

## **Gesetzentwurf**

### **des Bundesrates**

#### **Entwurf eines Strafrechtsänderungsgesetzes – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen**

##### **A. Problem und Ziel**

Vermehrt nutzen Straftäter die Möglichkeiten der Anonymisierung, die ihnen das Internet bietet. Eine häufig genutzte Form der Anonymisierung erfolgt 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. Insbesondere über das Tor-Netzwerk erfolgt der Zugang zum sogenannten Darknet. Zugang und Erreichbarkeit der Darknet-Angebote sind durch das Erfordernis besonderer Programme, wie des Tor-Browsers, beschränkt.

Die Angebote im Darknet umfassen, wie auch auf andere Weise zugangsbeschränkte Dienste, neben Foren für Whistleblower oder Chatrooms für politisch Verfolgte in autoritär geführten Staaten auch Inhalte bekannter Servicebetreiber, etwa Facebook. Ebenso finden sich jedoch Angebote mit strafrechtlicher Relevanz, darunter Handel mit Betäubungsmitteln, Kinderpornographie oder Waffen, mit Schadsoftware und Ausweispapieren. Vergleichbare Angebote finden sich auch in weiteren Teilen des Internets. In technischer Hinsicht entsprechen die angebotenen Dienste denen bekannter Online-Handelsplattformen mit Vorschaubildern der angebotenen Waren, Werbung, Bewertungen für Verkäufer und Hinweisen auf weitere möglicherweise für einen Nutzer interessante Angebote (vgl. Tzanetakis, Drogenhandel im Darknet, in: Aus Politik und Zeitgeschichte 2017, 46-47/2017, S. 41 ff.).

Das Kriminalitätsphänomen gewinnt in der Praxis der Strafverfolgung zunehmend an Gewicht und beschränkt sich dabei nicht auf wenige Einzelfälle. Aufgrund des ständigen Auftretens neuer Angebote und der auf Verschleierung angelegten Vorgehensweise liegen keine genauen Daten über die Anzahl einschlägiger Foren vor. Die Zentralstellen der Staatsanwaltschaften für die Verfolgung von Cybercrime der Länder haben in den vergangenen Jahren jedoch bereits zahlreiche Ermittlungsverfahren gegen die Verantwortlichen einschlägiger Foren oder Plattformen und deren Nutzer geführt, zum Beispiel „Deutschland im Deep Web“

oder „crimenetwork.biz“. Im internationalen Bereich wurden Verfahren gegen die Verantwortlichen von „Silkroad“, „AlphaBay“ und „Hansa Market“ geführt. Nach Einschätzung des Bundeskriminalamtes wurden im Jahr 2016 circa 50 einschlägige Plattformen unterhalten (vgl. Bundestagsdrucksache 18/9487, S. 2). Das dort betriebene Geschäftsmodell des „Cybercrime-as-a-Service“ wird in der kriminellen Szene weiter ausgebaut (vgl. Lagebild Cybercrime des Bundeskriminalamtes 2016, abrufbar unter [www.bka.de](http://www.bka.de), dort S. 16 ff.). Illegale Online-Handelsplattformen stellen aus Sicht von EUROPOL eine der zentralen Schnittstellen von Cybercrime und weiteren Formen – auch organisierter – Kriminalität dar (vgl. Internet Organised Crime Threat Assessment 2017, abrufbar unter [www.europol.eu](http://www.europol.eu)).

Die Erfahrungen aus den geführten Ermittlungsverfahren lassen ein arbeitsteiliges Zusammenwirken von Plattformbetreibern und Nutzern der Plattform, also sowohl Händlern als auch Käufern, erkennen. Es zeigt sich zudem, dass die klassischen Organisationsdelikte und die historischen gesetzgeberischen Vorstellungen von Täterschaft und Teilnahme auf moderne, internetbasierte Täterstrukturen kaum übertragbar sind. Die Betreiber selbst stellen lediglich eine – in einigen Fällen vollautomatisierte – technische Infrastruktur zur Verfügung. Aufgrund dieser Umstände ist eine Beihilfehandlung zu einer konkreten Haupttat in der Praxis nur schwer erweislich. Auch die Zurechnung von Einzeltaten unter dem Gesichtspunkt einer bandenmäßigen Tatbegehung ist häufig nicht möglich, da in der Regel kriminelle Foren und Marktplätze der Underground Economy in amorphen Organisationsstrukturen jenseits des überkommenen Bandenbegriffs geführt werden.

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

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 retrogrades 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.

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 es 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.

## **B. Lösung**

Der Gesetzentwurf führt einen neuen Straftatbestand des Anbietens von Leistungen zur Ermöglichung von Straftaten ein. Der Tatbestand erfasst ausschließlich internetbasierte Angebote in hinsichtlich Zugang und Erreichbarkeit beschränkten Netzwerken und setzt die Ausrichtung der Leistung auf die Ermöglichung von Delikten, deren Begehung besondere Gefahren für die öffentliche Sicherheit begründen, voraus. Ergänzt wird der Grundtatbestand durch eine Qualifikation im Falle gewerbsmäßiger Begehung. Lediglich diese Qualifikation soll Anknüpfungstat für die cyberspezifische, eingriffsintensive Ermittlungsmaßnahme der Überwachung der Telekommunikationsüberwachung sein. 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.

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.

## **C. Alternativen**

Beibehaltung des bisherigen, unbefriedigenden Zustands, der nicht sämtliche strafwürdigen Verhaltensweisen in angemessener Weise erfasst.

## **D. Haushaltsausgaben ohne Erfüllungsaufwand**

Keine.

## **E. Erfüllungsaufwand**

### **E.1 Erfüllungsaufwand für Bürgerinnen und Bürger**

Für die Bürgerinnen und Bürger entsteht oder entfällt kein Erfüllungsaufwand.

### **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.

### E.3 Erfüllungsaufwand der Verwaltung

Aufgrund der Ausweitung der Strafbarkeit ist zu erwarten, dass die Anzahl der Ermittlungs- und Strafverfahren in einem begrenzten Ausmaß zunimmt. Dies kann zu nicht näher quantifizierbaren Haushaltsmehrausgaben bei den für die Durchführung von Ermittlungs- und Strafverfahren primär zuständigen Strafverfolgungsbehörden der Länder führen.

### F. Weitere Kosten

Den Bürgerinnen und Bürgern sowie der Wirtschaft entstehen keine sonstigen Kosten. Auswirkungen auf das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

**BUNDESREPUBLIK DEUTSCHLAND**  
**DIE BUNDESKANZLERIN**

Berlin, 17. April 2019

An den  
Präsidenten des  
Deutschen Bundestages  
Herrn Dr. Wolfgang Schäuble  
Platz der Republik 1  
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich gemäß Artikel 76 Absatz 3 des Grundgesetzes den vom Bundesrat in seiner 975. Sitzung am 15. März 2019 beschlossenen

Entwurf eines Strafrechtsänderungsgesetzes – Einführung einer  
eigenständigen Strafbarkeit für das Betreiben von internetbasierten  
Handelsplattformen für illegale Waren und Dienstleistungen

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium der Justiz und für Verbraucherschutz.

Die Auffassung der Bundesregierung zu dem Gesetzentwurf ist in der als Anlage 2 beigefügten Stellungnahme dargelegt.

Mit freundlichen Grüßen

Dr. Angela Merkel



## Anlage 1

**Entwurf eines Strafrechtsänderungsgesetzes – Einführung einer  
eigenständigen Strafbarkeit für das Betreiben von internetbasierten  
Handelsplattformen für illegale Waren und Dienstleistungen**

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

**Artikel 1****Änderung des Strafgesetzbuches**

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 126 folgende Angabe eingefügt:  
„§ 126a Anbieten von Leistungen zur Ermöglichung von Straftaten“.
2. 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;“
3. Nach § 126 wird folgender § 126a eingefügt:

## „§ 126a

## Anbieten von Leistungen zur Ermöglichung von Straftaten

(1) Wer eine internetbasierte Leistung anbietet, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten im Sinne von Satz 2 zu ermöglichen oder zu fördern, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Rechtswidrige Taten im Sinne des Satzes 1 sind

1. § 95 Absatz 1 des Gesetzes über den Verkehr mit Arzneimitteln,
2. §§ 29 Absatz 1 Nummer 1, 29a, 30, 30a des Betäubungsmittelgesetzes,
3. § 19 Absatz 1 des Grundstoffüberwachungsgesetzes,
4. § 52 Absatz 1 Nummer 1 und Absatz 3 Nummer 1 des Waffengesetzes,
5. § 40 Absatz 1 und 2 des Sprengstoffgesetzes,
6. §§ 19 Absatz 1, 20 Absatz 1, 20a Absatz 1, 22a Absatz 1 Nummer 1, 2 und 4 des Gesetzes über die Kontrolle von Kriegswaffen sowie
7. §§ 146, 147, 149, 152a, 152b, 184b Absatz 1, 202a, 202b, 202c, 263a, 275, 276, 303a und 303b des Strafgesetzbuches.

(2) Die Strafe darf nicht schwerer sein, als die für die Tat im Sinne von Absatz 1 Satz 2 angedrohte Strafe.

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat gewerbsmäßig begeht.“

## 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 wird wie folgt gefasst:

„d) Straftaten gegen die öffentliche Ordnung nach den §§ 126a Absatz 3, 129 bis 130,“.

## Artikel 3

### Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

## Begründung

### A. Allgemeiner Teil

#### I. Zielsetzung und wesentlicher Inhalt des Gesetzentwurfs

Vermeehrt nutzen Straftäter die Möglichkeiten der Anonymisierung, die ihnen das Internet bietet. Eine häufig genutzte Form der Anonymisierung erfolgt 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. Über das Tor-Netzwerk erfolgt der Zugang zum sogenannten Darknet. Zugang und Erreichbarkeit der Darknet-Angebote sind durch das Erfordernis besonderer Programme, wie des Tor-Browsers, beschränkt.

Die Angebote im Darknet umfassen, wie auch auf andere Weise zugangsbeschränkte Dienste, neben Foren für Whistleblower oder Chatrooms für politisch Verfolgte in autoritär geführten Staaten auch Inhalte bekannter Servicebetreiber. Ebenso finden sich jedoch Angebote mit strafrechtlicher Relevanz, darunter Handel mit Betäubungsmitteln, Kinderpornographie oder Waffen, mit Schadsoftware und Ausweispapieren. Vergleichbare Angebote finden sich auch in weiteren Bereichen des Internets.

Die Zentralstellen für die Verfolgung von Cybercrime der Länder haben in den vergangenen Jahren zahlreiche Ermittlungsverfahren mit überwiegend internationalen Bezügen geführt und einschlägige Foren sowie Handelsplattformen schließen können. In der Praxis zeigt sich jedoch, dass Anbieter und Kunden ihre Aktivitäten mit allenfalls geringem zeitlichem Verzug über alternative Plattformen fortführen. Die Verfahren lassen im Übrigen durchweg ein arbeitsteiliges Zusammenwirken von Plattformbetreibern und Nutzern der Plattform, also sowohl Händlern als auch Käufern, erkennen. Die Erfahrungen zeigen zudem, dass die klassischen Organisationsdelikte und die historischen gesetzgeberischen Vorstellungen von Täterschaft und Teilnahme auf moderne, internetbasierte Täterstrukturen kaum übertragbar sind. Die Betreiber selbst stellen lediglich eine technische Infrastruktur zur Verfügung. Ihr Verdienst entsteht durch Werbung oder einen Treuhand-Service im Rahmen der Zahlungsverwicklung.

Das Kriminalitätsphänomen beschränkt sich auch nicht auf wenige Einzelfälle. Bereits im Jahr 2016 waren dem Bundeskriminalamt circa 50 einschlägige Plattformen bekannt (vgl. Bundestagsdrucksache 18/9487, S. 2). Das dort betriebene Geschäftsmodell des „Cybercrime-as-a-Service“ wird in der kriminellen Szene weiter ausgebaut (vgl. Lagebild Cybercrime des Bundeskriminalamtes 2016, abrufbar unter [www.bka.de](http://www.bka.de), dort S. 16 ff.). Illegale Online-Handelsplattformen stellen aus Sicht von EUROPOL eine der zentralen Schnittstellen von Cybercrime und weiteren Formen – auch organisierter – Kriminalität dar (vgl. Internet Organised Crime Threat Assessment 2017, abrufbar unter [www.europol.eu](http://www.europol.eu)). Gegenüber den bereits etablierten Handelsgütern, wie zum Beispiel Betäubungsmitteln, sei eine deutliche Zunahme bei Angeboten von Hackertools und -dienstleistungen zu verzeichnen. Diese Aspekte hat auch die Europäische Kommission in der gemeinsamen Mitteilung mit der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik an das Europäische Parlament und den Rat „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“ vom 13. September 2017 betont und auf das derzeit nur geringe Risiko der Tatentdeckung hingewiesen (JOIN(2017) 450, dort S. 18).

In der strafrechtlichen Praxis stellt sich das Problem, dass eine Beihilfe gemäß § 27 StGB zu den über die Plattform begangenen Straftaten oft nicht nachweisbar ist, da die Haupttaten bilateral zwischen den Beteiligten über verschlüsselte Kommunikationskanäle abgewickelt werden, jedenfalls aber nicht offen im Forum sichtbar sind. Zudem sind bei vielen Foren die Arten von Straftaten, die über sie abgewickelt werden sollen, zu Beginn nicht klar definiert. Die Täter stellen eine informationstechnische Struktur zur Verfügung und wissen um die strafrechtliche Relevanz der über den Dienst abgewickelten Geschäfte. Welche Art von Gütern konkret gehandelt wird,

spielt für die Täter dabei keine Rolle. Moderne Foren verfügen zudem häufig über vollautomatisierte Verkaufssysteme, bei denen eine Beihilfe zu einer konkreten Haupttat noch schwieriger nachzuweisen ist. Ungeachtet dessen erfasst die strafrechtliche Ahndung unter dem Gesichtspunkt der Beihilfe in der Regel nicht hinreichend den aktiven Charakter der Tathandlung, die die Grundlagen der Underground Economy schafft.

Auch eine Zurechnung von Einzeltaten unter dem Gesichtspunkt einer bandenmäßigen Tatbegehung ist häufig nicht möglich, da in der Regel kriminelle Foren und Marktplätze der Underground Economy von nur einer Person oder zwei Personen geführt werden. Bei Foren und Marktplätzen mit mehreren Personen in der Führungsebene ist überdies zu berücksichtigen, dass sich die Betreiber regelmäßig nicht persönlich kennen und oftmals kein übergeordnetes, homogenes Interesse vorliegt. Ist im Einzelfall eine Bande im strafrechtlichen Sinne anzunehmen, ist im Weiteren für jede einzelne Tat nach den allgemeinen Kriterien festzustellen, ob sich die anderen Bandenmitglieder hieran als Mittäter, Anstifter oder Gehilfen beteiligt oder ob sie gegebenenfalls überhaupt keinen strafbaren Tatbeitrag geleistet haben. Letzteres kann insbesondere dann in Betracht kommen, wenn einzelne Betreiber nur für die Aufrechterhaltung und Wartung der technischen Infrastruktur oder die Administration nicht strafrechtlich relevanter Bereiche zuständig sind und glaubhaft versichern, keine Kenntnis von oder jedenfalls kein Interesse an den über das Forum abgeschlossenen oder angebotenen illegalen Verkaufstätigkeiten gehabt zu haben. In derartigen Konstellationen kommt auch die Annahme eines uneigentlichen Organisationsdelikts durch den Aufbau und die Aufrechterhaltung eines auf Straftaten ausgerichteten Geschäftsbetriebs regelmäßig nicht in Betracht.

Eine effektive Strafverfolgung kommt schließlich auch unter dem Gesichtspunkt der Bildung einer kriminellen Vereinigung im Sinne des § 129 StGB nicht stets in Betracht. Die Anforderungen an den Nachweis konkreter Einzeltaten sind bei dem abstrakten Gefährdungsdelikt zwar erleichtert, in der Regel wird jedoch die für den Tatbestand erforderliche Festigkeit der Struktur nicht erreicht. Dies gilt ungeachtet der durch das 54. Gesetz zur Änderung des Strafgesetzbuches – Umsetzung des Rahmenbeschlusses 2008/841/JI des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität vom 17. Juli 2017 (BGBl. I S. 2440) erfolgten Ausweitung des Vereinigungsbegriffs im Sinne des § 129 Absatz 2 StGB, denn Voraussetzung einer Vereinigung ist weiterhin ein organisierter Zusammenschluss. Dies erfordert zumindest eine gewisse Organisationsstruktur sowie eine instrumentelle Vorausplanung und Koordinierung. Zusammenschlüsse, die sich zufällig zur unmittelbaren Begehung einer Straftat bilden, wie dies bei den hier relevanten Cyberstrukturen oft der Fall ist, dürften dem Vereinigungsbegriff des § 129 Absatz 2 StGB nicht unterfallen.

Weil der Zugang zu den einschlägigen Angeboten in der Regel keinen besonderen technischen Anforderungen unterliegt und die Erreichbarkeit zwar beschränkt, aber ohne erheblichen technischen Aufwand möglich ist, bieten die Handelsplattformen somit einen niedrighwelligen Zugriff auf logistische Infrastrukturen für die Begehung von Straftaten auch für Personen, die herkömmliche Beschaffungswege für Waffen, Betäubungsmittel oder kriminelle Dienstleistungen nicht beschreiten. Diese Angebote erhöhen durch die Verbreitung des illegalen Angebots gezielt die Gefahren für die durch das Verbot der Waren und Dienstleistungen geschützten Rechtsgüter und stellen damit eine darüber hinausgehende eigenständige erhebliche Gefahr für die öffentliche Sicherheit dar, ohne dass es nach der geltenden Rechtslage ausreichende Möglichkeiten für eine angemessene strafrechtliche Verfolgung gibt.

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 Telemedienangeboten mit kinderpornografischen Inhalten im Sinne des § 184b StGB 84 Prozent der dem Bundeskriminalamt im Jahr 2017 gemeldeten Internetseiten mit kinderpornographischen Inhalten im Ausland gehostet.

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 retrogrades 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.

Die im Strafrecht bestehende Lücke soll durch die Einführung einer neuen Vorschrift geschlossen werden. Der Entwurf zielt darauf, das Betreiben von auf die Förderung 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 Begehung von Straftaten erfassen, zum Beispiel § 29 Absatz 1 Nummer 10 BtMG, regelt § 126a StGB-E den Sonderfall der Tatbegehung mittels internetbasierter Leistungen. Dem Konkurrenzverhältnis wird insoweit durch eine Subsidiaritätsklausel in § 126a Absatz 1 Satz 1 StGB-E Rechnung getragen.

Im Sinne einer aus Gründen der Verhältnismäßigkeit angezeigten Beschränkung erfasst § 126a StGB-E nur bestimmte, als für das geschützte Rechtsgut besonders gefährlich einzustufende szenetypische Delikte im Sinne des § 126a Absatz 1 Satz 2 StGB-E. Die dort genannten Delikte bergen aufgrund der Gefährlichkeit der gehandelten Waren und Dienstleistungen bereits für sich eine besondere Gefahr für die öffentliche Sicherheit. Diese Gefahr wird durch die Begehung mittels internetbasierter Leistungen erheblich erhöht, da die Angebote 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.

Die Vorschrift beschränkt sich auf einen bestimmten Ausschnitt des kriminellen Online-Handels. Erfasst werden nur durch technische Vorkehrungen hinsichtlich Zugang und Erreichbarkeit beschränkte Angebote. Zugangs- und Erreichbarkeitsbeschränkungen können sich etwa durch die beschriebene Nutzung des Tor-Browsers im Darknet oder bei ähnlichen Zugangsbeschränkungen, zum Beispiel durch vor Zulassung erforderliche Keuschheitsproben, ergeben. 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.

Im Zusammenspiel mit den zum 1. Juli 2017 durch das Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung vom 13. April 2017 (BGBl. I S. 872) neu gefassten Abschöpfungsvorschriften sichert die Einführung des neuen Tatbestands zudem die effektive Bekämpfung auch der wirtschaftlichen Grundlagen der Underground Economy.

Der Grundtatbestand des § 126a Absatz 1 StGB-E ist aufgrund der wertungsmäßig einer Beteiligung entsprechenden Begehungsart und der Vorverlagerung der Strafbarkeit mit Geldstrafe oder Freiheitsstrafe von bis zu drei Jahren bedroht. Bei erhöhten Strafdrohungen in anderen Tatbeständen, zum Beispiel § 29 Absatz 1 Nummer 10 BtMG, greift die Subsidiaritätsklausel des § 126a Absatz 1 Satz 1 StGB-E. Aus Gründen der Verhältnismäßigkeit begrenzt § 126a Absatz 2 StGB-E die Strafdrohung auf die für die Katalogtat im Sinne von § 126a Absatz 1 Satz 2 StGB-E angedrohte Strafe. Neben dem Grundtatbestand sieht § 126a Absatz 3 StGB-E bei gewerbsmäßiger 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 zur Mehrung des eigenen Ansehens in der Szene bereit. Das Kriterium der Gewerbsmäßigkeit rechtfertigt daher die in der Qualifikation vorgesehene höhere Strafdrohung.

Die erhöhte Strafdrohung verdeutlicht überdies, dass die Qualifikation des § 126a Absatz 3 StGB-E dem Bereich der schweren Kriminalität zuzurechnen ist. Dies begründet in Verbindung mit den Besonderheiten der Tatbegehung mittels internetbasierter Leistung die Aufnahme des Qualifikationstatbestands in den Katalog der Ermittlungsmaßnahme des § 100a Absatz 2 Nummer 1 Buchstabe d StPO. Die Ermittlungen wegen eines ausschließlich den Grundtatbestand des § 126a Absatz 1 StGB-E erfüllenden Sachverhalts dürften zwar ohne die technischen Überwachungsmaßnahme des § 100a StPO nachhaltig erschwert werden, aus Gründen der Verhältnismäßigkeit ist jedoch die Aufnahme nur der Qualifikation sachgerecht.

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 den §§ 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.

## **II. Gesetzgebungskompetenz**

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes.

## **III. Auswirkungen**

Durch die Ausweitung der Strafbarkeit kann ein Mehraufwand für die Strafverfolgungsbehörden entstehen, dessen Umfang derzeit nicht quantifizierbar ist. Im Übrigen werden jedoch keine Mehrkosten entstehen. Für Bürgerinnen und Bürger und die Unternehmen entsteht kein Erfüllungsaufwand.

### **B. Zu den einzelnen Vorschriften**

#### **Zu Artikel 1 (Änderung des Strafgesetzbuches)**

##### **Zu Nummer 1 (Inhaltsübersicht zu § 126a StGB-E)**

Infolge der Einfügung eines neuen § 126a StGB in das Gesetz ist die Inhaltsübersicht entsprechend anzupassen.

##### **Zu Nummer 2 (§ 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.

### **Zu Nummer 3 (§ 126a StGB-E)**

#### **Zu Absatz 1**

Der besonderen Gefährlichkeit des Betriebens von zugangsbeschränkten, insbesondere Darknet-Angeboten, die sich ohne zeitliche, sachliche oder räumliche Grenzen an Personen jeden Alters richten, gegenüber anderen Online-Angeboten wird durch die Fokussierung des Tatbestands auf internetbasierte Leistungen Rechnung getragen, die typischerweise besonderen technischen Beschränkungen hinsichtlich des Zugangs und der Erreichbarkeit unterliegen, zum Beispiel der Nutzung des Tor-Browsers oder vergleichbarer Anforderungen. Das Erfordernis einer bloßen Zugangskennung zur Nutzung einer Leistung, ohne weitere Einschränkung, erfüllt die Anforderungen an eine besondere technische Vorkehrung nicht. Von einer technikoffenen Erfassung aller in Betracht kommenden Kommunikationsmittel, die eingesetzt werden könnten, ohne dass die Beteiligten gleichzeitig körperlich an einem bestimmten Ort anwesend sind, zum Beispiel offene Internetplattformen und -foren, Telemedien, E-Mails und Mobilfunkkontakten, wird aus Gründen der Begrenzung der Strafbarkeit abgesehen.

Der Begriff der Leistung beschreibt alle Angebote, die sich an einen oder mehrere Nutzer richten, ohne stets auf Dauer und wiederholte Nutzung abzielen. 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 des Angebots im Sinne des § 126a Absatz 1 StGB-E muss das Ermöglichen oder die Förderung von Taten im Sinne des Satzes 2 sein, die eine besondere Gefahr für den Rechtsfrieden darstellen. 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. 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.

Im Sinne einer aus Gründen der Verhältnismäßigkeit angezeigten Beschränkung erfasst § 126a StGB-E nur bestimmte, als für das geschützte Rechtsgut besonders gefährlich einzustufende szenetypische Delikte im Sinne des § 126a Absatz 1 Satz 2 StGB-E. Die dort genannten Tatbestände bergen aufgrund der Gefährlichkeit der gehandelten Waren und Dienstleistungen bereits für sich eine besondere Gefahr für die öffentliche Sicherheit. Die Erfahrungen in der Praxis zeigen, dass Schwerpunkte des illegalen Online-Handels die Bereiche Betäubungsmittel, Waffen, Falschgeld bzw. gefälschte Urkunden, Kinderpornographie und Cyberwerkzeuge, insbesondere Hacker-Programme, sind.

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. Der Bereich der Cyberwerkzeuge wird durch die in § 126a Absatz 1 Satz 2 Nummer 7 StGB-E genannten Delikte der §§ 202a, 202b, 202c, 303a und 303b StGB abgedeckt. So 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 gekapertter Drittrechner, die unter Täterkontrolle koordinierte Überlastangriffe auf legitime Webseiten und -services durchführen.

Die Begrenzung der Anknüpfungsdelikte auf als besonders gefährlich eingestufte szenetypische Delikte erleichtert die Abgrenzung zu den nicht dem Tatbestand unterfallenden legalen Handelsplattformen. Überdies werden so mögliche Abgrenzungsprobleme im Bereich der beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 StPO genannten Personen vermieden. Besonderer tatbestandsausschließender Regelungen, wie etwa in § 202d Absatz 3 StGB, bedarf es nicht.

### **Zu Absatz 2**

Aus Gründen der Verhältnismäßigkeit begrenzt § 126a Absatz 2 StGB-E die Strafdrohung auf die für die Katalogtat im Sinne von § 126a Absatz 1 Satz 2 StGB-E angedrohte Strafe. Dieses Vorgehen orientiert sich an den Regelungen in vergleichbaren Vorschriften, zum Beispiel die §§ 202d Absatz 2, 257 Absatz 2, 258 Absatz 3 StGB. Relevant werden kann diese Regelung angesichts der Strafdrohungen der Katalogtaten für die in § 126a Absatz 1 Satz 2 Nummer 7 StGB-E genannten Fälle der §§ 149, 202b, 202c, 275, 276 und 303a StGB. Die übrigen Taten enthalten jeweils Höchststrafdrohungen von mindestens drei Jahren Freiheitsstrafe.

### **Zu Absatz 3**

Neben dem Grundtatbestand sieht § 126a Absatz 3 StGB-E bei gewerbsmäßiger 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 zur Mehrung des eigenen Ansehens in der Szene bereit. 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 schweren Kriminalität zuzurechnen ist.

Der Strafrahmen orientiert sich auf Grundlage der erhöhten kriminellen Energie von auf Dauer angelegten, gewinnorientierten Strukturen an denen für vergleichbare Delikte bei gewerbsmäßiger Begehungsweise, zum Beispiel § 260 Absatz 1 Nummer 1 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 Ausstrahlungswirkung im Bereich des Cybercrime zukommt.

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

#### **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 Postdienstleiters 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 Ermittlungsrichters des Bundesgerichtshofs vom 11. Juli 2012 (3 BGs 211/12, BeckRS 2014, 05922) für Auskunftsverlangen über bereits ausgelieferte Sendungen (retrogrades 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 Postdienstleiters 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-E)**

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 eingriffsintensiver Ermittlungsmaßnahmen für alle Fälle der Informations- und Kommunikationskriminalität. Mit Blick auf das durch Maßnahmen gemäß § 100a StPO betroffene Grundrecht aus Artikel 10 des Grundgesetzes 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 (vgl. BVerfG NJW 2012, 833 – Rnr. 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 im Falle gewerbsmäßigen Handelns weist gegenüber dem Grundtatbestand aufgrund der auf Dauer ausgelegten Tatbegehung zur Erzielung einer nicht nur vorübergehenden Einnahmequelle einen deutlich gesteigerten Unrechtsgehalt auf, der auch in anderen Delikt Bereichen zu einer erhöhten Strafdrohung führt, zum Beispiel § 260 Absatz 1 Nummer 1 StGB. Damit werden die Gefahren für die bereits durch den Grundtatbestand und die Katalogtaten geschützten Rechtsgüter weiter und dauerhaft erhöht. In diesen Fällen, in denen ein Täter nicht nur gelegentlich oder ohne eigennütziges finanzielles Interesse gezielt Strukturen der kriminellen Infrastruktur schafft, handelt es sich demnach bereits um einen schwere Straftat im Sinne des § 100a StPO.

#### **Zu Artikel 3 (Inkrafttreten)**

Die Vorschrift regelt das Inkrafttreten des Gesetzes.

## Anlage 2

### Stellungnahme der Bundesregierung

Die Bundesregierung nimmt zu dem Gesetzentwurf des Bundesrates wie folgt Stellung:

#### **Zu Artikel 1 (Änderung des Strafgesetzbuches)**

Die Bundesregierung ist der Auffassung, dass es möglich sein muss, auch Straftaten, die unter Nutzung des Internets begangen werden, effektiv zu verfolgen. Der Koalitionsvertrag von CDU, CSU und SPD für die 19. Legislaturperiode sieht vor, dort, wo Strafbarkeitslücken bestehen, eine Strafbarkeit für das Betreiben krimineller Infrastrukturen einzuführen, um speziell im Internet eine Ahndung von Delikten wie z. B. das Betreiben eines Darknet-Handelsplatzes für kriminelle Waren und Dienstleistungen zu ermöglichen. Die Bundesregierung prüft derzeit, inwiefern konkrete Sachverhalte von der geltenden Gesetzeslage nicht oder nicht ausreichend strafrechtlich erfasst werden und wie etwaige Strafbarkeitslücken geschlossen werden können. Gegenstand dieser Prüfung werden auch die vom Bundesrat vorgeschlagenen Änderungen des Strafgesetzbuches sein.

#### **Zu Artikel 2 (Änderung der Strafprozessordnung – StPO)**

##### **Zu Nummer 1 (Änderung des § 99 Absatz StPO)**

Die vorgeschlagene Erweiterung der Ermittlungsbefugnisse für die Postbeschlagnahme steht nicht in einem engen inhaltlichen Zusammenhang mit Artikel 1 des Gesetzentwurfs. Der Vorschlag entspricht einem Beschluss der Justizministerkonferenz aus dem Jahr 2017. Aufgrund einer geänderten Rechtsprechung des Bundesgerichtshofs haben sich Fragen bei der Postbeschlagnahme ergeben, die sich auf elektronische, beim Postdienstleister befindliche Informationen über die Postsendung beziehen und bei denen umstritten ist, ob und auf welche Weise sie von den Strafverfolgungsbehörden beschlagnahmt werden können. Die Bundesregierung prüft derzeit die Vorlage eines eigenen Gesetzentwurfes zu diesem Thema.

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

Dieser Vorschlag des Bundesrates wird Gegenstand der oben zu Artikel 1 beschriebenen Prüfung der Bundesregierung sein.