den Strafverfolgungsbehörden ausdrücklich ermöglicht, von Postdienstleistern Auskünfte auch über noch nicht ein- sowie bereits ausgelieferte Sendungen zu verlangen.“

bb) Dem Abschnitt „B. Lösung“ ist folgender Absatz anzufügen:

„Schließlich schafft der Entwurf zur Klarstellung eine gesetzliche Regelung, die es Strafverfolgungsbehörden ausdrücklich ermöglicht, von Postdienstleistern Auskünfte auch über noch nicht ein- sowie bereits ausgelieferte Sendungen zu verlangen.“

cc) Im Abschnitt „E. Erfüllungsaufwand“ ist der Text im Unterabschnitt „E.2 Erfüllungsaufwand für die Wirtschaft“ wie folgt zu fassen:

„Der Aufwand, der für die Postunternehmen durch die Auskunftsverlangen über noch nicht ein- sowie bereits ausgelieferte Sendungen zu erwarten ist, kann nicht beziffert werden.“

b) Die Begründung ist wie folgt zu ändern:

aa) Im Abschnitt „A. Allgemeines“ ist der Abschnitt „I. Zielsetzung und wesentlicher Inhalt des Gesetzesentwurfs“ wie folgt zu ändern:

aaa) Nach Absatz 8 ist folgender Absatz 8a einzufügen:

„Zur Identifizierung der Tatverdächtigen, die über die entsprechenden Plattformen ihre kriminellen Geschäfte abwickeln, ergeben sich am Übergang von der digitalen in die analoge Welt erfolgversprechende Ermittlungsansätze, nämlich aus den Daten, die bei der Aufgabe und Annahme entsprechender Waren-

sendungen von den Postdienstleistern festgehalten werden. Jedoch können die Strafverfolgungsbehörden nach dem Beschluss eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) mangels Rechtsgrundlage dann keine Auskunft über diese Daten von den Postdienstleistern verlangen, wenn die Sendung bereits ausgeliefert ist und sich damit nicht mehr im Gewahrsam des Postdienstleisters befindet (sog. retrograde Auskunftsverlangen). Ähnliches dürfte – wie der Ermittlungsrichter in dem vorgenannten Beschluss anmerkt – auch für Postsendungen gelten, die sich noch nicht im Gewahrsam des Postdienstleisters befinden. Die entsprechende Gesetzeslücke zu schließen, sei Aufgabe des Gesetzgebers.“

bbb) Folgender Absatz ist anzufügen:

„Schließlich schafft der Entwurf mit § 99 Absatz 2 StPO-E eine klarstellende gesetzliche Regelung, die es den Strafverfolgungsbehörden ausdrücklich ermöglicht, von Postdienstleistern Auskünfte auch über noch nicht ein- sowie bereits ausgelieferte Sendungen zu verlangen. Diese Regelung trägt dem Beschluss eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) Rechnung, in dem in ausdrücklichem Widerspruch zu einer früheren Entscheidung eines anderen Ermittlungsrichters des Bundesgerichtshofs vom 11. Juli 2012 (3 BGs 211/12, BeckRS 2014, 05922) entschieden wurde, dass für retrograde Auskunftsverlangen keine Rechtsgrundlage existiere und auch für Auskunftsverlangen über noch nicht im Gewahrsam des Postdienstleisters befindliche Postsendungen keine Rechtsgrundlage existieren dürfte. Auch wenn offen ist, ob andere Ermittlungsrichter beim Bundesgerichtshof sich dieser Auffassung anschließen werden, ist jedenfalls zur Vermeidung von Rechtsunsicherheiten eine gesetzliche Klarstellung notwendig. Die Auskünfte von Postdienstleistern liefern einen effektiven Ermittlungsansatz zur Identifizierung von Verdächtigen, insbesondere in den Fällen des Handels mit illegalen Waren im Internet, aber auch im Bereich anderer Kriminalitätsphänomene wie etwa beim Betrug

im Versandhandel oder in Staatsschutz- und Terrorismusverfahren. Die praktische Bedeutung retrograder Auskunftsverlangen auch in Staatsschutz- und Terrorismusverfahren wird dabei durch den Umstand belegt, dass dem vorgenannten Beschluss eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 ein Antrag des Generalbundesanwalts zugrunde lag, der in einem Ermittlungsverfahren wegen des Verdachts der Beihilfe zur Vorbereitung einer schweren staatsgefährdenden Gewalttat gemäß §§ 89a, 27 StGB unter anderem zum Ziel hatte, Name und Anschrift der jeweiligen Absender von Sendungen an einen bestimmten Adressaten innerhalb eines bestimmten Zeitraums zu ermitteln.“

- bb) Im Abschnitt „B. Zu den einzelnen Vorschriften“ ist nach der Zwischenüberschrift „Zu Artikel 2 (Änderung der Strafprozessordnung)“ folgender Text einzufügen:

**„Zu Nummer 1 Buchstabe b (§ 99 Absatz 2 StPO-E)**

Mit § 99 Absatz 2 StPO-E wird eine klarstellende gesetzliche Regelung geschaffen, die es den Strafverfolgungsbehörden ausdrücklich ermöglicht, von Postdienstleistern Auskünfte über Sendungen zu verlangen und zwar unabhängig davon, ob sich die jeweilige Sendung in deren Gewahrsamsbereich befindet oder nicht.

Satz 1 des § 99 Absatz 2 StPO-E regelt hierzu, dass der Richter, unter den Voraussetzungen des § 100 StPO auch der Staatsanwalt, von Personen oder Unternehmen, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen, statt einer Beschlagnahme Auskunft über Postsendungen und Telegramme verlangen kann, die vom Beschuldigten herrühren oder für ihn bestimmt sind. Damit wird die bereits bisher weitgehend anerkannte Möglichkeit, unter den Voraussetzungen des § 99 StPO an Stelle einer Beschlagnahme als Minus von den Postdienstleistern Auskunft über Postsendungen zu verlangen, im Gesetz ausdrücklich klargestellt.

Satz 2 des § 99 Absatz 2 StPO-E stellt klar, dass Auskunft auch über solche Sendungen verlangt werden kann, die sich bei Eingang des Ersuchens nicht mehr oder noch nicht im Machtbereich des Postdienstleisters befinden. Damit wird dem Umstand Rechnung getragen, dass

bislang sowohl in der Rechtsprechung als auch der Literatur unterschiedliche Auffassungen dazu vertreten wurden, ob Auskünfte auch über noch nicht ein- und bereits ausgelieferte Sendungen zu erteilen sind. Während einige Stimmen dies bejahten und sich dabei auf eine analoge Anwendung von § 99 StPO stützen oder die Vorschriften der §§ 94, 95 und 98 StPO heranzogen, lehnten andere die Zulässigkeit solcher Auskunftsverlangen mangels einschlägiger Rechtsgrundlage ab. Der zuletzt genannten Auffassung hat sich auch ein Ermittlungsrichter beim Bundesgerichtshof mit Beschluss vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) in ausdrücklichem Widerspruch zur früheren Entscheidung eines anderen Ermittlungsrichter des Bundesgerichtshofs vom 11. Juli 2012 (3 BGs 211/12, BeckRS 2014, 05922) für Auskunftsverlangen über bereits ausgelieferte Sendungen (retrograde Auskunftsverlangen) angeschlossen und angemerkt, dass ähnliches auch für noch nicht eingelieferte Sendungen gelten dürfte. Auch wenn offen ist, ob sich auch andere Ermittlungsrichter beim Bundesgerichtshof dieser Auffassung anschließen werden, ist zur Vermeidung von Rechtsunsicherheiten eine gesetzliche Klarstellung erforderlich, die mit dem Satz 2 des § 99 Absatz 2 StPO-E umgesetzt wird.

Im Ergebnis wird damit für die Ermittlungsbehörden die Möglichkeit geschaffen, Auskünfte über Postsendungen und Telegramme zu verlangen, die sich im Gewahrsam des Postdienstleisters befinden, befunden haben oder zur dortigen Einlieferung (etwa aufgrund einer online Frankierung) ankündigt sind.

### **Zu Nummer 2“**

#### Begründung (nur gegenüber dem Plenum):

In Ergänzung zum Straftatbestand für den Betrieb krimineller Infrastrukturen müssen auch die Ermittlungsbefugnisse der Strafverfolgungsbehörden ausgebaut werden. Der im Gesetzentwurf vorgesehene Ausbau dieser Ermittlungsbefugnisse geht allerdings nicht weit genug. Erfolgsversprechende Ermittlungsansätze ergeben sich auch am Übergang von der digitalen in die analoge Welt, nämlich bei der Aufgabe und Annahme entsprechender Warensendungen.

Die Befugnis der Strafverfolgungsbehörden, Auskunft auch über solche Warensendungen zu verlangen, die sich noch nicht oder nicht mehr im Machtbereich der Postdienstleister befinden, ist jedoch aufgrund der Entscheidung eines Ermittlungsrichters beim Bundesgerichtshof vom 27. Oktober 2016 (1 BGs 107/16, NJW 2017, 680) zweifelhaft geworden. Denn in dieser Entscheidung

wurde in ausdrücklichem Widerspruch zu einer früheren Entscheidung eines anderen Ermittlungsrichters des Bundesgerichtshofs vom 11. Juli 2012 (3 BGs 211/12, BeckRS 2014, 05922) festgestellt, dass für Auskunftsverlangen über bereits ausgelieferte Sendungen (sog. retrograde Auskunftsverlangen) keine Eingriffsnorm existiere und dass Ähnliches auch für noch nicht eingelieferte Sendungen gelten dürfte. Die entsprechende Gesetzeslücke zu schließen, sei Aufgabe des Gesetzgebers. Auch wenn offen ist, ob sich andere Ermittlungsrichter beim Bundesgerichtshof dieser Auffassung anschließen werden, sollte – entsprechend dem einstimmig gefassten Beschluss der Justizministerinnen und Justizminister im Rahmen ihrer Frühjahrskonferenz am 21. und 22. Juni 2017 – zur Vermeidung von Rechtsunsicherheiten umgehend eine gesetzliche Klarstellung erfolgen. Eine entsprechende Empfehlung hat auch die Länder-Arbeitsgruppe „Digitale Agenda für das Straf- und Strafprozessrecht“ in ihrem Abschlussbericht 2018 ausgesprochen.

## **B.**

6. Der **Rechtsausschuss** schlägt dem Bundesrat vor,

Minister Peter Biesenbach  
(Nordrhein-Westfalen)

gemäß § 33 der Geschäftsordnung des Bundesrates zum Beauftragten des Bundesrates für die Beratung des Gesetzentwurfs im Deutschen Bundestag und in seinen Ausschüssen zu bestellen.