Entwurf eines Strafrechtsänderungsgesetzes -
Gesetz zur Verbesserung der Bekämpfung der Cyberkriminalität
(Stand 5. April 2019)

A. Problem und Ziel

Die fortschreitende Digitalisierung, insbesondere die immer stärkere Nutzung des Internets, wirkt sich in allen Bereichen von Staat, Wirtschaft und Gesellschaft aus. Sie bringt neben großen Potentialen und Freiräumen aufgrund vielfältiger Missbrauchsmöglichkeiten auch ein neues Maß an Verwundbarkeit. Diese Verwundbarkeit nutzen insbesondere sogenannte Hacker aus, die immer häufiger fremde Computersysteme infiltrieren und dabei auch immer größere Mengen an sensiblen Daten unbefugt abgreifen, manipulieren oder zerstören sowie diese Daten für weitere Straftaten missbrauchen.

Die bekannt gewordenen "Datenleaks" der letzten Jahre verdeutlichen dabei die enorme Dimension, die diese Datenabgriffe inzwischen erlangt haben. So wurden bei MySpace 360 Mio. Datensätze, bei Sony 102 Mio. Datensätze, bei Dropbox 69 Mio. Datensätze, bei LinkedIn 177 Mio. Datensätze, bei Yahoo 500 Mio. Datensätze und bei Ashley Madison 36 Mio. Datensätze unbefugt abgegriffen. Eine im Januar 2019 bekanntgewordene Sammlung von Passwort-Leaks enthielt bei einem Volumen von 935 Gigabyte über 2,2 Milliarden Accounts. Bundesweites Aufsehen erregte Ende des Jahres 2018/Anfang 2019 die Meldung, dass ein Hacker mit offenbar einfachen Mitteln massenhaft persönliche Daten von mehreren hundert Politikern, Prominenten und Journalisten ausgespäht und auf der Internetplattform Twitter verbreitet hatte. Neben diesen "Datenleaks" kam es zuletzt auch vermehrt zu Cyberattacken, bei denen Verschlüsselungstrojaner (sog. Ransomware) in die IT-Infrastruktur von Unternehmen oder Krankenhäusern eingeschleust wurden, die dort zu massiven Betriebsstörungen und Schäden führten.

Diese aktuellen Vorfälle zeigen, dass die Cyberkriminalität inzwischen ein Ausmaß erreicht hat, das die Privatsphäre und das Sicherheitsgefühl der Menschen massiv bedroht und das Potential hat, die Grundlagen von Demokratie, Staat und Wirtschaft zu gefährden. Die Cyberkriminalität ist geeignet, das Vertrauen in die

Handlungsfähigkeit staatlicher Organe und in den Rechtsstaat nachhaltig zu beeinträchtigen. Die wirtschaftlichen Schäden, die etwa durch Produktionsausfälle, den Verlust von Geschäftsgeheimnissen oder die Kosten für eine Wiederherstellung von Daten entstehen, sind groß. Gleiches gilt für die negativen Folgen, die für den Einzelnen oder staatliche Institutionen mit der Veröffentlichung sensibler Informationen verbunden sein können. Im Extremfall können Cyberangriffe etwa auf Krankenhäuser, Flughäfen oder Verteidigungseinrichtungen sogar den Verlust von Menschenleben fordern.

Es ist Aufgabe des Strafrechts, die für solche Angriffe verantwortlichen Personen zügig zu ermitteln und schuldangemessen zu bestrafen - nicht zuletzt um andere potentielle Täter abzuschrecken, die Gesellschaft zu schützen und das Vertrauen in die staatliche Handlungsfähigkeit zu erhalten. Diese Aufgabe kann das Strafrecht derzeit jedoch nur bedingt erfüllen.

Der materiell-strafrechtliche Schutz vor Delikten aus dem Phänomenbereich der Cyberkriminalität, der gegenwärtig im Wesentlichen durch die §§ 202a ff., §§ 303a f. StGB gewährt wird, ist unzureichend. Digitale Daten sind de lege lata strafrechtlich nicht vergleichbar geschützt wie körperliche Gegenstände, da die Computer- und Datendelikte im Gegensatz zu den klassischen Eigentums- und Vermögensdelikten (wie Diebstahl oder Betrug) ganz überwiegend als "Bagatellkriminalität" ausgestaltet sind. So liegen die Strafrahmen der §§ 202a ff., 303a f. StGB ganz überwiegend im unteren Bereich. Zudem fehlt es - anders als bei den klassischen Deliktsbereichen - auch weitgehend an Qualifikationstatbeständen und Regelbespielen mit erhöhten Strafdrohungen, um auf schwerwiegende Taten mit einem gesteigerten Unrechtsgehalt tat- und schuldangemessen reagieren zu können.

Dies hat zur Folge, dass beispielsweise ein Hacker, der sich unbefugt Zugang zu einer Datenbank verschafft und dabei mehrere Millionen Datensätze abgreift, derzeit lediglich eine Freiheitsstrafe von maximal drei Jahren oder eine Geldstrafe zu befürchten hat - selbst wenn er gewerbsmäßig handelt und große Schäden für den Einzelnen oder das Gemeinwesen verursacht. Auch können Firmen als Opfer eines Angriffs existentiell betroffen sein, wenn beispielsweise die gesamte Kundendatenbank oder wichtige Betriebsgeheimnisse ausgespäht werden. Datenabgriffe dieses Ausmaßes, die infolge der heutigen technischen Möglichkeiten immer leichter möglich werden und das Vertrauen großer Teile der Bevölkerung in die Sicherheit der

modernen Informationstechnologie beeinträchtigen, entsprechen ersichtlich nicht mehr dem, was der Gesetzgeber im Blick hatte, als er 1986 im Zeitalter der Magnetbänder und Disketten das Ausspähen von Daten in § 202a StGB unter Strafe stellte.

Die Bagatellisierung der Computer- und Datendelikte im materiellen Strafrecht setzt sich im Strafprozessrecht fort. Denn beim Verdacht einer Straftat nach den §§ 202a ff., §§ 303a f. StGB können derzeit häufig die Täter nicht ermittelt und überführt werden, weil den Strafverfolgungsbehörden die strafprozessualen Befugnisse für erfolgversprechende Ermittlungen in der digitalen Welt nicht oder nur eingeschränkt zur Verfügung stehen. So ist eine Überwachung der Telekommunikation in Form der „Serverüberwachung“ oder eine Online-Durchsuchung zur Identifizierung der Täter, zur Aufhellung der verwendeten Infrastruktur und zum Führen des Tatnachweises mangels Vorliegens einer Katalogtat nach § 100a Absatz 2 bzw. § 100b Absatz 2 StPO derzeit rechtlich nicht zulässig. Die Erhebung von Verkehrsdaten ist de lege lata nur eingeschränkt nach § 100g Absatz 1 Satz 1 Nummer 2 StPO zulässig, mangels Vorliegens einer Katalogtat aber nicht nach § 100g Absatz 1 Satz 1 Nummer 1 oder § 100g Absatz 2 StPO. Diese technischen Ermittlungsmaßnahmen stellen aber oftmals den einzig erfolgversprechenden Ermittlungsansatz dar, da die Delikte der Cyberkriminalität in den allermeisten Fällen auch oder ausschließlich unter Zuhilfenahme von Telekommunikationsdiensten begangen werden.

Die geschilderten Defizite im materiellen Strafrecht und Strafprozessrecht werden weder der gesellschaftlichen und wirtschaftlichen Bedeutung digitaler Daten noch der Bedeutung des Grundrechts auf informationelle Selbstbestimmung in der heutigen digitalen Welt gerecht.

Vor diesem Hintergrund hat der Strafrechtsausschuss der Justizministerkonferenz und der Arbeitskreis II der Innenministerkonferenz die Gemeinsame Arbeitsgruppe Justiz/Polizei (GAG) bereits im Jahr 2011 beauftragt, sich unter anderem mit dem Thema Cybercrime zu befassen. Die Unterarbeitsgruppe "Cybercrime" unter Federführung des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz hat sich mit den aktuellen Rechtsfragen bei der Bekämpfung von Cybercrime befasst und in ihrem 2013 vorgelegten Abschlussbericht u.a. die Schaffung qualifizierter Begehungsweisen für den Bereich der Computerdelikte empfohlen.

Zuletzt hat sich im Jahr 2018 die durch die Justizministerkonferenz eingesetzte und unter dem Vorsitz Hessens arbeitende Länder-Arbeitsgruppe „Digitale Agenda für das Straf- und Strafprozessrecht“ in ihrem Abschlussbericht mit der Thematik der Bagatellisierung der Cyberkriminalität befasst und gesetzgeberischen Handlungsbedarf gesehen. Die Justizministerinnen und Justizminister der Länder haben auf ihrer Herbstkonferenz am 15. November 2018 den Abschlussbericht der Arbeitsgruppe des Strafrechtsausschusses „Digitale Agenda für das Straf- und Strafprozessrecht“ als Bestandsaufnahme der sich aus der technischen Entwicklung für die Strafverfolgungspraxis ergebenden Anforderungen und als Beitrag zur rechtspolitischen Diskussion zur Kenntnis genommen. Außerdem haben sie die Bundesministerin der Justiz und für Verbraucherschutz darum gebeten, die in dem Bericht enthaltenen Empfehlungen der Arbeitsgruppe zu würdigen und die ggf. erforderlichen gesetzgeberischen Schritte zu unternehmen.

.

B. Lösung

Der Entwurf beseitigt die unangemessene Bagatellisierung der Computer- und Datendelikte, indem er die Strafrahmen der §§ 202a ff., 303a f. StGB an die heutige digitale Welt anpasst und dabei insbesondere auch Qualifikationstatbestände und Regelbeispiele mit erhöhten Strafdrohungen schafft, um den differenzierten Unrechtsgehalt der in Betracht kommenden Fallgestaltungen sachgerecht erfassen zu können. Daneben führt er bei den §§ 202a, 202b und 202d StGB auch eine Versuchsstrafbarkeit ein, um den Rechtsgutsschutz rechtzeitig beginnen zu lassen.

Ferner verbessert der Entwurf die Möglichkeiten der Täterermittlung und Sachverhaltsaufklärung, indem er unter Wahrung der Vorgaben des Bundesverfassungsgerichts die Straftatkataloge der §§ 100a Absatz 2, 100b Absatz 2 und 100g Absatz 2 StPO um bestimmte, qualifizierte Begehungsweisen der Cybercrime-Delikte ergänzt und damit den Anwendungsbereich der Telekommunikationsüberwachung, Online-Durchsuchung und Verkehrsdatenerhebung an die Bedürfnisse einer effektiven Strafverfolgung anpasst. Der Entwurf trägt damit dem Umstand Rechnung, dass die Strafverfolgungsbehörden bei Delikten in der digitalen Welt darauf angewiesen sind, auch digital ermitteln zu können.

C. Alternativen

Beibehaltung des bisherigen, unbefriedigenden Zustands.

D. Haushaltsaufgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Keiner.

Davon Bürokratiekosten aus Informationspflichten.

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Keiner.

F. Weitere Kosten

Die vorgeschlagenen Neuregelungen im materiellen Strafrecht und die Erweiterung des Anwendungsbereichs der technischen Ermittlungsmaßnahmen können zu einem Mehraufwand für Polizei und Justiz führen, dessen Umfang derzeit noch nicht quantifizierbar ist. Der Mehraufwand ist angesichts des verbesserten Rechtsgüterschutzes gerechtfertigt.

Entwurf eines Strafrechtsänderungsgesetzes -
Gesetz zur Verbesserung der Bekämpfung der Cyberkriminalität

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Strafgesetzbuchs

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

1. § 202a wird wie folgt geändert:

   a) In Absatz 1 wird das Wort "drei" durch das Wort "fünf" ersetzt.

   b) Nach Absatz 2 werden folgende Absätze 3 bis 5 neu eingefügt:

      "(3) Der Versuch ist strafbar.

      (4) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe von drei Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

         1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat,

         2. eine große Menge von Daten ausspäht oder in der Absicht handelt, durch die fortgesetzte Begehung von Taten nach Absatz 1 Daten einer großen Anzahl von Personen auszuspähen,

3. Daten kritischer Infrastrukturen ausspäht oder durch die Tat die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet oder

4. Daten ausspäht, die den höchstpersönlichen Lebensbereich berühren.

(5) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, wird bestraft, wer in den Fällen des Absatzes 4 Satz 2 Nummer 1 erste Alternative oder Nummern 2 bis 4 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat."

2. § 202b wird wie folgt geändert:

a) Der bisherige § 202b wird § 202b Absatz 1. Zugleich wird im bisherigen § 202b das Wort "zwei" durch das Wort "drei" ersetzt.

b) Nach Absatz 1 werden folgende Absätze 2 bis 4 neu eingefügt:

"(2) Der Versuch ist strafbar.

(3) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat,

2. eine große Menge von Daten abfängt oder in der Absicht handelt, durch die fortgesetzte Begehung von Taten nach Absatz 1 Daten einer großen Anzahl von Personen abzufangen,

3. Daten kritischer Infrastrukturen abfängt oder durch die Tat die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet oder

4. Daten abfängt, die den höchstpersönlichen Lebensbereich berühren.

(4) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren, wird bestraft, wer in den Fällen des Absatzes 3 Satz 2 Nummer 1 erste Alternative oder Nummern 2 bis 4 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat."

3. § 202c StGB wird wie folgt geändert:

a) In Absatz 1 wird das Wort ",verbreitet" gestrichen und
das Wort "zwei" durch das Wort "drei" ersetzt.

b) Nach Absatz 2 werden folgende Absätze 3 und 4 neu eingefügt:

"(3) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat, oder

2. die in Absatz 1 genannten Sicherungscodes und Computerprogramme einer großen Anzahl von Personen zugänglich macht.

(4) Mit Freiheitsstrafe von drei Monaten bis zu zehn Jahren wird bestraft, wer in den Fällen des Absatzes 3 Satz 2 Nummer 1 erste Alternative oder Nummer 2 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat."

4. § 202d StGB wird wie folgt gefasst:

   a) In Absatz 1 wird das Wort ",verbreitet" gestrichen und das Wort "drei" durch das Wort "fünf" ersetzt und.

   b) Nach Absatz 1 werden folgende Absätze 2 bis 4 neu eingefügt:

      "(2) Der Versuch ist strafbar.

      (3) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

         1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat,

         2. die Datenhehlerei einer großen Menge von Daten oder in der Absicht begeht, durch die fortgesetzte Tatbegehung sich oder einem anderen die Daten einer großen Anzahl von Personen zu verschaffen oder die Daten einer großen Anzahl von Personen zugänglich zu machen,

         3. die Datenhehlerei von Daten kritischer Infrastrukturen begeht oder durch die Tat die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet oder

         4. die Datenhehlerei von Daten begeht, die den höchstpersönlichen Lebensbereich berühren.

      (4) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, wird bestraft, wer in den Fällen des Absatzes 3 Satz 2 Nummer 1 erste Alternative oder Nummern 2 bis 4 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat."

c) Der bisherige Absatz 2 wird Absatz 5; der bisherige Absatz 3 wird Absatz 6.

5. § 205 wird wie folgt geändert:

a) In § 205 Absatz 1 Satz 2 wird hinter den Angaben "202a", "202b" und "202d" jeweils die Angabe "Abs. 1" eingefügt.

b) In § 205 Absatz 2 Satz 1 werden die Wörter "; dies gilt nicht in den Fällen der §§ 202a, 202b und 202d" gestrichen.

6. § 303a wird wie folgt geändert:

a) Nach Absatz 2 werden die folgenden Absätze 3 und 4 neu eingefügt:

"(3) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat,

2. die Datenveränderung einer großen Menge von Daten oder in der Absicht begeht, durch die fortgesetzte Tatbegehung die Daten einer großen Anzahl von Personen zu löschen, zu unterdrücken, unbrauchbar zu machen oder zu verändern,

3. die Datenveränderung von Daten kritischer Infrastrukturen begeht oder durch die Tat die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet, oder

4. die Datenveränderung von Daten begeht, die den höchstpersönlichen Lebensbereich berühren.

(4) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren, wird bestraft, wer in den Fällen des Absatzes 3 Satz 2 Nummer 1 erste Alternative oder Nummern 2 bis 4 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat."

b) Der bisherige Absatz 3 wird Absatz 5.

7. § 303b wird wie folgt geändert:

a) Absatz 4 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter "des Absatzes 2" durch die Wörter "der Absätze 1 und 2" ersetzt.

bb) In Satz 2 Nummer 1 werden nach dem Wort "herbeiführt" die Wörter "oder in der Absicht handelt, durch die fortgesetzte Begehung von Computersabotage eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen" eingefügt.

cc) In Satz 2 Nummer 2 wird das Wort "Computersabotage" durch die Wörter "Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b" ersetzt.

dd) Satz 2 Nummer 3 wird wie folgt neu gefasst:
"durch die Tat die Datenverarbeitung einer kritischen Infrastruktur erheblich stört oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet."

b) Nach Absatz 4 werden die folgenden Absätze 5 und 6 neu eingefügt:

"(5) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, wird

bestraft, wer in den Fällen des Absatzes 4 Satz 2 Nummer 1, Nummer 2 erste Alternative oder Nummer 3 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat.

(6) Verursacht der Täter durch die Computersabotage wenigstens leichtfertig den Tod eines anderen Menschen, so ist die Strafe Freiheitsstrafe nicht unter drei Jahren, in minder schweren Fällen von einem Jahr bis zu zehn Jahren. Verursacht der Täter durch die Computersabotage wenigstens leichtfertig eine schwere Gesundheitsschädigung eines anderen Menschen, so ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen von sechs Monaten bis zu fünf Jahren."

c) Der bisherige Absatz 5 wird Absatz 7.

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. § 100a Absatz 2 Nummer 1 wird wie folgt geändert:

a) Nach Buchstabe g) wird folgender Buchstabe h) neu eingefügt:

"h) Computer- und Datendelikte nach §§ 202a, 202b Absatz 3 und 4, 202c Absatz 3 und 4, 202d, 303a Absatz 3 und 4, 303b Absatz 2 bis 6,"

b) Die bisherigen Buchstaben h) bis u) werden zu Buchstaben i) bis v).

2. § 100b Absatz 2 Nummer 1 wird wie folgt geändert:

a) Nach Buchstabe e) wird folgender Buchstabe f) neu eingefügt:

"f) Computer- und Datendelikte nach §§ 202a Absatz 4 und 5, 202b Absatz 4, 202c Absatz 4, 202d Absatz 3 und 4, 303a Absatz 4 und 303b Absatz 4 bis 6,"

b) Die bisherigen Buchstaben f) bis m) werden zu Buchstaben g) bis n).

3. § 100g Absatz 2 Satz 2 Nummer 1 wird wie folgt geändert:

a) Nach Buchstabe d) wird folgender Buchstabe e) neu eingefügt:

"e) Computer- und Datendelikte nach §§ 202a Absatz 4 und 5, 202b Absatz 4, 202c Absatz 4, 202d Absatz 3 und 4, 303a Absatz 4 und 303b Absatz 4 bis 6,"

b) Die bisherigen Buchstaben e) bis h) werden zu Buchstaben f) bis i).

Artikel 3

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung des Entwurfs und Notwendigkeit der Regelungen

Die fortschreitende Digitalisierung, insbesondere die immer stärkere Nutzung des Internets, wirkt sich in allen Bereichen von Staat, Wirtschaft und Gesellschaft aus. Sie bringt neben großen Potentialen und Freiräumen aufgrund vielfältiger Missbrauchsmöglichkeiten auch ein neues Maß an Verwundbarkeit. Diese Verwundbarkeit nutzen insbesondere sogenannte Hacker aus, die immer häufiger fremde Computersysteme infiltrieren und dabei auch immer größere Mengen an sensiblen Daten unbefugt abgreifen, manipulieren oder zerstören sowie diese Daten für weitere Straftaten missbrauchen.

Die bekannt gewordenen "Datenleaks" der letzten Jahre verdeutlichen dabei die enorme Dimension, die diese Datenabgriffe inzwischen erlangt haben. So wurden bei MySpace 360 Mio. Datensätze, bei Sony 102 Mio. Datensätze, bei Dropbox 69 Mio. Datensätze, bei LinkedIn 177 Mio. Datensätze, bei Yahoo 500 Mio. Datensätze und bei Ashley Madison 36 Mio. Datensätze unbefugt abgegriffen. Eine im Januar 2019 bekanntgewordene Sammlung von Passwort-Leaks enthielt bei einem Volumen von 935 Gigabyte über 2,2 Milliarden Accounts. Bundesweites Aufsehen erregte Ende des Jahres 2018/Ende 2019 die Meldung, dass ein Hacker mit offenbar einfachen Mitteln massenhaft persönliche Daten von mehreren hundert Politikern, Prominenten und Journalisten ausgespäht und auf der Internetplattform Twitter verbreitet hatte. Neben diesen "Datenleaks" kam es zuletzt auch vermehrt zu Cyberattacken, bei denen Verschlüsselungstrojaner (sog. Ransomware) in die IT-Infrastruktur von Unternehmen oder Krankenhäusern eingeschleust wurden, die dort zu massiven Betriebsstörungen und Schäden führten.

Diese aktuellen Vorfälle zeigen, dass die Cyberkriminalität inzwischen ein Ausmaß erreicht hat, das die Privatsphäre und das Sicherheitsgefühl der Menschen massiv bedroht und das Potential hat, die Grundlagen von Demokratie, Staat und Wirtschaft zu gefährden. Die Cyberkriminalität ist geeignet, das Vertrauen in die Handlungsfähigkeit staatlicher Organe und in den Rechtsstaat nachhaltig zu beeinträchtigen. Die wirtschaftlichen Schäden, die etwa durch Produktionsausfälle, den Verlust von Geschäftsgeheimnissen oder die Kosten für eine Wiederherstellung von Daten

entstehen, sind groß. Gleiches gilt für die negativen Folgen, die für den Einzelnen oder staatliche Institutionen mit der Veröffentlichung sensibler Informationen verbunden sein können. Im Extremfall können Cyberangriffe etwa auf Krankenhäuser, Flughäfen oder Verteidigungseinrichtungen sogar den Verlust von Menschenleben fordern.

Es ist Aufgabe des Strafrechts, die für solche Angriffe verantwortlichen Personen zügig zu ermitteln und schuldangemessen zu bestrafen - nicht zuletzt um andere potentielle Täter abzuschrecken, die Gesellschaft vor Cyberangriffen zu schützen und das Vertrauen in die staatliche Handlungsfähigkeit zu erhalten. Diese Aufgabe kann das Strafrecht derzeit jedoch nur bedingt erfüllen.

Der materiell-strafrechtliche Schutz vor Delikten aus dem Phänomenbereich der Cyberkriminalität, der gegenwärtig im Wesentlichen durch die §§ 202a ff., §§ 303a f. StGB gewährt wird, ist unzureichend. Digitale Daten sind de lege lata strafrechtlich nicht genauso geschützt wie körperliche Gegenstände, da die Computer- und Datendelikte im Gegensatz zu den klassischen Eigentums- und Vermögensdelikten (wie Diebstahl oder Betrug) ganz überwiegend als "Bagatellkriminalität" ausgestaltet sind. So ist etwa für das Ausspähen von Daten (§ 202a Absatz 1 StGB), die Datenhehlerei (§ 202d Absatz 1 StGB) und den Grundtatbestand der Computersabotage (§ 303b Absatz 1 StGB) lediglich eine Freiheitsstrafe von bis zu drei Jahren oder Geldstrafe vorgesehen. Das Abfangen von Daten (§ 202b StGB), das Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c Absatz 1 StGB) und die Datenveränderung (§ 303a Absatz 1 StGB) werden sogar nur mit einer Freiheitsstrafe von maximal zwei Jahren oder mit Geldstrafe bestraft. Diese Strafrahmen liegen alle im unteren Bereich, während bei den klassischen Eigentums- und Vermögensdelikten bereits für den einfachen Diebstahl oder Betrug eine Freiheitsstrafe von bis zu fünf Jahren oder Geldstrafe vorgesehen ist.

Anders als bei den klassischen Eigentums- und Vermögensdelikten fehlt es auch an Qualifikationstatbeständen und Regelbespielen mit erhöhten Strafdrohungen, um Fallgestaltungen mit einem gesteigerten Unrechtsgehalt in einer angemessenen Weise erfassen zu können und der Bedeutung der Daten in der digitalen Welt von heute gerecht zu werden. Lediglich bei der Computersabotage finden sich Regelungen für qualifizierende und besonders schwere Fälle (§§ 303b Absätze 2 und 4 StGB), wobei die Computersabotage im Fall des § 303b Absatz 1 Nummer 1 StGB

ihrerseits eine Qualifikation der Datenveränderung nach § 303a StGB darstellt. Im Übrigen fehlt es im Bereich der Cybercrime-Delikte aber an der Möglichkeit, auf schwerwiegende Taten mit einem gesteigerten Unrechtsgehalt tat- und schuldangemessen zu reagieren.

Dies hat zur Folge, dass beispielsweise ein Hacker, der sich unbefugt Zugang zu einer Datenbank verschafft und dabei mehrere Millionen Datensätze abgreift, derzeit lediglich eine Freiheitsstrafe von maximal drei Jahren oder eine Geldstrafe zu befürchten hat - selbst wenn er gewerbsmäßig handelt und große Schäden für den Einzelnen oder das Gemeinwesen verursacht. Datenabgriffe dieses Ausmaßes, die infolge der heutigen technischen Möglichkeiten immer leichter möglich werden und das Vertrauen großer Teile der Bevölkerung in die Sicherheit der modernen Informationstechnologie erschüttern, entsprechen ersichtlich nicht mehr dem, was der Gesetzgeber im Blick hatte, als er 1986 im Zeitalter der Magnetbänder und Disketten das Ausspähen von Daten in § 202a StGB unter Strafe stellte. Die technische Entwicklung und damit einhergehend auch die wachsende Bedrohung durch die Cyberkriminalität haben dazu geführt, dass die im Kerncomputerstrafrecht vorgesehenen Strafrahmen dem verwirklichen Unrecht und general- wie spezialpräventiven Strafbedürfnissen in vielen Fällen nicht mehr gerecht werden.

Ferner sehen einige Delikte aus der digitalen Welt keine Versuchsstrafbarkeit vor, ohne dass dies sachlich zu rechtfertigen wäre. So ist beispielsweise der Versuch der Datenausspähung nach § 202a StGB oder der Datenhehlerei nach § 202d StGB nicht strafbar, der Versuch des Diebstahls nach § 242 Absatz 2 StGB oder der Sachhehlerei nach § 259 Absatz 3 StGB aber schon. Ein virtueller Einbruchsversuch bleibt damit straflos, gleichgültig ob der Erfolg aus Unfähigkeit des Täters oder aufgrund der Effektivität der Zugangssicherung ausbleibt. Dies ist nicht sachgerecht.

Die Bagatellisierung der Computer- und Datendelikte im materiellen Strafrecht setzt sich im Strafprozessrecht fort. Denn beim Verdacht einer Straftat nach den §§ 202a ff., §§ 303a f. StGB können derzeit häufig die Täter nicht ermittelt und überführt werden, weil den Strafverfolgungsbehörden die strafprozessualen Befugnisse für erfolgversprechende Ermittlungen in der digitalen Welt nicht oder nur eingeschränkt zu Verfügung stehen. So ist eine Überwachung der Telekommunikation in Form der „Serverüberwachung“ oder eine Online-Durchsuchung zur Identifizierung der Täter, zur Aufhellung der verwendeten Infrastruktur und zum Führen des

Tatnachweises mangels Vorliegen einer Katalogtat nach § 100a Absatz 2 bzw. § 100b Absatz 2 StPO derzeit rechtlich nicht zulässig. Die Erhebung von Verkehrsdaten ist de lege lata nur eingeschränkt nach § 100g Absatz 1 Satz 1 Nummer 2 StPO zulässig, mangels Vorliegens einer Katalogtat aber nicht nach § 100g Absatz 1 Satz 1 Nummer 1 oder § 100g Absatz 2 StPO. Diese technischen Ermittlungsmaßnahmen stellen aber oftmals den einzig erfolgversprechenden Ermittlungsansatz dar, da die Delikte der Cyberkriminalität in den allermeisten Fällen auch oder ausschließlich unter Zuhilfenahme von Telekommunikationsdiensten begangen werden.

Das gilt zum Beispiel insbesondere für die Straftaten im Zusammenhang mit der sog. Botnetzkriminalität, bei der zahlreiche Computersysteme über das Internet mittels einer Schadsoftware infiltriert und zu einem mitunter mehrere Millionen Geräte umfassenden Verbund, einem sog. Botnetz, zusammengeschlossen werden. Dieser Verbund lässt sich durch den Angreifer über das Internet fernsteuern und beispielsweise für sog. "Distributed-denial-of-service (DDos) - Attacken" benutzen, die darauf abzielen, ein bestimmtes Zielsystem durch eine Vielzahl von gleichzeitigen Anfragen der zum Botnetz gehörenden Rechner derart zu belasten, dass dieses unter der Last des Datenaufkommens zusammenbricht. So führte im Oktober 2016 der Angriff des „Mirai-Botnetzes“, bestehend aus ca. 300.000 Geräten internetfähiger Steuerungs- und Überwachungshardware (IoT), zum Ausfall eines großen DNS-Dienstes, wodurch mehrere große Plattformen nicht mehr erreichbar waren. Derartige Straftaten können nur mit Mitteln der modernen Informationstechnik, insbesondere des Internets, begangen werden, so dass die oben genannten technischen Ermittlungsmaßnahmen oftmals den einzigen Ermittlungsansatz darstellen, um die Täter zu identifizieren und die dahinter stehenden Netzwerke aufzudecken.

Die geschilderten Defizite im materiellen Strafrecht und Strafprozessrecht werden weder der gesellschaftlichen und wirtschaftlichen Bedeutung digitaler Daten und informationstechnischer Systeme noch der Bedeutung des Grundrechts auf informationelle Selbstbestimmung gerecht.

Diese Defizite sollen durch den Entwurf behoben werden. Der Entwurf zielt darauf ab, den strafrechtlichen Schutz digitaler Daten und informationstechnischer Systeme an deren gestiegene gesellschaftliche und wirtschaftliche Bedeutung anzupassen und den Strafverfolgungsbehörden die rechtlichen Ermittlungsbefugnisse an die Hand zu geben, die zur effektiven Bekämpfung der Cyberkriminalität unabdingbar

sind. Der Entwurf dient damit letztlich dem Schutz der modernen Informationsgesellschaft vor der wachsenden Bedrohung durch die Cyberkriminalität.

Zu diesem Zweck sieht der Entwurf vor, die Strafdrohungen der Straftatbestände für die digitale Welt zu verschärfen und bei bestimmten Delikten auch die Versuchsstrafbarkeit einzuführen. Dazu gehört neben einer Anhebung der Strafrahmen bei manchen (Grund-) Tatbeständen der §§ 202a ff., §§ 303a f. StGB auch, Strafzumessungsregeln für besonders schwere Fälle, Qualifikationstatbestände und erfolgsqualifizierte Tatbestände mit erhöhten Strafdrohungen zu schaffen. Der Entwurf beschränkt sich dabei mit Blick auf den Schuld- und Verhältnismäßigkeitsgrundsatz auf solche Fallgestaltungen, die typischerweise einen deutlich gesteigerten Unrechtsgehalt aufweisen. So sieht der Entwurf aufgrund der hohen kriminellen Energie bzw. des hohen Schadens- und Gefahrenpotentials - für die einzelnen Straftatbestände differenziert - erhöhte Strafdrohungen für solche Taten vor, die gewerbs- und/oder bandenmäßig begangen werden, eine große Menge an Daten oder eine große Anzahl von Personen betreffen, Daten kritischer Infrastrukturen angehen, die Sicherheit der Bundesrepublik Deutschland oder der Länder gefährden, höchstpersönliche und damit besonders sensible Daten zum Gegenstand haben oder leichtfertig den Tod eines Menschen verursachen.

Soweit sich der Entwurf dabei für die Strafrahmen der Delikte aus der digitalen Welt an die Straftatbestände aus der analogen Welt anlehnt, wird nicht verkannt, dass die in beiden Deliktsbereichen betroffenen Tatobjekte ihrem Wesen nach durchaus Unterschiede aufweisen. So sind digitale Daten im Gegensatz zu körperlichen Gegenständen nicht exklusiv und nicht abnutzbar, das heißt, prinzipiell beliebig kopierbar und von mehreren Personen zur gleichen Zeit ohne Verschleiß nutzbar. Daher ist es zum Beispiel im Falle eines "Datendiebstahls" möglich, dass dem Opfer die Nutzung der vom Täter kopierten Daten erhalten bleibt, während das Opfer eines Sachdiebstahls den entwendeten körperlichen Gegenstand nicht mehr nutzen kann. Jedoch hindern diese Wesensunterschiede den Gesetzgeber nicht, für digitale Daten angesichts ihres Bedeutungszuwachses ein vergleichbares Schutzniveau wie für körperliche Gegenstände vorzusehen, zumal die Bevölkerung inzwischen die Cyberkriminalität ebenso als massive Bedrohung ihrer Sicherheit im privatesten Lebensbereich wahrnimmt wie die klassische Eigentums- und Vermögenskriminalität. Zudem können die Folgen für das Opfer bei Taten in der digitalen Welt mindesten ebenso

schwer sein wie bei Taten in der analogen Welt. Mag das Opfer seine Daten unter Umständen auch nach dem "Datendiebstahl" noch nutzen können, so können mit der Tat doch schwerwiegende Folgen für das Opfer verbunden sein, die weit über die Frage der fortbestehenden Nutzungsmöglichkeit hinausgehen. So haben die Opfer, gerade wenn vom Täter Daten mit Details etwa aus ihrem Intimleben erbeutet und im Internet verbreitet werden, oftmals lange mit Schockzuständen, Schamgefühlen und empfindlichen Beeinträchtigungen im privaten wie beruflichen Bereich zu kämpfen.

In Ergänzung zu den materiell-rechtlichen Strafschärfungen sieht der Entwurf vor, die strafprozessualen Ermittlungsbefugnisse der Strafverfolgungsbehörden auszubauen, indem er - bei Wahrung der Vorgaben des Bundesverfassungsgerichts und unter Berücksichtigung der Bedürfnisse einer effektiven Strafverfolgung - die Straftatenkataloge der §§ 100a Absatz 2, 100b Absatz 2, 100g Absatz 2 StPO und damit den Anwendungsbereich der Telekommunikationsüberwachung, Online-Durchsuchung und Verkehrsdatenerhebung erweitert. Der Entwurf ermöglicht es somit den Strafverfolgungsbehörden, bei digitalen Delikten auch digital ermitteln zu können. Er beschränkt diese Möglichkeit zur Wahrung des Verhältnismäßigkeitsgrundsatzes aber von vornherein auf solche Delikte, die als schwer bzw. besonders schwer einzustufen sind. Damit trägt er den Vorgaben des Bundesverfassungsgerichts Rechnung, wonach die genannten Ermittlungsmaßnahmen zur Rechtfertigung der mit ihnen verbunden, nicht unerheblichen Grundrechtseingriffe auf die Verfolgung von Straftaten mit einem entsprechenden Schweregrad zu beschränken sind (vgl. etwa BVerfG NJW 2016, 1781 [1784]; NJW 2012, 833 [836]; NJW 2010, 833 [841]). Soweit die Delikte aber den notwendigen Schweregrad erreichen, ist ihre Aufnahme in die Anlasstatenkataloge der technischen Ermittlungsmaßnahmen nach §§ 100a, 100b und 100g StPO nicht zur zulässig, sondern auch geboten, da die wirksame Aufklärung gerade schwerer Straftaten - wie das Bundesverfassungsgericht wiederholt betont hat (BVerfG NJW 2004, 999 [1008]) - ein wesentlicher Auftrag des rechtsstaatlichen Gemeinwesens ist. In Erfüllung dieses Auftrags bestimmt der Entwurf zur effektiven Bekämpfung der Cyberkriminalität in den neuen § 100a Absatz 2 Nummer 1 Buchstabe h, § 100b Absatz 2 Nummer 1 Buchstabe f und § 100g Absatz 2 Satz 2 Nummer 1 Buchstabe e StPO-E, dass auch schwere bzw. besonders schwere Computer- und Datendelikte als Anlasstaten für die dort geregelten Ermittlungsmaßnahmen in Betracht kommen.

Insgesamt betrachtet, schafft der Entwurf durch das Zusammenspiel der materiellen Strafschärfungen mit den verbesserten strafprozessualen Ermittlungsbefugnissen die Möglichkeit, der wachsenden Bedrohung durch die Cyberkriminalität nachhaltig und effektiv entgegenzutreten und das Vertrauen der Bevölkerung in die Handlungsfähigkeit staatlicher Organe und in den Rechtsstaat zu erhalten.

II. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Art. 74 Absatz 1 Nummer 1 des Grundgesetzes (Strafrecht).

III. Auswirkungen

Durch die vorgeschlagenen Änderungen im materiellen Strafrecht und Strafprozessrecht, insbesondere durch die Erweiterung des Anwendungsbereichs der technischen Ermittlungsmaßnahmen nach §§ 100a, 100b und 100g StPO kann ein Mehraufwand für die Strafverfolgungsbehörden entstehen, dessen Umfang derzeit noch nicht quantifizierbar ist. Der Mehraufwand ist jedoch angesichts des verbesserten Rechtsgüterschutzes gerechtfertigt. Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Strafgesetzbuchs)

Zu Nummer 1 (§ 202a StGB-E)

Zu Buchstabe a (Absatz 1 StGB-E)

Der Entwurf sieht in Absatz 1 des § 202a eine Erhöhung der Höchststrafe von drei auf fünf Jahren vor, um dem in der zunehmend von Digitalisierung geprägten Welt steigenden Interesse des Berechtigten am Schutz der in gespeicherten Daten verkörperten Informationen gerecht zu werden sowie den Strafrahmen des Ausspähens von Daten an den des Diebstahls von Sachen anzugleichen. Die kriminelle Energie, die ein Täter beim unberechtigten Zugriff auf informationstechnische Systeme und digitale Daten aufwenden muss, kann mindestens ebenso so groß - wenn nicht sogar größer - sein wie diejenige, die für die Begehung eines einfachen Diebstahls erforderlich ist, zumal der Täter für die Verwirklichung des § 202a StGB - anders als für

die Verwirklichung des § 242 StGB - sogar eine besondere Zugangssicherung überwinden muss. Wenn einem Täter ein automatisierter Angriff auf über 100 Webseiten gelingt und er hierbei Millionen von Kunden- und Zahlungsdaten ausspäht, um durch den Verkauf dieser Daten seinen Lebensunterhalt zu bestreiten, verbleibt es bei dem Strafrahmen des Grunddelikts von derzeit bis zu drei Jahren. Über die Verhältnismäßigkeitsprüfung hat dieser geringe Strafrahmen auch Auswirkungen für die Haftfrage, selbst wenn konkrete Anhaltspunkte für eine Verdunkelungsgefahr bestehen.

Die derzeitige Ausgestaltung der Datenausspähung als Bagatelldelikt wird im Übrigen auch der gewachsenen gesellschaftlichen und wirtschaftlichen Bedeutung digitaler Daten nicht gerecht. Die Nutzung informationstechnischer Systeme ist für die Lebensführung vieler Bürger von zentraler Bedeutung und aus ihrem Alltagsleben kaum noch wegzudenken. Aber auch andere Bereiche des modernen Lebens, wie etwa die öffentliche Verwaltung oder der Unternehmenssektor, sind angesichts der fortschreitenden Digitalisierung mehr denn je auf informationstechnische Systeme angewiesen. Vor diesem Hintergrund ist es angemessen, informationstechnische Systeme und Daten strafrechtlich besser vor unberechtigten Zugriffen zu schützen. Da die Gefahren und Schäden durch unberechtigte Datenabgriffe für die Geschädigten ebenso groß sein können wie etwa bei den klassischen Eigentumsdelikten, ist eine Anhebung des Strafrahmens auch aus general- und spezialpräventiven Gründen geboten.

Zu Buchstabe b (Absatz 3 bis 5 StGB-E)

Der Entwurf schafft mit den Absätzen 4 und 5 des § 202a StGB-E einen Qualifikationstatbestand und eine Strafzumessungsregel für besonders schwere Fälle der Datenausspähung, die sich vom Strafrahmen des Grundtatbestandes nicht immer angemessen erfassen lassen. § 202a StGB sieht de lege lata keine Möglichkeit vor, Taten mit einem besonderen Unrechtsgehalt schärfer und damit schuldangemessen zu bestrafen. Insbesondere haben bisher bestimmte Tatvarianten, die sich in vielen Bereichen des Kernstrafrechts strafschärfend auswirken, wie etwa eine gewerbs- oder bandenmäßige Tatbegehung, bei der Datenausspähung keine Auswirkung auf den in Betracht kommenden Strafrahmen. Dies ist insbesondere bei einem Vergleich mit den klassischen Diebstahlsdelikten, die in den §§ 243 ff. StGB Strafschärfungen für qualifizierte Begehungsweisen erhalten, nicht sachgerecht. Ebenso wenig ist es sach- und systemgerecht, dass § 202a StGB-E bislang keine Versuchsstrafbarkeit

vorsieht, weshalb der Entwurf mit dem neuen Absatz 3 den Versuch der Datenausspähung für strafbar erklärt. Im Einzelnen:

1. Der Entwurf erklärt in Absatz 3 des § 202a StGB-E den Versuch der Datenausspähung für strafbar. Damit wird nicht nur der strafrechtliche Schutz für digitale Daten an denjenigen für körperliche Gegenstände angeglichen, sondern zugleich auch die derzeit bestehende Inkonsistenz beseitigt, dass zwar die Vorbereitung einer Datenausspähung nach § 202c StGB strafbar ist, der Versuch aber nicht. De lege lata bleiben damit selbst massenhaft begangene Versuchshandlungen straflos, unabhängig davon, ob diese an dem Unvermögen des Täters oder an der Qualität der Zugangssicherung scheitern (Ernst NJW 2007, 2661 [2662]; Graf in: MüKo-StGB, 3. Aufl. 2017, § 202a Rn. 109). Straflos sind derzeit beispielsweise computergesteuerte Cyberangriffe auf Firmen, bei denen in einem "trial and error - Verfahren" unter Umständen mehrere Tage lang mittels eines automatisiert ablaufenden Hacking-Tools erfolglos versucht wird, den Zugang zur Firmendatenbank zu hacken, um an die Kunden- und Kreditkartendaten zu gelangen (Graf in: MüKo-StGB, 3. Aufl. 2017, § 202a Fn. 360). Gleiches gilt für automatisierte Versuche mittels spezieller Programme, Passwörter von Privatpersonen, Unternehmen oder der öffentlichen Verwaltung zu "knacken". Den Opfern dieses Vorgehens stehen derzeit bestenfalls technische Gegenmaßnahmen zur Verfügung. Solche Handlungen im Versuchsstadium sind aber mindestens ebenso - wenn nicht sogar noch eher - strafwürdig als vorgelagerte Handlungen im bloßen Vorbereitungsstadium, wo bereits die einmalige Verschaffung eines entsprechenden Hacking-Tools in § 202c StGB unter Strafe gestellt ist. Die fehlende Versuchsstrafbarkeit im geltenden Recht ist daher sachlich nicht nachvollziehbar. Auch aus dogmatischer Sicht vermag es zu nicht zu überzeugen, dass das geltende Recht zwar vor der bloß abstrakten Rechtsgutsgefährdung durch eine Vorbereitungshandlung, nicht aber vor der im Versuch liegenden konkreten Rechtsgutsgefährdung schützt.

   Um diese Inkonsistenzen zu beseitigen, sieht der Entwurf mit dem neuen Absatz 3 die Einführung einer Versuchsstrafbarkeit vor. Danach ist der Versuch eines Vergehens nach § 202a Absatz 1 StGB-E gemäß § 202a Absatz 3 StGB-E in Verbindung mit §§ 23 Absatz 1 Alternative 2, 12 Absatz 2 StGB strafbar. Die

Strafbarkeit des vorgeschlagenen Verbrechenstatbestandes nach § 202a Abs. 5 StGB-E ergibt sich aus §§ 23 Absatz 1 erste Alternative, 12 Absatz 1 StGB.

2. Der vorgeschlagene Absatz 4 des § 202a StGB-E sieht eine Strafzumessungsregel für besonders schwere Fälle der Datenausspähung mit einem erhöhten Strafrahmen von drei Monaten bis zu zehn Jahren vor. Dabei werden in Nummer 1 bis 4 des § 202a Absatz 4 Satz 2 StGB-E zur Konkretisierung mehrere Regelbeispiele benannt:

   - Nach Nummer 1 des § 202a Absatz 4 Satz 2 StGB-E liegt ein besonders schwerer Fall in der Regel dann vor, wenn das Ausspähen von Daten gewerbs- oder bandenmäßig begangen wird. Die Auslegung dieser Merkmale kann sich an der Auslegung der entsprechenden Merkmale in anderen Regelungen im StGB orientieren (vgl. etwa §§ 243 Absatz 1 Satz 2 Nummer 3, 244 Absatz 1 Nummer 2, 263 Absatz 3 Satz 2 Nummer 1 StGB). Im Falle der bandenmäßigen Begehung muss sich die Bandenabrede auf eine Tat nach §§ 202a bis 202d, 263a, 269, 303a oder 303b beziehen. Erfasst sind also nicht nur die Computer- und Datendelikte im engeren Sinn nach §§ 202a bis 202d, 303a oder 303b StGB, sondern auch die oftmals mitverwirklichten Delikte des Computerbetrugs nach § 263a StGB und der Fälschung beweiserheblicher Daten nach § 269 StGB. Dadurch wird sichergestellt, dass auch solche Banden unter das Regelbeispiel fallen, deren überwiegendes Ziel die Begehung von Verwertungstaten ist und für die die Begehung etwa einer Datenausspähung lediglich einen den eigentlichen Bandenzweck vorbereitenden Charakter aufweist.

     Der im Vergleich zum Grundtatbestand erhöhte Strafrahmen rechtfertigt sich aus der erhöhten kriminellen Energie, die mit der gewerbs- oder bandenmäßigen Tatbegehung im Regelfall verbunden ist. Hinzu kommt bei Bandendelikten die erhöhte Gefährlichkeit, die aus dem auf eine gewisse Dauer angelegten Zusammenschluss von mehr als zwei Tätern zu einer Bande und dem damit einhergehenden Anreiz zur Begehung weiterer Straftaten resultiert.

Anders als bei den Diebstahlsdelikten (vgl. § 244 Absatz 1 Nummer 2 StGB), aber entsprechend den Betrugsdelikten (§ 263 Absatz 3 Satz 2 Nummer 1 StGB), gestaltet der Entwurf die bandenmäßige Tatbegehung lediglich als Regelbeispiel und nicht als Qualifikation aus, um unverhältnismäßige Sanktionen im Einzelfall zu verhindern. Dies gilt umso mehr, als der Entwurf - anders als § 244 Absatz 1 Nummer 2 StGB, aber wie § 263 Absatz 3 Satz 2 Nummer 1 StGB - auf das Erfordernis der Mitwirkung eines anderen Bandenmitglieds an der Tat verzichtet, so dass aufgrund der fehlenden Mitwirkung eines zweiten Bandenmitglieds bei der Tatausführung die Gefahr für das geschützte Rechtsgut im Einzelfall auch geringer sein kann als beim Bandendiebstahl nach § 244 Absatz 1 Nummer 2 StGB.

- Nummer 2 des § 202a Absatz 4 Satz 2 StGB-E sieht ein Regelbeispiel für den Fall vor, dass der Täter eine große Menge von Daten ausspäht oder in der Absicht handelt, durch die fortgesetzte Tatbegehung Daten einer großen Anzahl von Personen auszuspähen. Mit dem Wort "ausspähen" wird auf die Tathandlung des Grundtatbestandes nach § 202a Absatz 1 StGB Bezug genommen, so dass - wie beim Grundtatbestand - auch für die Verwirklichung des Regelbeispiels die bloße Zugangsverschaffung ausreicht. Das Regelbeispiel ist erfüllt, wenn der Täter sich oder einem anderen den Zugang zu einer großen Menge von Daten verschafft oder in der Absicht handelt, sich oder einem anderen durch die fortgesetzte Tatbegehung den Zugang zu Daten von einer großen Anzahl von Personen zu verschaffen. Für die Zugangsverschaffung genügt es dabei, wenn der Täter so weit in ein informationstechnisches System eindringt, dass er ohne weiteres Hindernis im nächsten Schritt auf die nicht für ihn bestimmten Daten zugreifen kann. Er muss sich also nicht diese Daten, sondern lediglich den Zugang zu den Daten verschaffen (indem er sich etwa das Passwort oder einen anderen Zugangsschlüssel besorgt). Dies betrifft die in der Praxis auftretenden Fälle, in denen der Täter den erlangten Zugang nicht unmittelbar für den Download der Daten nutzt, sondern sich, um unentdeckt zu bleiben, lediglich den konkreten Zugriff auf wertvoll erscheinende Daten sichert.

  Bei der "großen Menge an Daten" und "großen Anzahl von Personen" handelt

es sich um unbestimmte Rechtsbegriffe, die nach objektiven Gesichtspunkten unter Berücksichtigung des technischen Fortschritts zu bestimmen sind.

Ob eine große Menge von Daten vorliegt, bestimmt sich nach dem Informationsgehalt der Daten. Die absolute physikalische Größe des Datenvolumens ist als maßgebliches Kriterium unzureichend. Entscheidend sind hier auch das Datenformat und der Dateityp. Eine hochauflösende Videodatei kann beispielsweise bei nur drei Minuten Laufzeit des Videos eine Dateigröße von einem Gigabyte (=1000 Megabyte) erreichen, ohne dass eine große Menge an Daten vorliegen würde. Für eine komprimierte Textdatei, die 30.000 E-Mail-Adressen und die dazugehörigen Passwörter umfasst, wäre dagegen ein Speicherplatz von nur einem Megabyte ausreichend. Hinsichtlich einer Addition der Datenmengen kommt es darauf an, ob eine Tat im Sinne von § 52 StGB vorliegt.

Eine große Anzahl von Personen liegt entsprechend zu den zu § 263 Absatz 3 Nr. 2 StGB entwickelten Grundsätzen jedenfalls dann vor, wenn die Daten von mehr als fünfzig Personen ausgespäht werden. Mit diesem Regelbeispiel sollen insbesondere auch solche Fälle erfasst werden, in denen ein Täter bei einer Vielzahl von unterschiedlichen Personen jeweils nur eine kleine Menge an Daten ausspäht. Das Regelbeispiel ist dabei - ebenso wie das ähnliche Regelbeispiel in § 263 Absatz 3 Satz 2 Nummer 2 Alternative 2 StGB - nicht erst dann erfüllt, wenn der Täter eine große Anzahl von Personen ausgespäht hat, sondern bereits dann, wenn er in der Absicht handelt, die Daten einer großen Zahl von Personen auszuspähen. Liegt eine solche Absicht vor, reicht schon die erste Tatbegehung für die Erfüllung des Regelbeispiels aus, auch wenn es dann entgegen der Intention des Täters nicht zu weiteren Ausspähhandlungen bei anderen Personen kommt.

- Nach Nummer 3 des § 202a Absatz 4 Satz 2 StGB-E liegt ein besonders schwerer Fall in der Regel vor, wenn der Täter sich oder einem anderen den Zugang zu Daten kritischer Infrastrukturen verschafft oder durch die Tat die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet.

Kritische Infrastrukturen sind nach der allgemeinen Definition der KRITIS-Strategie der Bundesregierung "Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden" (siehe Bundesministerium des Innern, für Bau und Heimat: Nationale Strategie zum Schutz Kritischer Infrastrukturen [KRITIS-Strategie], S. 3, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html). Diese allgemeine Definition kann zur näheren Konkretisierung auf die Begriffsbestimmung des § 2 Absatz 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und die dazugehörige Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) zurückgreifen, geht aber darüber hinaus. Denn § 2 Absatz 10 BSIG benennt nur die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, während nach der allgemeinen Definition der Bundesregierung auch die Sektoren Staat und Verwaltung sowie Medien und Kultur erfasst sind (vgl. https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html;jsessionid=B129E95380725F74369887B463F1F0F9.2_cid330; Buchberger in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, BSIG, § 2 Rn. 12). Kritische Infrastrukturen im Sinne des hier vorgeschlagenen Regelbeispiels können also zum Beispiel nicht nur Krankenhäuser, Kernkraftwerke, Flughäfen oder Banken, sondern auch Regierungs-, Verwaltungs- oder Justizbehörden, der Deutsche Bundestag oder Rundfunkeinrichtungen sein. Die Aufnahme dieser kritischen Infrastrukturen in den Katalog der Regelbeispiele trägt den Umstand Rechnung, dass diese Infrastruktur besonders schutzwürdig sind, da sie aufgrund der fortschreitenden Digitalisierung in hohem Maße auf informationstechnische Systeme angewiesen sind und unberechtigte Zugriffe auf diese Systeme schwerwiegende Folgen auch für die Allgemeinheit haben können.

Die Sicherheit der Bundesrepublik Deutschland umfasst die innere und

äußere Sicherheit. Die Begriffsbestimmung kann sich - wie bei § 303b Absatz 4 Satz 2 Nummer 3 StGB - an § 92 Absatz 3 Nummer 2 StGB orientieren. Gemeint ist also die Fähigkeit der Bundesrepublik, sich nach außen und innen gegen Störungen zur Wehr zu setzen. Entsprechendes gilt für die Sicherheit eines der Länder der Bundesrepublik Deutschland. Allerdings ist nach dem Entwurf nicht erforderlich, dass diese Fähigkeit durch die Tat konkret beeinträchtigt wird. Vielmehr soll aus generalpräventiven Gründen bereits die bloße Gefährdung der Sicherheit genügen, um die erhöhte Strafdrohung der Strafzumessungsregel auszulösen.

- Nummer 4 des § 202a Absatz 4 Satz 2 StGB-E bestimmt schließlich, dass ein besonders schwerer Fall in der Regel vorliegt, wenn der Täter sich oder einem anderen den Zugang zu Daten verschafft, die den höchstpersönlichen Lebensbereich berühren. Die Aufnahme in den Regelbeispielskatalog für besonders schwere Fälle ist geboten, da es sich bei diesen Daten um äußerst sensible und damit besonders schutzwürdige Daten handelt. Das Bundesverfassungsgericht rechnet solche Daten in ständiger Rechtsprechung dem Kernbereich privater Lebensgestaltung eines Menschen zu und unterstellt sie damit dem Schutz des aus der Menschenwürdegarantie (Art. 1 Absatz 1 GG) fließenden Achtungs- und Schutzanspruchs, was die besondere Schutzwürdigkeit dieser Daten belegt.

  Bei der Auslegung des Begriffs des "höchstpersönlichen Lebensbereichs" kann auf die zu § 201a StGB entwickelten Grundsätze, die sich ihrerseits an der Rechtsprechung des Bundesverfassungsgerichts zum Kernbereich privater Lebensgestaltung orientieren, zurückgegriffen werden. Höchstpersönlich sind danach zum Beispiel Daten, die innere Vorgänge wie Gedanken, Empfinden oder Gefühle wiedergeben (etwa in einer digitalen "Tagebuchdatei") oder intime Nacktaufnahmen aus dem privaten Sexualleben eines Menschen enthalten (vgl. BT-Drs. 15/2466, S. 5, BVerfG NJW 2016, 1781 [1786]).

3. Der vorgeschlagene Absatz 5 des § 202a StGB-E sieht schließlich einen Qualifikationstatbestand vor. Danach wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten

bis zu fünf Jahren, bestraft, wer in den Fällen des Absatzes 4 Satz 2 Nummer 1 erste Alternative und Nummern 2 bis 4 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Delikten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b verbunden hat.

Der Entwurf erhebt damit - in Anlehnung an die Regelungen in §§ 244a, 260a und 263 Absatz 5 StGB - die bandenmäßige Begehung von Datenausspähungen unter erschwerenden Umständen (nämlich unter den Umständen des Absatz 4 Satz 2 Nummer 1 erste Alternative oder Nummer 2 bis 4) zu einem Verbrechenstatbestand. Hierdurch wird erreicht, dass zur schweren Kriminalität zählende Cyberattacken insbesondere aus dem Bereich des Organisierten Cybercrime von den Gerichten in einer schuldangemessenen Weise bestraft werden können.

Zum Organisierten Cybercrime zählt die vom Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Computer- und Datendelikten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind und an denen mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen, unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken (vgl. Ziff. 2. 1 der Gemeinsamen Richtlinien der Justizminister/-senatoren und der Innenminister/-senatoren der Länder über die Zusammenarbeit bei der Verfolgung der Organisierten Kriminalität; Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Auflage 2018, Kapitel 1 Rn. 37). Der Bekämpfung dieser besonders schwerwiegenden Kriminalitätsform dient Absatz 5, der insbesondere durch die kumulative Verbindung der gewerbsmäßigen mit der bandenmäßigen Begehungsweise wesentliche Bereiche der Organisierten Cyber-Kriminalität erfasst.

Zu Nummer 2 (§ 202b StGB-E)

Zu Buchstabe a (Absatz 1 StGB-E)

Der Entwurf sieht vor, dass der bisherige Normtext des § 202b als neuer Absatz 1 des § 202b StGB-E den Grundtatbestand für das Abfangen von Daten bildet. In Anlehnung an § 201 StGB wird dabei das Höchstmaß der zulässigen Freiheitsstrafe von zwei auf drei Jahre erhöht.

Das Abfangen von Daten nach § 202b StGB stellt in gewisser Weise das digitale Pendant zum unbefugten Abhören und Aufzeichnen von Telefongesprächen dar (Fischer, Strafgesetzbuch, 66. Auflage, 2019, § 202b Rn. 2: § 202b StGB "entspricht" insoweit § 201 StGB), das in § 201 StGB als Verletzung der Vertraulichkeit des Wortes mit einer Freiheitsstrafe von bis zu drei Jahren oder mit Geldstrafe bedroht ist. Ein Großteil moderner Kommunikation findet nicht mehr im direkten verbalen Austausch in Echtzeit statt, sondern verlagert sich auf datenbasierte Kommunikationsplattformen. Dennoch ist auch diese Form der Kommunikation in Chats und Messenger-Diensten nicht öffentlich und daher besonders schutzwürdig. Es erscheint daher auch sachgerecht, beide Konstellationen im Strafrahmen gleich zu behandeln.

Im Vergleich zum Ausspähen von Daten nach § 202a Absatz 1 StGB-E, für das der Entwurf eine Höchststrafe von fünf Jahren vorschlägt, ist bei § 202b Absatz 1 StGB-E eine Strafdrohung von maximal drei Jahren Freiheitsstrafe ausreichend, aber auch erforderlich. Die bereits bisher vorgesehene Abstufung des Strafrahmens zwischen § 202a und § 202b StGB bleibt damit durch den Entwurf erhalten. Diese Abstufung ist mit Blick auf den unterschiedlichen Unrechtsgehalt beider Delikte auch angemessen, zumal § 202b StGB - im Gegensatz zu § 202a StGB - nicht verlangt, dass der Täter eine besondere Zugangssicherung überwindet.

Zu Buchstabe b (Absätze 2 bis 4 StGB-E)

Der Entwurf fügt in § 202b StGB zudem einen neuen Absatz 3 mit einer Strafzumessungsregel für besonders schwere Fälle des Abfangens von Daten und einen neuen Absatz 4 mit einem Qualifikationstatbestand ein, um auch Taten mit einem gesteigerten Unrechtsgehalt in einer schuldangemessenen, den Bedürfnissen der General- und Spezialprävention genügenden Weise bestrafen zu können. Ferner sieht der

Entwurf mit dem neuen Absatz 2 vor, die Versuchsstrafbarkeit für das Abfangen von Daten einzuführen. Im Einzelnen:

1. In Parallele zu der in § 202a Absatz 3 StGB-E vorgeschlagenen Versuchsstrafbarkeit für das Ausspähen von Daten sieht der Entwurf mit dem neuen Absatz 2 des § 202b StGB-E auch für das Abfangen von Daten vor, den Versuch für strafbar zu erklären. Dadurch reagiert der Entwurf - wie bei § 202a StGB - auf die derzeit bestehende und nicht hinnehmbare Inkonsistenz, dass die (bloß) abstrakte Gefährdung des geschützten Rechtsguts im Vorbereitungsstadium nach § 202c StGB strafrechtlich sanktioniert wird, die konkrete Rechtsgutsgefährdung im Versuchsstadium nach geltendem Recht aber straflos bleibt. Darüber hinaus ist es auch wenig stimmig, dass der Versuch des unbefugten Abhörens und Aufzeichnens von Telefongesprächen nach § 201 Absatz 4 StGB strafbar ist, der Versuch des Abfangens von Daten als digitales Pendant zum unbefugten Zugriff auf Telefongespräche hingegen straflos. Diese Inkonsistenzen werden mit dem vorgeschlagenen Absatz 2 des § 202b StGB-E beseitigt.

2. In diesem Sinne sieht Absatz 3 des § 202b StGB-E vor, besonders schwere Fälle des Abfangens von Daten mit einer Freiheitsstrafe von drei Monaten bis zu fünf Jahren zu bestrafen. Zur Konkretisierung werden in den Nummern 1 bis 4 des § 202b Absatz 3 Satz 2 StGB-E - in Anlehnung an § 202a Absatz 4 Satz 2 StGB-E - Regelbeispiele für besonders schwere Fälle benannt. Ein besonders schwerer Fall liegt danach in der Regel vor, wenn das Abfangen von Daten gewerbs- oder bandenmäßig begangen wird (Nummer 1), eine große Menge an Daten oder eine große Anzahl von Personen betrifft (Nummer 2), sich auf Daten kritischer Infrastrukturen bezieht oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet (Nummer 3) oder höchstpersönliche Daten erfasst (Nummer 4).

   Für diese Regelbeispiele gelten die obigen Ausführungen zu § 202a Absatz 4 StGB-E entsprechend mit der Maßgabe, dass in den Fällen des § 202b Absatz 3 StGB-E im Gegensatz zu § 202a Absatz 4 StGB-E ein Verschaffen der Daten und nicht des bloßen Zugangs zu Daten erforderlich ist. Dies ergibt sich daraus, dass bereits der Grundtatbestand des Abfangens von Daten nach § 202b Absatz 1

StGB-E - im Unterschied zum Ausspähen von Daten nach § 202a Absatz 1 StGB-E - eine bloße Zugangsverschaffung nicht ausreichen lässt.

3. Der in Absatz 4 des § 202b StGB-E vorgesehene Qualifikationstatbestand dient in Anlehnung an § 202a Absatz 5 StGB-E insbesondere der Bekämpfung der schweren Kriminalitätsform des Organisierten Cybercrime, indem er die bandenmäßige Tatbegehung unter erschwerten Umständen (nämlich unter den Umständen des Absatz 3 Satz 2 Nummer 1 erste Alternative oder Nummer 2 bis 4) mit einer erhöhten Strafdrohung von sechs Monaten bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren, belegt. Anders als § 202a Absatz 5 StGB-E wurde dabei davon abgesehen, den § 202b Absatz 4 StGB als Verbrechenstatbestand auszugestalten, um dem auch bereits im jeweiligen Grundtatbestand zum Ausdruck kommenden abgestuften Unrechtsgehalt beider Straftatbestände Rechnung zu tragen.

Zu Nummer 3 (§ 202c StGB-E)

Zu Buchstabe a (Absatz 1 StGB-E)

Absatz 1 des § 202c StGB, der das Vorbereiten des Ausspähens und Abfangens von Daten als abstraktes Gefährdungsdelikt unter Strafe stellt, wird durch den Entwurf in zweierlei Hinsicht geändert:

Zum einen wird die zulässige Höchststrafe von zwei auf drei Jahren angehoben. Der Entwurf trägt damit dem Umstand Rechnung, dass die derzeit vorgesehene Strafrahmenobergrenze von zwei Jahren jedenfalls dann nicht mehr ausreichend ist, wenn ein besonders schwerer oder qualifizierter Fall des Ausspähens oder Abfangens von Daten im Sinne §§ 202a Absatz 4 und 5, 202b Absatz 3 und 4 StGB-E vorbereitet wird. Denn wer beispielsweise einen besonders schweren Fall des Ausspähens von Daten vorbereitet, verwirklicht ein höheres Unrecht als derjenige, der nur den Grundtatbestand einer Datenausspähung vorbereitet. Verschafft ein Täter einem anderen eine selbst programmierte Software zum Ausspähen von Accounts in dem Wissen, dass diese für ein gewerbsmäßiges Handeln verwendet wird, erscheint der vorgegebene Strafrahmen zu gering, auch wenn der Täter selbst nicht gewerbsmäßig vorging. Um dem differenzierten Unrechtsgehalt der in Betracht kommenden

Fallgestaltungen in einer schuldangemessenen Weise erfassen zu können, erscheint daher die Anhebung des Strafrahmenobergrenze für das Vorbereitungsdelikt des § 202c Absatz 1 StGB von zwei auf drei Jahren geboten.

Zum anderen verzichtet der Entwurf im Vergleich zur bisherigen Fassung darauf, die Tathandlung des Verbreitens in § 202c Absatz 1 StGB explizit im Grundtatbestand zu erwähnen, da die Verbreitung nur eine Form des ebenfalls in Absatz 1 erwähnten Zugänglichmachens ist, bei der die Tatobjekte an einen größeren, nach Zahl und Individualität unbestimmten oder für den Täter nicht mehr kontrollierbaren Personenkreis weitergeben werden (vgl. zur Definition der Tathandlung des Verbreitens etwa Eisele in: Schönke/Schröder, 30. Auflage 2018, § 202d Rn. 12). Diese Form der Zugänglichmachung soll künftig aufgrund des gesteigerten Unrechtsgehalts in § 202c Absatz 3 Satz 2 Nummer 2 StGB-E als Regelbeispiel für einen besonders schweren Fall einer Vorbereitungshandlung erfasst werden.

Zu Buchstabe b (Absätze 3 und 4 StGB-E)

Der Entwurf sieht ferner vor, zwei neue Absätze 3 und 4 in § 202c StGB einzufügen, um auch dem erhöhten Unrechtsgehalt besonders schwerer oder qualifizierter Vorbereitungshandlungen in einer schuldangemessenen Weise Rechnung tragen zu können.

1. Zu diesem Zweck schafft der Entwurf mit dem neuen Absatz 3 des § 202c StGB-E eine Strafzumessungsregel für besonders schwere Fälle von Vorbereitungshandlungen. Ein besonders schwerer Fall liegt nach Satz 2 des § 202c Absatz 3 StGB-E in der Regel vor, wenn die Vorbereitungshandlung gewerbs- oder bandenmäßig begangen wird (Nummer 1) oder die in Absatz 1 genannten Tatobjekte in Form von Sicherungscodes oder Computerprogrammen einer großen Anzahl von Personen zugänglich gemacht werden (Nummer 2). Eine große Anzahl von Personen liegt dabei entsprechend der zu § 263 Absatz 3 Nr. 2 StGB entwickelten Maßstäbe jedenfalls dann vor, wenn der Personenkreis mehr als fünfzig Personen umfasst. Die vorgeschlagenen Regelbeispiele weisen einen über den Normalfall hinausgehenden, gesteigerten Unrechtsgehalt auf, der sich mit dem Strafrahmen des Grundtatbestandes des § 202c Absatz 1 StGB nicht immer angemessen erfassen lässt.

2. Der vorgeschlagene neue Absatz 4 des § 202c StGB enthält einen Qualifikationstatbestand für den Fall, dass die Vorbereitungshandlung bandenmäßig begangen wird und dabei zugleich eines der Regelbeispiele aus § 202c Absatzes 3 Satz 2 Nummer 1 erste Alternative oder Nummer 2 StGB verwirklicht. Wer also bei der Vorbereitung eines Ausspähens oder Abfangens von Daten banden- und zugleich gewerbsmäßig handelt oder wer bei der Vorbereitung als Mitglied einer Bande die Sicherungscodes bzw. Computerprogramme einer großen Anzahl von Personen zugänglich macht, hat nach dem Entwurf eine Freiheitsstrafe von drei Monaten bis zu zehn Jahren zu befürchten. Diese Strafdrohung ist aus general- und spezialpräventiven Gründen geboten und mit Blick auf das verwirklichte Unrecht auch gerechtfertigt.

Zu Nummer 4 (§ 202d StGB-E)

Zu Buchstabe a (Absatz 1 StGB-E)

In Anlehnung an die Sachhehlerei (§ 259 Absatz 1 StGB) hebt der Entwurf die zulässige Höchststrafe bei der Datenhehlerei (§ 202d Absatz 1 StGB) von drei auf fünf Jahren Freiheitsstrafe an, mit der Folge, dass digitale Daten strafrechtlich gegen Hehlerei geschützt werden wie körperliche Gegenstände. Dies ist angesichts der gewachsenen gesellschaftlichen und wirtschaftlichen Bedeutung digitaler Daten nicht nur angemessen, sondern auch die konsequente Schlussfolgerung aus dem Umstand, dass die Datenhehlerei vom Gesetzgeber ursprünglich weitgehend nach dem Vorbild der Sachhehlerei konzipiert worden ist (vgl. BT-Drs. 18/5088, S. 24 ff., 45 ff.).

Selbst wenn man sich - wie der historische Gesetzgeber - für den Strafrahmen der Datenhehlerei an der Strafdrohung der praktisch wohl bedeutsamsten Vortat, nämlich der Datenausspähung nach § 202a Absatz 1 StGB, orientieren will (vgl. BT-Drs. 18/5088, S. 47), ist eine Anhebung der Strafobergrenze von drei auf fünf Jahre Freiheitsstrafe nur konsequent, da der Entwurf die Strafobergrenze in § 202a Absatz 1 StGB ebenfalls von drei auf fünf Jahre anhebt.

Schließlich stärkt die Anhebung der Strafobergrenze bei § 202d Absatz 1 StGB mit Blick auf die spezial- und generalpräventive Wirkung nicht nur den strafrechtlichen Schutz gegen Datenhehlerei, sondern in letzter Konsequenz auch den

strafrechtlichen Schutz digitaler Daten gegen die Vortaten (wie etwa §§ 202a, 202b StGB), da die Abschreckung potentieller Datenhehler auch den durch die Hehlerei geschaffenen Anreiz zur Verübung von Vortaten minimiert.

Der Entwurf streicht in § 202d Absatz 1 StGB - wie bei § 202c Absatz 1 StGB - das Wort "verbreiten", da die Verbreitung nur eine Form des ebenfalls in Absatz 1 erwähnten Zugänglichmachens ist, bei der die Daten an einen größeren, nicht mehr überschaubaren Personenkreis weitergegeben werden (vgl. zur Definition der Tathandlung des Verbreitens etwa Eisele in: Schönke/Schröder, 30. Auflage 2018, § 202d Rn. 12). Diese Form der Zugänglichmachung soll künftig aufgrund des gesteigerten Unrechtsgehalts in § 202d Absatz 3 Satz 2 Nummer 2 StGB-E als Regelbeispiel für einen besonders schweren Fall erfasst werden.

Zu Buchstabe b (Absätze 2 bis 4 StGB-E)

Der Entwurf führt mit dem neuen Absatz 2 auch für die Datenhehlerei eine Versuchsstrafbarkeit ein. Ferner schafft er mit den Absätzen 3 und 4 eine Strafzumessungsregel für besonders schwere Fälle und einen Qualifikationstatbestand, um auch Taten mit einem erhöhten Unrechtsgehalt in einer schuldangemessenen Weise bestrafen zu können. Ein praktisches Bedürfnis für erhöhte Strafdrohungen bei der Datenhehlerei besteht insbesondere mit Blick auf den lebhaften Handel mit "gestohlenen Daten" im Darknet. So stellt der Handel mit Kreditkartendaten oder Accounts bei Zahlungsdienstleistern und Verkaufsplattformen auf den universellen Marktplätzen im Darknet, gleich nach dem Angebot von Betäubungsmitteln, derzeit eine der größten Kategorien dar (z.B. Kategorie „Fraud“ auf den Plattformen „Dream Market“ oder „Wallstreet Market“). Im Einzelnen:

1. In Parallele zu § 259 Absatz 3 StGB, wo die Versuchsstrafbarkeit für die Sachhehlerei geregelt ist, erklärt der Entwurf mit dem neuen Absatz 2 des § 202d StGB-E auch den Versuch des Vergehens der Datenhehlerei nach § 202d Absatz 1 StGB für strafbar. Die Strafbarkeit des Versuchs des vorgeschlagenen Verbrechenstatbestandes nach § 202d Absatz 4 StGB-E ergibt sich aus §§ 23 Absatz 1 erste Alternative, 12 Absatz 1 StGB.

2. Der Entwurf schafft mit dem neuen Absatz 3 des § 202d StGB-E die Möglichkeit, besonders schwere Fälle der Datenhehlerei mit Freiheitsstrafe von sechs

Monaten bis zu zehn Jahren zu bestrafen. Die besonders schweren Fälle werden dabei in den Nummern 1 bis 4 des § 202d Absatz 3 Satz 2 StGB-E mit vier Regelbeispielen konkretisiert, die weitgehend den Regelbeispielen aus § 202a Absatz 4 Satz 2 Nummer 1 bis 4 und § 202b Absatz 3 Satz 2 Nummer 1 bis 4 StGB entsprechen bzw. zumindest an diese angelehnt sind.

So werden als erschwerende Umstände in Nummer 1 die Gewerbs- oder Bandenmäßigkeit genannt. Nummer 2 stuft die Datenhehlerei in der Regel als besonders schweren Fall ein, wenn sie eine große Menge von Daten betrifft oder in der Absicht begangen wird, durch die fortgesetzte Tatbegehung sich oder einem anderen die Daten einer großen Anzahl von Personen zu verschaffen oder die Daten einer großen Anzahl von Personen zugänglich zu machen. Über dieses Regelbeispiel sollen insbesondere auch solche Fälle erfasst werden, in denen der Täter an eine große Anzahl von Personen jeweils nur eine kleine Datenmenge verbreitet. Gerade auf den Marketplaces im Darknet ist es durchaus üblich, dass große Mengen von aktuellen und daher werthaltigen Zahlungsdaten in kleinere Tranchen geteilt und veräußert werden, da hierdurch ein weitaus höherer Gewinn zu erzielen ist. Nummer 3 stellt auf die Betroffenheit von Daten kritischer Infrastrukturen oder die Gefährdung der Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder ab. Schließlich ist nach Nummer 4 ein besonders schwerer Fall in der Regel anzunehmen, wenn höchstpersönliche Daten Gegenstand der Datenhehlerei sind. Zur näheren Konkretisierung dieser Regelbeispiele kann weitgehend auf die obigen Ausführungen zu § 202a Absatz 4 StGB-E Bezug genommen werden, die an dieser Stelle entsprechend gelten.

3. Der vorgeschlagene Absatz 4 des § 202d StGB-E erhebt in Anlehnung an § 202a Absatz 5 StGB-E und § 260a Absatz 1 StGB die bandenmäßig begangene Datenhehlerei zum Verbrechen, sofern der Täter zugleich einen der erschwerenden Umstände aus § 202d Absatz 3 Satz 2 Nummer 1 erste Alternative oder Nummer 2 bis 4 StGB-E verwirklicht. Hierdurch soll vor allem dem organisierten Schwarzmarkthandel mit "gestohlenen" Daten im Darknet Rechnung getragen werden.

Zu Buchstabe c (Absätze 5 und 6 StGB-E)

Es handelt sich lediglich um eine Folgeänderung aus der Einfügung der neuen Absätze 2 bis 4, die dazu führt, dass die bisherigen Absätze 2 und 3 zu den Absätzen 5 und 6 werden.

Zu Nummer 5 (§ 205 StGB-E)

Zu Buchstabe a (Absatz 1 Satz 2 StGB-E)

Nach dem Entwurf soll im Ergebnis in dem Umfang an dem Strafantragserfordernis für das Ausspähen von Daten (§ 202a StGB), das Abfangen von Daten (§ 202b StGB) und die Datenhehlerei (§ 202d StGB) festgehalten werden, in dem es bislang nach § 205 Absatz 1 Satz 2 StGB gilt. Die Strafantragsregelung in § 205 Absatz 1 Satz 2 StGB ist daher dahingehend abzuändern, dass sie nur die Grundtatbestände der vorgenannten Delikte (§§ 202a Absatz 1, 202b Absatz 1, 202d Absatz 1StGB-E) erfasst, nicht aber auch die Strafzumessungsregeln und die Qualifikationstatbestände (§§ 202a Absätze 4 und 5, 202b Absätze 3 und 4, 202d Absätze 3 und 4 StGB-E), die der Entwurf für die vorgenannten Delikte vorschlägt.

Eine Einbeziehung der Regelungen zu den besonders schweren und qualifizierten Fällen in das Strafantragserfordernis des § 205 Absatz 1 Satz 2 StGB erscheint mit Blick auf den erhöhten Unrechtsgehalt dieser Taten nicht sachgerecht, zumal die Strafverfolgungsbehörden in diesen Fällen aufgrund der Schwere der Taten ohnehin in aller Regel das besondere öffentliche Interesse an der Strafverfolgung zu bejahen hätten. Dementsprechend hat der Gesetzgeber im Übrigen auch bei den Diebstahlsdelikten in § 248a StGB davon abgesehen, die besonders schweren und qualifizierten Fallgestaltungen der §§ 243 ff. StGB dem Strafantragserfordernis zu unterstellen.

Zu Buchstabe b (Absatz 2 Satz 1 StGB-E)

In § 205 Absatz 2 Satz 1 StGB, der den Übergang des Antragsrechts im Falle des Todes des Verletzten auf die Angehörigen nach § 77 Absatz 2 StGB regelt, wird durch den Entwurf der einschränkende zweite Halbsatz, der diesen Übergang bei Taten nach §§ 202a, 202b und 202 StGB bislang ausschließt, gestrichen. Diese Rechtsverkürzung ist gerade angesichts der zunehmenden Werthaltigkeit vieler elektronischer Daten heute nicht mehr angemessen und zeitgemäß (so Graf in Mü-

Ko-StGB, 3. Auflage 2017, § 205 Rn. 13). Die Streichung erscheint ferner sachgerecht, weil beim Ausspähen und anschließenden Veröffentlichen von höchstpersönlichen Daten ein Bedürfnis besteht, es auch den Angehörigen zu ermöglichen, gemäß § 77 Absatz. 2 StGB eine Strafverfolgung in die Wege leiten zu können.

Zu Nummer 6 (§ 303a StGB-E)

Zu Buchstabe a (Absätze 3 und 4 StGB-E)

Der Entwurf sieht in den neuen Absätzen 3 und 4 des § 303a StGB-E erhöhte Strafdrohungen für besonders schwere und qualifizierte Fälle vor, die sich vom Strafrahmen des Grundtatbestandes in § 303a Absatz 1 StGB und des bereits vorhandenen Qualifikationstatbestandes in § 303b Absatz 1 Nummer 1 StGB nicht immer angemessen erfassen lassen. Das Interesse der Verfügungsberechtigten an der ungestörten, jederzeit möglichen Nutzung ihrer in Datenspeichern enthaltenen Informationen erfordert angesichts der gestiegenen gesellschaftlichen und wirtschaftlichen Bedeutung digitaler Daten und des starken Anstiegs der Fallzahlen in diesem Deliktsbereich in den letzten Jahren aus general- und spezialpräventiven Gründen einen verstärkten strafrechtlichen Schutz (vgl. zum Anstieg der Fallzahlen Wieck-Noodt in: MüKo-StGB, 3. Auflage 2019, § 303a Rn. 5).

1. Zu diesem Zweck schafft der Entwurf in dem neuen Absatz 3 des § 303a StGB-E eine Strafzumessungsregel für besonders schwere Fälle, die in ihrem Satz 2 zur Konkretisierung auch vier Regelbeispiele mit erschwerenden Umständen benennt, nämlich die Gewerbs- oder Bandenmäßigkeit (Nummer 1), die große Menge an betroffenen Daten oder die große Anzahl betroffener Personen (Nummer 2), die Daten kritischer Infrastrukturen oder die Gefährdung der Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder (Nummer 3) sowie der höchstpersönliche Charakter der tatgegenständlichen Daten (Nummer 4). Die Auslegung dieser Regelbeispiele kann sich weitgehend an den entsprechenden bzw. ähnlichen Regelbeispielen in § 202a Absatz 4 Satz 2 StGB-E, § 202b Absatz 3 Satz 2 StGB-E, § 202d Absatz 3 Satz 2 StGB-E orientieren.

   Die vorgeschlagene Strafdrohung (Freiheitsstrafe bis zu fünf Jahre oder Geldstrafe) erscheint unter Berücksichtigung der drohenden Schäden für das geschützte Rechtsgut erforderlich, aber auch ausreichend. Insbesondere sieht der

Entwurf davon ab, eine im Mindestmaß erhöhte Strafdrohung festzusetzen. Hintergrund ist, dass der Gesetzgeber den Tatbestand der Datenveränderung (§ 303a StGB) weitgehend in Anlehnung an und als Ergänzung zum Tatbestand der Sachbeschädigung (§ 303 StGB) geschaffen und ausgestaltet hat (vgl. BT-Drs. 10/5058, S. 34 f.). Die in den qualifizierten Fällen der Sachbeschädigung vorgesehenen Strafrahmen nach §§ 304 ff. StGB enthalten aber ganz überwiegend (mit Ausnahme des Sonderfalls der einfachen Brandstiftung nach § 306 StGB) auch keine im Mindestmaß erhöhte Strafdrohung. Vielmehr sehen beispielsweise die §§ 305 Absatz 1, 305a Absatz 1 StGB für die Zerstörung von Bauwerken (wie etwa Brücken oder Schienennetz der Eisenbahn) und von wichtigen Arbeitsmitteln (etwa der Polizei, der Bundeswehr oder des Katastrophenschutzes) eine Freiheitsstrafe von bis zu fünf Jahren oder Geldstrafe vor, ohne die untere Grenze des Strafrahmens über das Mindestmaß hinaus zu erhöhen.

2. Der Entwurf sieht zudem in dem vorgeschlagenen Absatz 4 des § 303a StGB-E eine Qualifikationstatbestand vor, wonach mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft wird, wer die Datenveränderung bandenmäßig begeht und dabei zugleich einen der erschwerenden Umstände verwirklicht, die in Absatz 3 Satz 2 Nummer 1 erste Alternative oder Nummer 2 bis 4 genannt sind. Dieser erhöhte Strafrahmen scheint insbesondere zur Bekämpfung der schwerwiegenden Kriminalitätsform des Organisierten Cybercrime geboten. Durch die gleichzeitige Regelung eines minder schweren Falls bleibt es den Gerichten zudem möglich, auch auf Fallgestaltungen, in denen die strafmildernden Umstände beträchtlich überwiegen, angemessen zu reagieren.

Zu Buchstabe b (Absatz 5 StGB-E)

Der bisherige Absatz 3, der für die Vorbereitung einer Datenveränderung die entsprechende Anwendung des § 202c StGB anordnet, wird Absatz 5. Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 7 (§ 303b StGB-E)

Zu Buchstabe a (Absatz 4 StGB-E)

Zu Buchstabe aa (Absatz 4 Satz 1 StGB-E)

Der Entwurf erweitert den Anwendungsbereich der Strafzumessungsregel für besonders schwere Fälle in § 303b Absatz 4 StGB, der bislang nach Satz 1 auf die Fälle des Absatzes 2 beschränkt ist, auf die Fälle des Absatzes 1. Dies hat zur Folge, dass eine Strafschärfung nicht mehr nur dann möglich ist, wenn die Computersabotage nach Absatz 2 einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde betrifft, sondern auch dann, wenn die Computersabotage nach Absatz 1 zum Nachteil einer Privatperson begangen wird.

Diese Erweiterung des Anwendungsbereichs der Strafzumessungsregel erscheint aus general- und spezialpräventiven Gründen zum Schutz von Privatpersonen geboten, da auch deren informationstechnische Systeme zunehmend von Sabotageakten betroffen sind. Breites Aufsehen in der Öffentlichkeit erregten in den letzten Jahren insbesondere die Schadprogramme "Locky", "WannaCry" und „GrandCrab“, sowie andere Verschlüsselungs- bzw. Erpressungstrojaner, die massenhaft Computersysteme auch von Privatpersonen infizierten, den Zugriff auf die Systeme sperrten bzw. die darauf gespeicherten Daten verschlüsselten und die Freigabe von der Zahlung eines "Lösegeldes" abhängig machten. Anders als im gewerblichen Umfeld sind im privaten Bereich ausreichende Backups häufig nicht vorhanden. Der Verlust der gesamten privaten „digitalen Vergangenheit“, bestehend aus unersetzbaren Dokumenten, Lichtbildern und sonstigen wichtigen Daten, führt dann zu einer erheblichen Beeinträchtigung des Sicherheitsgefühls der Opfer.

Die Erweiterung des Anwendungsbereichs der Strafzumessungsregel ist aber nicht nur aus Gründen der General- und Spezialprävention geboten, sondern mit Blick auf das von § 303b StGB geschützte Rechtsgut auch sachgerecht und konsequent, da der Straftatbestand der Computersabotage ganz allgemein das Interesse der Betreiber und Nutzer von Datenverarbeitungen an deren ordnungsgemäßer Funktionsweise schützt. Mag die Computersabotage im betrieblichen, unternehmerischen oder behördlichen Bereich auch zu höheren Schäden führen können, so kann es doch nicht überzeugen, dass beispielsweise der Eintritt eines Vermögensverlusts großen

Ausmaßes (§ 303b Absatz 4 Satz 2 Nummer 1 StGB) nur deshalb keine Auswirkung auf den in Betracht kommenden Strafrahmen haben soll, weil es eine Privatperson ist, die den Verlust erleidet. Der Verlust von 50.000 EUR oder mehr dürfte eine Privatperson typischerweise sogar noch empfindlicher treffen als ein großes Unternehmen.

Zu Buchstabe bb (Absatz 4 Satz 2 Nummer 1 StGB-E)

Der Entwurf ergänzt den in Nummer 1 des § 303b Absatz 4 Satz 2 StGB genannten erschwerenden Umstand der Herbeiführung eines Vermögensverlusts großen Ausmaßes um ein weiteres Regelbeispiel. Danach soll künftig in Anlehnung an § 263 Absatz 3 Satz 2 Nummer 2 StGB ein besonders schwerer Fall nicht mehr nur dann vorliegen, wenn der Täter einen Vermögensverlust großen Ausmaßes herbeiführt (erste Alternative), sondern auch dann, wenn der Täter in der Absicht handelt, durch die fortgesetzte Begehung von Computersabotage eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen (Alternative 2). Diese Ergänzung trägt dem Umstand Rechnung, dass das Handeln eines Täters, der durch mehrere rechtlich selbständige Sabotagehandlungen zwar eine große Zahl von Menschen schädigt oder schädigen will, wobei die Schäden jeweils aber kein großes Ausmaß erreichen, nicht unter die bisherige Regelung in § 303b Absatz 4 Satz 2 Nummer 1 StGB subsumiert werden kann. Denn eine Addition der Einzelschäden kommt weder bei mehreren Tatopfern noch bei mehreren rechtlich selbständigen Handlungen in Betracht. Bei der Auslegung der vom Entwurf vorgeschlagenen Neuregelung der Regelbeispiele in Nummer 1 kann auf die Auslegung der gleichlautenden Regelung in § 263 Absatz 3 Satz 2 Nummer 2 StGB zurückgegriffen werden.

Zu Buchstabe cc (Absatz 4 Satz 2 Nummer 2 StGB-E)

Der Entwurf trägt mit der Ersetzung des Wortes "Computersabotage" in Nummer 2 des § 303b Absatz 4 Satz 2 StGB durch die allgemeine Formulierung "Taten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b" dem Umstand Rechnung, dass sich Banden im Bereich der Cyberkriminalität in aller Regel nicht ausschließlich zur Begehung von Delikten der Computersabotage, sondern allgemein zur Begehung von Delikten nach §§ 202a bis 202d, 263a, 269, 303a oder 303b StGB zusammenschließen.

Zu Buchstabe dd (Absatz 4 Satz 2 Nummer 3 StGB-E)

Die Nummer 3 des § 303b Absatz 4 Satz 2 StGB wird durch die Neufassung im Entwurf in zweierlei Hinsicht geändert:

Zum einen ersetzt der Entwurf die bisherige Fassung der ersten Alternative der Nummer 3, die eine Beeinträchtigung der Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen verlangt, durch die etwas allgemeiner gefasste Formulierung, dass die Datenverarbeitung einer kritischen Infrastruktur erheblich gestört sein muss. Damit soll einem zu engen Verständnis, das sich etwa aus dem Begriff "lebenswichtig" ergeben könnte, vorgebeugt und gewährleistet werden, dass alle kritischen Infrastrukturen den gleichen strafrechtlichen Schutz erhalten. Zugleich wird damit eine begriffliche Anpassung an die entsprechenden Regelbeispiele bei den anderen Straftatbeständen aus § 202a, 202b, 202d, 303a StGB-E erreicht (vgl. § 202a Absatz 4 Satz 2 Nummer 3, § 202b Absatz 3 Satz 2 Nummer 3, § 202d Absatz 3 Satz 2 Nummer 3, § 303a Absatz 3 Satz 2 Nummer 3 StGB-E).

Zum anderen passt der Entwurf auch die Alternative 2 der Nummer 3 an die entsprechenden Regelungen bei den vorgenannten Straftatbeständen an. Hierfür wird die bereits jetzt im Gesetz erwähnte Sicherheit der Bundesrepublik Deutschland um die Sicherheit eines der Länder ergänzt. Ferner erweitert der Entwurf den Anwendungsbereich der Alternative 2 auch insofern, als er keine Beeinträchtigung der Sicherheit mehr verlangt, sondern eine Gefährdung der Sicherheit ausreichen lässt. Diese Erweiterung ist mit Blick auf das Ausmaß der potentiell drohenden Schäden sachgerecht, zumal es oftmals nur vom Zufall abhängen wird, ob sich die geschaffene Gefahr auch in konkreten Sicherheitsbeeinträchtigungen realisiert. Vor diesem Hintergrund stellt es auch keine unverhältnismäßige Sanktion dar, wenn derjenige, der eine Computersabotage begeht und dabei billigend in Kauf nimmt, beispielsweise die Verteidigungsfähigkeit und damit die äußere Sicherheit der Bundesrepublik Deutschland zu gefährden, eine Freiheitsstrafe von mindestens sechs Monaten bis maximal zehn Jahren zu befürchten hat. Eine solche Strafdrohung scheint vielmehr - wie bei einem Cyberangriff auf kritische Infrastrukturen - aufgrund des hohen Gefahrenpotentials aus generalpräventiven Gründen geboten, um potentielle Täter von vornherein von der Begehung entsprechender Taten abzuschrecken.

Zu Buchstabe b (Absätze 5 und 6 StGB-E)

Der Entwurf schlägt des Weiteren vor, in § 303b StGB zwei neue Absätze 5 und 6 mit einem qualifizierten und einem erfolgsqualifizierten Tatbestand für Fallgestaltungen einzufügen, die sich aufgrund ihres erhöhten Unrechtsgehalts mit den bestehenden Strafrahmen der Absätze 1, 2 oder 4 nicht in einer schuldangemessenen Weise erfassen und bestrafen lassen.

1. Der in Absatz 5 des § 303b StGB-E vorgeschlagene Qualifikationstatbestand erhebt in Anlehnung an § 202a Absatz 5 StGB-E die bandenmäßig begangene Computersabotage unter erschwerten Umständen zum Verbrechenstatbestand. Wer also als Mitglied einer Bande handelt und dabei zugleich kumulativ einen der in § 303b Absatz 4 Satz 2 Nummer 1, Nummer 2 erste Alternative oder Nummer 3 genannten, erschwerenden Umstände verwirklicht, hat nach dem Entwurf eine Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen eine Freiheitstrafe von sechs Monaten bis zu fünf Jahren zu erwarten. Der Qualifikationstatbestand erfasst insbesondere durch die kumulative Verbindung der gewerbs- und bandenmäßigen Begehungsweise wesentliche Bereiche der organisierten und damit schweren Cyberkriminalität, so dass die Ausgestaltung als Verbrechenstatbestand sachgerecht ist. Dies gilt umso mehr, als alle Bereiche des modernen Lebens aufgrund der fortschreitenden Digitalisierung in einem zunehmenden Maße von einem störungsfreien Funktionieren ihrer Datenverarbeitungsanlagen abhängig sind und mit Akten der Computersabotage gerade im Bereich der Wirtschaft immense wirtschaftliche Schäden verbunden sein können, die etwa im Falle von Produktionsausfällen bis zum wirtschaftlichen Ruin eines Unternehmens und dem Verlust von Arbeitsplätzen reichen können.

2. Der Entwurf schlägt zudem vor, in einem neuen Absatz 6 eine als Verbrechenstatbestand ausgestaltete Erfolgsqualifikation für den Fall zu schaffen, dass der Täter durch die Computersabotage wenigstens leichtfertig den Tod (Satz 1) oder eine schwere Gesundheitsschädigung (Satz 2) eines anderen Menschen verursacht. Hierdurch sollen insbesondere Fallgestaltungen angemessen erfasst werden, in denen der Täter durch die Computersabotage vorsätzlich eine erhebliche Störung der informationstechnischen Systeme von Krankenhäusern, Flughäfen oder anderen kritischen Infrastrukturen herbeiführt und dadurch wenigstens

leichtfertig den Tod oder eine schwere Gesundheitsschädigung eines Menschen verursacht (etwa weil lebenserhaltende Geräte in einem Krankenhaus oder die Steuerungselektronik von Ampelanlagen oder Herzschrittmachern ausfallen, oder weil die Flugsicherungssysteme eines Fluglotsen derart gestört werden, dass es zu einem Absturz oder Zusammenstoß zweier Flugzeuge kommt). Angesichts der schweren Tatfolgen ist - in Anlehnung an die Strafrahmen der §§ 226 Absatz 1, 227 Absatz 1 StGB - beim Verlust eines Menschenlebens eine im Mindestmaß erhöhte Strafdrohung von nicht unter drei Jahren und bei einer schweren Gesundheitsschädigung eine Strafdrohung von einem bis zu zehn Jahren sachgerecht, um eine schuldangemessene Bestrafung zu gewährleisten und general- wie spezialpräventiven Strafbedürfnissen gerecht zu werden. Sofern im konkreten Einzelfall strafmildernde Umstände beträchtlich überwiegen sollten, ist durch die gleichzeitige Regelung von minder schweren Fällen mit niedrigeren Strafrahmen von einem bis zehn Jahren (im Fall der Verursachung des Todes eines Menschen) und von sechs Monaten bis zu fünf Jahren (im Fall der Verursachung einer schweren Gesundheitsschädigung) sichergestellt, dass die Gerichte auch in solchen Fällen schuldangemessen reagieren können.

Zu Buchstabe c (Absatz 7 StGB-E)

Der bisherige Absatz 5, der für die Vorbereitung einer Computersabotage die entsprechende Anwendung des § 202c StGB anordnet, wird Absatz 7. Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 2 (Änderung der Strafprozessordnung)

Zu Nummer 1 (§ 100a Absatz 2 Nummer 1 StPO)

Zu Buchstabe a (Buchstabe h StPO-E)

Der Entwurf erweitert den Anwendungsbereich der Telekommunikationsüberwachung, indem er den Straftatenkatalog des § 100a Absatz 2 StPO um die schweren Computer- und Datendelikte nach §§ 202a, 202b Absatz 3 und 4, 202c Absatz 3 und 4, 202d, 303a Absatz 3 und 4, 303b Absatz 2 bis 6 StGB-E ergänzt. Diese Delikte werden entsprechend der bisherigen Gesetzessystematik, welche die Katalogtaten

nach ihrer Paragraphenzahl in aufsteigender Reihenfolge anordnet, in den Katalog als neuer Buchstabe h aufgenommen.

Die Aufnahme dieser Delikte in den Anlasstatenkatalog des § 100a Absatz 2 Satz 1 StPO ist zur effektiven Bekämpfung der schweren Cyberkriminalität kriminalpolitisch notwendig und unter Berücksichtigung der bundesverfassungsgerichtlichen Vorgaben auch zulässig.

Notwendig ist die Aufnahme, da ohne die Eröffnung technischer Ermittlungsmaßnahmen wie der Telekommunikationsüberwachung Straftaten aus dem Bereich der Cyberkriminalität kaum erfolgreich aufgeklärt werden können. Diese Taten werden der Natur der Sache nach in den allermeisten Fällen auch oder ausschließlich unter Zuhilfenahme von Telekommunikationsdiensten begangen, so dass die Überwachung der Telekommunikation zum Beispiel in Form der Server- oder DSL-Überwachung oftmals den einzigen Ermittlungsansatz zur Identifizierung der Täter und zur Aufklärung des Sachverhalts darstellen. Der Entwurf trägt damit den Bedürfnissen der Strafverfolgungspraxis Rechnung, die seit längerem eine entsprechende Erweiterung des Anwendungsbereichs der Telekommunikationsüberwachung fordert.

Die Aufnahme der genannten Computer- und Datendelikte in den Katalog des § 100a Absatz 2 StPO ist verfassungsrechtlich auch zulässig. Das Bundesverfassungsgericht gewährt dem Gesetzgeber ausdrücklich einen Beurteilungsspielraum bei der Bestimmung des Unrechtsgehalts eines Delikts und bei der Entscheidung darüber, welche Straftaten er zum Anlass für bestimmte strafprozessuale Ermittlungsmaßnahmen machen will (BVerfG NJW 2012, 833 [836]). Erforderlich für die Aufnahme in den Katalog von Anlasstaten ist aufgrund des Eingriffs in das Fernmeldegeheimnis aus Art. 10 GG zur Wahrung der Verhältnismäßigkeit lediglich, dass es sich um eine schwere Straftat handelt. Für die Qualifizierung einer Straftat als schwer können insbesondere der Strafrahmen, aber auch das geschützte Rechtsgut und dessen Bedeutung für die Rechtsgemeinschaft von Bedeutung sein (BVerfG NJW 2012, 833 [836]).

Schwere Straftaten sind nach der Definition des Gesetzgebers grundsätzlich solche Straftaten, die mit einer Mindesthöchststrafe von fünf Jahren Freiheitsstrafe bedroht sind (BT-Drs 16/5846, S. 40). In Einzelfällen kann aufgrund der besonderen Bedeutung des geschützten Rechtsguts oder des besonderen öffentlichen Interesses an

der Strafverfolgung sogar auch eine geringere Freiheitsstrafe ausreichen. Bei dieser Strafrahmenbetrachtung bleiben Strafmilderungen, die das Gesetz für minder schwere Fälle vorsieht, unberücksichtigt (BT-Drs 16/5846, S. 40). Das Bundesverfassungsgericht hat diese Definition mit der Einschränkung gebilligt, dass neben der Strafrahmenbetrachtung auch eine Gesamtschau, die insbesondere die jeweils geschützten Rechtsgüter in den Blick nimmt, die Qualifizierung einer Straftat als "schwer" rechtfertigten muss (BVerfG NJW 2012, 833 [836]).

Nach diesen Maßstäben ist die Aufnahme der Computer- und Datendelikte nach §§ 202a, 202b Absatz 3 und 4, 202c Absatz 3 und 4, 202d, 303a Absatz 3 und 4, 303b Absatz 2 bis 6 StGB-E in den Katalog der schweren Straftaten aus § 100a Absatz 2 StPO nicht zu beanstanden:

1. Die besonders schweren bzw. qualifizierten Fälle des Ausspähens von Daten nach § 202a Absatz 4 und 5 StGB-E, des Abfangens von Daten nach § 202b Absatz 4 StGB-E, des Vorbereitens von bestimmten Delikten nach § 202c Absatz 4 StGB-E, der Datenhehlerei nach § 202d Absatz 3 und 4 StGB-E, der Datenveränderung nach § 303a Absatz 4 StGB-E und der Computersabotage nach § 303b Absatz 4 bis 6 StGB-E sehen alle eine höhere Höchststrafe als fünf Jahre vor, so dass es sich nach dem Begriffsverständnis des Bundesverfassungsgerichts (BVerfG NJW 2004, 999 [1011]) abstrakt nicht bloß um schwere, sondern sogar um besonders schwere Straftaten handelt.

2. Soweit der Entwurf darüber hinaus vorschlägt, den Straftatenkatlog auch um die Grundtatbestände des Ausspähens von Daten nach § 202a Absatz 1 StGB-E und der Datenhehlerei nach § 202d Absatz 1 StGB-E, um die besonders schweren Fälle des Abfangens von Daten nach 202b Absatz 3 StGB-E, des Vorbereitens bestimmter Datendelikte nach § 202c Absatz 3 StGB-E und der Datenveränderung nach § 303a Absatz 3 StGB sowie um den Qualifikationstatbestand der Computersabotage nach § 303b Absatz 2 StGB zu ergänzen, handelt es sich um Delikte, deren Begehung mit einer Höchststrafe von fünf Jahren Freiheitsstrafe bedroht ist.

   Diese Delikte sind auch bei einer Gesamtschau, welche die geschützten Rechtsgüter und deren Bedeutung für die Rechtsgemeinschaft in den Blick nimmt, als

"schwer" einzustufen. Die §§ 202a bis 202d StGB schützen das formelle Datengeheimnis, § 303a StGB das Interesse des Berechtigten an der unversehrten Verwendbarkeit seiner Daten und § 303b StGB das Interesse aller Betreiber und Nutzer von Datenverarbeitungen allgemein an deren ordnungsgemäßer Funktionsweise (vgl. Graf in: MüKo-StGB, 3. Aufl. 2017, § 202a Rn. 2, § 202b Rn. 2, § 202c Rn. 2, § 202d Rn. 3, § 303a Rn. 2, § 303b Rn. 1). Diesen Rechtsgütern kommt in der modernen Informationsgesellschaft, in der informationstechnische Systeme allgegenwärtig und die Menschen auf die Nutzung dieser Systeme zunehmend angewiesen sind, eine hohe Bedeutung zu. Das Bundesverfassungsgericht hat daraus sogar ein grundrechtlich erhebliches Schutzbedürfnis gefolgert und aus dem allgemeinen Persönlichkeitsrecht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet (BVerfG NJW 2008, 822 [825]). Vor diesem Hintergrund besteht ein hohes öffentliches Aufklärungsinteresse in Bezug auf solche Delikte, die sich gegen die vorgenannten Rechtsgüter richten. Dies gilt umso mehr, als die Cyberkriminalität inzwischen ein Ausmaß erreicht hat, das die Privatsphäre und das Sicherheitsgefühl der Bevölkerung massiv bedroht, die Grundlagen von Staat, Wirtschaft und Gesellschaft gefährdet und zudem geeignet ist, das Vertrauen in den Rechtsstaat und die Handlungsfähigkeit staatlicher Organe nachhaltig zu erschüttern. Die Zuordnung der vorgenannten Delikte zu den schweren Straftaten ist daher vom Beurteilungsspielraum des Gesetzgebers umfasst.

Zu Buchstabe b (Buchstabe i bis v StPO-E)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 2 (§ 100b Absatz 2 Nummer 1 StPO-E)

Zu Buchstabe a (Buchstabe f StPO-E)

Zur effektiven Bekämpfung von Cyberkriminalität erweitert der Entwurf ferner den Anwendungsbereich der Online-Durchsuchung, indem er den Straftatenkatalog des § 100b Absatz 2 StPO um die besonders schweren Computer- und Datendelikte nach §§ 202a Absatz 4 und 5, 202b Absatz 4, 202c Absatz 4, 202d Absatz 3 und 4, 303a Absatz 4 und 303b Absatz 4 bis 6 StGB-E ergänzt.

Diese Ergänzung ist notwendig, da mit der fortschreitenden, alle Lebensbereiche durchdringenden Digitalisierung auch die Bedrohung durch die Cyberkriminalität drastisch zugenommen hat. Die Täter sind dabei derzeit für die Strafverfolgungsbehörden nicht oder nur schwer zu ermitteln, da diese vermehrt die Möglichkeiten der Anonymisierung nutzen, die ihnen das Internet und die moderne Informationstechnik bietet. Die Telekommunikationsüberwachung nach § 100a StPO reicht dabei alleine nicht aus, um die Täter und Teilnehmer zu identifizieren, die verwendete Infrastruktur aufzuhellen und die dahinter stehenden Netzwerke aufzudecken. Denn die Maßnahme nach § 100a StPO erlaubt nur die Überwachung der laufenden Telekommunikation, nicht aber den Zugriff auf die auf einem informationstechnischen System gespeicherten Daten (etwa aus einer bereits beendeten Telekommunikation des Täters). Diese Daten können für die Täteridentifizierung, die Aufhellung der verwendeten Infrastruktur und das Führen des Tatnachweises im Bereich der schwer ermittelbaren Cyberkriminalität aber von entscheidender Bedeutung sein. Umso wichtiger ist es daher, dass die Strafverfolgungsbehörden bei Taten in der digitalen Welt auch digital ermitteln können. Dafür ist es unabdingbar, dass den Strafverfolgungsbehörden bei besonders schweren Computer- und Datendelikten die Möglichkeit eingeräumt wird, im Wege der Online-Durchsuchung verdeckt auf fremde informationstechnische Systeme und die darauf gespeicherten Daten zuzugreifen.

Diese Notwendigkeit rechtfertigt indes nicht, die Online-Durchsuchung für alle Formen der Cyberkriminalität zuzulassen. Denn mit dieser Ermittlungsmaßnahme ist ein schwerwiegender Eingriff in das allgemeine Persönlichkeitsrecht nach Art. 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verbunden, der nach der Rechtsprechung des Bundesverfassungsgerichts in seiner Intensität mit der Eingriffsintensität einer Wohnraumüberwachung vergleichbar ist (BVerfG NJW 2016, 1781 [1794]). Folglich kommt eine Online-Durchsuchung mit Blick auf den Verhältnismäßigkeitsgrundsatz nur bei besonders schweren Straftaten in Betracht. Diese besondere Schwere weisen nach den Vorgaben des Bundesverfassungsgerichts nur solche Straftaten auf, die mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bedroht sind (BVerfG NJW 2004, 999 [1011]).

Eine solche Mindesthöchststrafe von mehr als fünf Jahren sehen all diejenigen Delikte vor, die nach dem Entwurf in den Katalog des § 100b Absatz 2 StPO

aufgenommen werden sollen. So sehen die besonders schweren bzw. qualifizierten Fälle des Ausspähens von Daten nach § 202a Absatz 4 und 5 StGB-E, des Abfangens von Daten nach § 202b Absatz 4 StGB-E, des Vorbereitens von bestimmten Delikten nach § 202c Absatz 4 StGB-E, der Datenhehlerei nach § 202d Absatz 3 und 4 StGB-E, der Datenveränderung nach § 303a Absatz 4 StGB-E und der Computersabotage nach § 303b Absatz 4 bis 5 StGB-E alle eine Höchststrafe von zehn Jahren vor. Der erfolgsqualifizierte Verbrechenstatbestand nach § 303b Absatz 6 StGB-E (in Verbindung mit § 38 Absatz 2 StGB) sieht sogar eine Höchststrafe von fünfzehn Jahren vor. Es handelt sich damit um besonders schwere Straftaten, die insbesondere mit Blick auf die betroffenen Rechtsgüter ein besonders schweres Tatunrecht aufweisen und damit den Bereich der mittleren Kriminalität eindeutig deutlich übersteigen. Die genannten Straftaten fügen sich daher in verfassungsrechtlich nicht zu beanstandender Weise in den bereits bestehenden Straftatenkatalog des § 100b Absatz 2 StPO ein.

Zu Buchstabe b (Buchstabe g bis n StPO-E)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 3 (§ 100g Absatz 2 Satz 2 Nummer 1 StPO-E)

Zu Buchstabe a (Buchstabe e StPO-E)

Der Entwurf sieht schließlich vor, die in den §§ 202a Absatz 4 und 5, 202b Absatz 4, 202c Absatz 4, 202d Absatz 3 und 4, 303a Absatz 4 und 303b Absatz 4 bis 6 StGB-E vorgeschlagenen Delikte in den Katalog des § 100g Absatz 2 StPO für die Erhebung von anlassunabhängig gespeicherten Verkehrsdaten nach § 113b TKG aufzunehmen.

Die vorgenannten Delikte fügen sich nahtlos in den Kreis der besonders schweren Katalogtaten des § 100g Absatz 2 StPO ein, da sie allesamt mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bedroht sind. Insoweit wird auf die Begründung zu § 100b Absatz 2 Nummer 1 Buchstabe f StPO-E Bezug genommen. Verfassungsrechtlich ist die Aufnahme dieser besonders schweren Computer- und Datendelikte in den Katalog des § 100g Absatz 2 StPO im Übrigen schon deshalb unproblematisch, weil das Bundesverfassungsgericht für den Abruf der Daten als Anlasstat

"nur" eine schwere und keine besonders schwere Straftat gefordert hat (BVerfG NJW 2010, 833 [841]). Indem der Entwurf also nur die Aufnahme von besonders schweren Computer- und Datendelikte in den Anlasstatenkatalog vorschlägt, geht er sogar über die Vorgaben des Bundesverfassungsgerichts hinaus.

Die Aufnahme der vorgeschlagenen besonders schweren Computer- und Datendelikte in den Katalog des § 100g Absatz 2 StPO ist mit Blick auf die gesetzgeberische Intention bei der Schaffung des Katalogs auch konsequent. Denn nach der Vorstellung des historischen Gesetzgebers sollten in Anknüpfung an die bundesverfassungsgerichtlichen Vorgaben von dem Katalog namentlich auch solche besonders schweren Straftaten erfasst werden, bei denen die gespeicherten Verkehrsdaten nach kriminalistischer Erfahrung besonders wertvolle Dienste leisten können und damit eine besondere Bedeutung haben (BT-Drs. 18/5088, S. 32; vgl. auch BVerfG NJW 2010, 833 [841]). Eben dies ist aber gerade bei den besonders schweren Straftaten im Bereich der Cyberkriminalität der Fall, da diese Taten in den allermeisten Fällen auch oder ausschließlich unter Zuhilfenahme von Telekommunikationsdiensten begangen werden. Die dabei anfallenden Verkehrsdaten stellen daher schon aufgrund der Art und Weise der Tatbegehung, die sich praktisch ausschließlich in oder über die digitale Welt vollzieht, häufig den einzig erfolgversprechenden Ermittlungsansatz dar. Spuren in der realen Welt gibt es meist nicht.

Von besonderer Bedeutung sind hier die nach § 113b Abs. 3 TKG gespeicherten Daten der Internetzugangsdienste, sowie die von den Telefondiensten gemäß § 113b Abs. 2 Nr. 5 TKG gespeicherten Internetprotokolladressen. Denn auch wenn viele gewerbs- und bandenmäßig agierende Täter durch technische Vorkehrungen versuchen, ihre wahren Adressen zu verschleiern, so benötigen sie dennoch für den ersten Zugang zum Internet eine originäre Internetprotokolladresse. Gelingt es den Ermittlungsbehörden, diese zu ermitteln, führt erst die Zuordnung der Adresse zu einem konkreten Teilnehmer zur Identifizierung der Täter.

Zu Buchstabe b (Buchstabe f bis i StPO-E)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 3 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.