Deutscher Bundestag **Drucksache 18/1288**

18. Wahlperiode 30.04.2014

Gesetzentwurf

des Bundesrates

Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei

A. Problem und Ziel

Mit den rasanten Fortschritten im Bereich der Informationstechnologie nimmt auch der Handel mit rechtswidrig erlangten digitalen Identitäten immer mehr zu. Zu den digitalen Identitäten gehören z. B. Kreditkartendaten oder Zugangsdaten zu Onlinebanking, E-Mail-Diensten oder sozialen Netzwerken. Mittels des Einsatzes von Schadsoftware werden von den Tätern über das Internet in großem Umfang Daten ausgespäht oder anderweitig rechtswidrig erhoben und auf Servern gespeichert. Dabei nehmen die Täter, die sich solche Daten verschaffen, häufig selbst keine unmittelbaren Vermögensverfügungen mit den ausgespähten oder entwendeten Daten vor. Vielmehr findet über Webportale und Foren ein intensiver Handel mit widerrechtlich erlangten Daten aller Art statt. Die Erkenntnisse der nationalen und internationalen Strafverfolgungsorgane deuten darauf hin, dass Fallzahlen und Schäden in diesem Zusammenhang deutlich steigen.

Die mit Bereicherungs- oder Schädigungsabsicht vorgenommene Weitergabe der rechtswidrig erlangten Daten selbst ist aber bisher nur in Teilbereichen von den bestehenden Strafnormen erfasst, so dass der Gefahr des massenhaften Missbrauchs dieser Daten nicht ausreichend wirksam begegnet werden kann. Der besondere strafrechtliche Schutzbedarf in diesem Bereich ist dabei insbesondere durch das vom Bundesverfassungsgericht formulierte „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ veranlasst (vgl. BVerfGE 120, 274 ff. – Urteil vom 27. Februar 2008).

Hinzu kommt, dass die Polizeiliche Kriminalstatistik (PKS) seit Jahren rapide ansteigende Fallzahlen im Bereich der Delikte gegen die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme und Daten zeigt. Angriffe in Form von Trojanern, Viren und Ähnlichem sind – ausweislich verschiedener Studien – inzwischen Massenphänomene, die zahlenmäßig weit über die Angaben der PKS hinausgehen.

Diese Angriffe werden in vielen Fällen von internationalen, arbeitsteilig strukturierten Gruppen verübt, die in speziellen – meist nicht öffentlich zugänglichen – Diskussionsforen und Chat-Diensten eine breite Palette von Diensten anbieten und damit hohe Gewinne erzielen. Die Angriffe erfolgen zwar regelmäßig aus finanziellen, in manchen Fällen aber auch aus politischen Gründen und hier dann zum Teil mit terroristischem Hintergrund.

B. Lösung

Der Gesetzentwurf trägt dem Anliegen der Schließung bestehender Strafbarkeitslücken in Fällen des Handelns mit rechtswidrig erlangten Daten durch die Einführung eines neuen Straftatbestands der Datenhehlerei (§ 202d StGB-E) Rechnung. Um den Anwendungsbereich der Norm zu begrenzen, werden nur solche Daten von der Norm erfasst, an deren Nichtweiterverwendung ein schutzwürdiges Interesse besteht und die nicht aus allgemein zugänglichen Quellen entnommen werden können. Nach § 202d Absatz 5 StGB-E werden Handlungen eines Amtsträgers oder seiner Beauftragten nicht vom Tatbestand der Datenhehlerei erfasst, wenn diese in Erfüllung gesetzlicher Pflichten handeln bzw. die Daten ausschließlich in einem Besteuerungs-, Straf- oder Ordnungswidrigkeitenverfahren verwertet werden.

Die Bekämpfung der organisierten Cyberkriminalität kann nur wirksam erfolgen, wenn zum einen eine angemessene Sanktionierung aufgrund einschlägiger Tatbestände möglich ist und zum anderen den Strafverfolgungsbehörden die zur wirkungsvollen Strafverfolgung notwendigen Mittel zur Verfügung gestellt werden.

Zweites Kernstück des Gesetzentwurfs sind daher eine Erhöhung der Strafrahmen des Ausspähens und Abfangens von Daten (§§ 202a, 202b StGB) – der einschlägigen Delikte bei Angriffen gegen die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme und Daten – im Falle des Handelns mit Bereicherungs- oder Schädigungsabsicht, die Schaffung entsprechender Qualifikationstatbestände für Fälle des gewerbs- oder bandenmäßigen Handelns sowie die Einführung einer Versuchsstrafbarkeit. Die Ausgestaltung der Tatbestände der §§ 202a, 202b und 202d StGB-E erfolgt insoweit im Wesentlichen gleichlaufend.

Um eine wirkungsvolle Strafverfolgung in Fällen des gewerbs- oder bandenmäßigen Handelns, d. h. im Fall des Vorliegens von organisierter Kriminalität, zu ermöglichen, sind zudem Änderungen des Rechts der Telekommunikationsüberwachung (§ 100a StPO), der Maßnahmen ohne Wissen des Betroffenen (§ 100c StPO) sowie des Rechts der Untersuchungshaft (§ 112a StPO) erforderlich. Die Kataloge des § 100a Absatz 2 Nummer 1 StPO, des § 100c Absatz 2 Nummer 1 StPO und des § 112a Absatz 1 Satz 1 Nummer 2 StPO werden für die Fälle der gewerbs- und bandenmäßigen Begehungsweise ergänzt und somit den Strafverfolgungsbehörden die notwendigen Ermittlungsmaßnahmen zur Verfügung gestellt. Da es sich bei der Datenhehlerei um ein Anschlussdelikt handelt, bedürfen auch die korrespondierenden Regelungen in der Strafprozessordnung (§§ 3, 60 Nummer 2, § 68b Absatz 1 Satz 4 Nummer 1, § 97 Absatz 2 Satz 3, §§ 102, 138a Absatz 1 Nummer 3, § 160a Absatz 4 Satz 1 StPO) der Anpassung.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht oder entfällt kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht oder entfällt kein Erfüllungsaufwand.

E.3 Erfüllungsaufwand der Verwaltung

Aufgrund der Ausdehnung des deutschen Strafrechts ist zu erwarten, dass die Anzahl der Strafverfahren in einem begrenzten Ausmaß zunimmt. Dies kann zu nicht näher quantifizierbaren Haushaltsmehrausgaben bei den für die Durchführung von Strafverfahren primär zuständigen Strafverfolgungsbehörden der Länder führen. Dies gilt vor allem angesichts der hohen Anforderungen an die technische Ausstattung und die notwendige Fachkunde der Ermittlungsbehörden in den zu erwartenden Ermittlungs- und Strafverfahren. Gleiches gilt für die entsprechenden Erweiterungen des Strafprozessrechts. Im Zuständigkeitsbereich des Bundes anfallende Haushaltsmehrausgaben sind allenfalls in geringem Umfang zu erwarten.

Der Mehraufwand bei den Strafverfolgungs- und Vollstreckungsbehörden ist jedoch angesichts der bestehenden Strafbarkeitslücken und des verbesserten Rechtsgüterschutzes gerechtfertigt.

F. Weitere Kosten

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

BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

Berlin, 30. April 2014

An den
Präsidenten des
Deutschen Bundestages
Herrn Prof. Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich gemäß Artikel 76 Absatz 3 des Grundgesetzes den vom Bundesrat in seiner 920. Sitzung am 14. März 2014 beschlossenen

Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium der Justiz und für Verbraucherschutz.

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

Mit freundlichen Grüßen

Dr. Angela Merkel

Anlage 1

Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei

Vom …

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), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 202c folgende Angabe eingefügt:

   „§ 202d Datenhehlerei“.

2. Dem § 202a werden die folgenden Absätze 3 bis 6 angefügt:

   „(3) Handelt der Täter in den Fällen des Absatzes 1 in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

   (4) Handelt der Täter in den Fällen des Absatzes 3 gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 202a, 202b, 202d, 263 bis 264, 267 bis 269, 303a oder 303b verbunden hat, so ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren.

   (5) Der Versuch ist strafbar.

   (6) In den Fällen des Absatzes 4 ist § 73d anzuwenden.“

3. § 202b wird wie folgt geändert:

   a) Der Wortlaut wird Absatz 1.

   b) Die folgenden Absätze 2 bis 5 werden angefügt:

      „(2) Handelt der Täter in den Fällen des Absatzes 1 in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

      (3) Handelt der Täter in den Fällen des Absatzes 2 gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 202a, 202b, 202d, 263 bis 264, 267 bis 269, 303a oder 303b verbunden hat, so ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren.

      (4) Der Versuch ist strafbar.

      (5) In den Fällen des Absatzes 3 ist § 73d anzuwenden.“

4. Nach § 202c wird folgender § 202d eingefügt:

„§ 202d

Datenhehlerei

(1) Wer Daten im Sinne von § 202a Absatz 2, die ein anderer ausgespäht oder sonst durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, an deren Nichtweiterverwendung der Berechtigte ein schutzwürdiges Interesse hat und die nicht aus allgemein zugänglichen Quellen entnommen werden können.

(3) Handelt der Täter gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 202a, 202b, 202d, 263 bis 264, 267 bis 269, 303a oder 303b verbunden hat, so ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren.

(4) Der Versuch ist strafbar.

(5) Die Absätze 1 bis 4 gelten nicht für Handlungen, die ausschließlich der Erfüllung gesetzlicher Pflichten durch Amtsträger oder deren Beauftragte dienen. Die Absätze 1 bis 4 gelten ebenfalls nicht für Handlungen von Amtsträgern oder deren Beauftragten, um Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zuzuführen.

(6) In den Fällen des Absatzes 3 ist § 73d anzuwenden.“

5. In § 205 Absatz 1 Satz 2 und Absatz 2 Satz 1 werden jeweils die Wörter „der §§ 202a und 202b“ durch die Wörter „des § 202a Absatz 1 und 3, § 202b Absatz 1 und 2 sowie § 202d Absatz 1“ ersetzt.

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. In § 100a Absatz 2 Nummer 1 wird nach Buchstabe g folgender Buchstabe g_1 eingefügt:

   „g_1) Verletzung des persönlichen Lebens- und Geheimbereichs nach § 202a Absatz 4, § 202b Absatz 3 und § 202d Absatz 3,“.

2. In § 100c Absatz 2 Nummer 1 wird nach Buchstabe e folgender Buchstabe e_1 eingefügt:

   „e_1) Verletzung des persönlichen Lebens- und Geheimbereichs nach § 202a Absatz 4, § 202b Absatz 3 und § 202d Absatz 3,“.

3. In § 112a Absatz 1 Satz 1 Nummer 2 werden nach der Angabe „125a,“ die Wörter „nach § 202a Absatz 4, § 202b Absatz 3 und § 202d Absatz 3,“ eingefügt.

4. In den §§ 3, 60 Nummer 2, § 68b Absatz 1 Satz 4 Nummer 1, § 97 Absatz 2 Satz 3, den §§ 102, 138a Absatz 1 Nummer 3 und § 160a Absatz 4 Satz 1 wird jeweils vor dem Wort „Begünstigung“ das Wort „Datenhehlerei“ und ein Komma eingefügt.

Artikel 3

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und wesentlicher Inhalt des Gesetzentwurfs

Die immer stärkere Verbreitung und Nutzung von Informations- und Kommunikationstechnologien, insbesondere die Nutzung des Internets, wirken sich unmittelbar auf alle Bereiche der Gesellschaft aus. Die Einbeziehung von Telekommunikations- und Informationssystemen, die eine entfernungsunabhängige Speicherung und Übertragung von Daten aller Art gestatten, bietet ein breites Spektrum neuer Möglichkeiten, aber auch des Missbrauchs.

Mit dem Einundvierzigsten Strafrechtsänderungsgesetz (41. StrÄndG) vom 7. August 2007 (BGBl. I S. 1786), mit welchem der deutsche Gesetzgeber dem aus dem Übereinkommen des Europarates über Computerkriminalität vom 23. November 2001 (Cybercrime Convention) sowie dem aus dem Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme (ABl. L 69, S. 67) resultierenden Umsetzungsbedarf nachgekommen ist, wurden zuletzt Regelungen getroffen, um den Missbrauch der Informationstechnologie zu bekämpfen.

Diese genügen jedoch noch nicht, da die Internetkriminalität nicht nur eine Vielzahl unterschiedlicher Deliktsformen umfasst, sondern auch an Intensität zugenommen hat. Den Schlüssel zu Angriffen gegen die Integrität von Computersystemen und -daten bildet der – auch als Hacking bezeichnete – unberechtigte Zugang zu Computersystemen, der durch das technische Eindringen in fremde Systeme sowie das Abfangen von Daten verwirklicht wird (vgl. auch nachfolgend: Gutachten C von Prof. Dr. Ulrich Sieber zum 69. Deutschen Juristentag „Straftaten und Strafverfolgung im Internet“, S. 18 ff.). Das Eindringen in fremde Systeme umfasst eine Vielzahl von Handlungen, mit denen die Sicherheitsmaßnahmen von Computersystemen auf technischem Wege umgangen werden, z. B. das „Knacken“ von Passwörtern. Von größerer Relevanz ist inzwischen das Ausnutzen von Sicherheitslücken auf Computersystemen durch sogenannte Exploits.

Während in den Anfangszeiten der Internetkriminalität noch einzelne – oftmals jugendliche – Hacker tätig waren, sind es heute eher internationale, arbeitsteilig strukturierte Gruppen, die in speziellen – meist nicht öffentlich zugänglichen – Diskussionsforen und Chat-Diensten eine breite Palette von Diensten anbieten und damit hohe Gewinne erzielen (vgl. Sieber, a. a. O., C 22 m. w. N.). Die Angriffe gegen die Integrität von Computersystemen und -daten erfolgen jedoch nicht nur aus finanziellen Gründen. In den letzten Jahren wurden einige aufsehenerregende Hackingangriffe im Rahmen des sogenannten Hacktivismus – zumindest vorgeblich – auch aus politischer Motivation begangen. Ebenso können terroristische Motive eine Rolle spielen, etwa durch gezieltes Hacking von sicherheitsrelevanten Infrastruktureinrichtungen wie Krankenhäusern oder Kraftwerken. Auch in kriegerischen Auseinandersetzungen ist der Einsatz solcher Cyberangriffe absehbar (vgl. Sieber, a. a. O., C 24 m. w. N.).

Die Polizeiliche Kriminalstatistik (PKS) verzeichnet – bei unterdurchschnittlicher Aufklärungsquote – seit Jahren rapide ansteigende Fallzahlen im Bereich der Delikte gegen die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme und Daten. Angriffe in Form von Trojanern, Viren und ähnlichem sind inzwischen Massenphänomene, die zahlenmäßig weit über die Angaben der PKS hinausgehen, weswegen es auch schwer ist, die in dieser Deliktsgruppe entstehenden Schäden abzuschätzen (vgl. Sieber, a. a. O., C 25 m. w. N.).

Die Bekämpfung der genannten Formen der organisierten Kriminalität kann nur wirksam erfolgen, wenn zum einen eine angemessene Sanktionierung aufgrund einschlägiger Tatbestände möglich ist und zum anderen den Strafverfolgungsbehörden die zur wirkungsvollen Strafverfolgung notwendigen Mittel zur Verfügung gestellt werden.

Da die Strafrahmen der einschlägigen Tatbestände der §§ 202a und 202b StGB nicht ausreichend sind, um den genannten Kriminalitätsformen gerecht zu werden, bedürfen sie der Anpassung und der Qualifizierung. Weiter bedarf es der Einführung einer Versuchsstrafbarkeit (so auch Sieber, a. a. O., C 86 ff.).

Darüber hinaus hat die strafrechtliche Praxis gezeigt, dass weiterhin spürbare Strafbarkeitslücken bestehen. Grund hierfür ist, dass das Strafgesetzbuch in seiner gegenwärtigen Form primär auf materielle Güter und nicht auf immaterielle Daten zugeschnitten ist. Für letztere besteht daher noch kein umfassender Schutz, auch wenn bereits einige „datenbezogene“ Straftatbestände in das Strafgesetzbuch eingefügt wurden. Nachdem das

Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung vom 27. Februar 2008 als besondere Ausprägung des allgemeinen Persönlichkeitsrechts (Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes) das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ formuliert hat, ist dem Regelungsanliegen jedoch grundrechtliche Relevanz beizumessen (BVerfGE 120, 274 ff.). Danach gewährleistet das allgemeine Persönlichkeitsrecht, dass in der Rechtsordnung gegebenenfalls die Bedingungen geschaffen und erhalten werden, unter denen der Einzelne selbstbestimmt an Kommunikationsprozessen teilnehmen und so seine Persönlichkeit entfalten kann (Kammerbeschluss vom 23. Oktober 2006, 1 BvR 2027/02, Rn. 33 – juris – zur Geltung des Rechts auf informationelle Selbstbestimmung im Privatrechtsverkehr).

Eine Strafbarkeitslücke besteht beim Handel mit rechtswidrig erlangten Daten.

Mit den rasanten Fortschritten im Bereich der Informationstechnologie hat auch der Handel mit rechtswidrig erlangten digitalen Identitäten immer mehr zugenommen. Zu den digitalen Identitäten gehören zum Beispiel Kreditkartendaten oder Zugangsdaten zu Onlinebanking, E-Mail-Diensten oder sozialen Netzwerken. Mittels des Einsatzes von Schadsoftware werden von den Tätern über das Internet in großem Umfang Daten ausgespäht oder anderweitig rechtswidrig erhoben und auf Servern gespeichert. Neben Keylogging- und Phishing-Angriffen erfolgen auch immer häufiger zielgerichtete Hacking-Angriffe auf Onlineportale, bei denen teilweise Millionen von Kundeninformationen erbeutet werden. Mittels dieser rechtswidrig erlangten Daten ist es den Tätern regelmäßig möglich, sich einen unberechtigten Zugang zu einem „Account“ zu verschaffen und anschließend im Rahmen „traditioneller“ Delikte weitere strafbare Handlungen zu begehen, zum Beispiel indem entweder das Opfer – etwa durch Kontoplünderung oder Erstellung einer Kreditkartendublette – unmittelbar in seinem Vermögen beeinträchtigt oder seine Identität zur Begehung weiterer krimineller Handlungen missbraucht wird. Dabei nehmen die Täter, die sich solche Daten verschaffen, häufig selbst keine unmittelbaren Vermögensverfügungen mit den ausgespähten oder entwendeten Daten vor. Vielmehr findet über Webportale und Foren vor dem „Einsatz“ dieser widerrechtlich erlangten Daten zunächst ein intensiver Handel statt.

Die Datensätze werden über spezielle nichtöffentliche Plattformen im Internet frei verkauft. Ihre Preise ergeben sich aus dem Umfang der Daten, deren Aktualität und den Bewertungen des Verkäufers, die dieser zuvor von anderen „Kunden“ erhalten hat. Besonders attraktive Datensätze werden zusammen mit weiteren persönlichen Daten des Kontoinhabers wie (Geburts-)Name, Geburtstag und – in den USA von besonderer Relevanz – Sozialversicherungsnummer angeboten, wodurch eine weitgehende Übernahme der digitalen Identität einer Person gelingen kann. Derart qualifizierte Datensätze werden etwa im Fall von Bankkonten zu Stückpreisen zwischen 5 bis 260 US-Dollar gehandelt. Um bei der anschließenden Plünderung der Konten durch den Aufkäufer der Daten die Zahlungswege zu verschleiern, werden „Finanzagenten“ zwischengeschaltet, die sich gegen eine Provision das Geld auf ihr Konto überweisen lassen und dieses im Wege des Bargeldtransfers an den Haupttäter weiterleiten. Diese Finanzagenten werden in der Regel durch Spam-Mails angeworben und sind sich in vielen Fällen ihrer Rolle als Geldwäscher nicht bewusst. Zur anonymen Bezahlung hat sich auf dem digitalen Schwarzmarkt mittlerweile eine Reihe spezieller Währungen etabliert. Dazu gehören neben Prepaid-Bezahlmethoden auch virtuelle Währungen, die Bezahlvorgänge dezentral über ein verschlüsseltes Peer-to-Peer-Netzwerk abwickeln (vgl. Sieber, a. a. O., C 23 m. w. N.).

Präzise Fallzahlen in diesem Kriminalitätsbereich liegen nicht vor, was unter anderem auch darauf zurückzuführen sein dürfte, dass Kreditkartenemittenten den durch den missbräuchlichen Einsatz von Kartendaten entstandenen finanziellen Schaden in vielen Fällen ersetzen und somit der Karteninhaber keinen Grund für eine Anzeigeerstattung sieht. Auch ist deshalb von einem großen Dunkelfeld auszugehen, da die Geschädigten in aller Regel nicht wissen, dass ihre Rechner infiziert und verschiedene Bestandteile ihrer digitalen Identität entwendet wurden. Nur dann, wenn es zu einem missbräuchlichen Einsatz der Daten kommt, erfolgt unter Umständen eine Mitteilung an die Strafverfolgungsbehörden.

Die Erkenntnisse der nationalen und internationalen Strafverfolgungsorgane deuten aber darauf hin, dass die Fallzahlen und die daraus resultierenden Schäden auch in diesem Bereich deutlich steigen.

Die bestehenden Strafnormen (z. B. in den §§ 202a ff., 263, 263a, 269 StGB, §§ 106 ff. UrhG, §§ 43, 44 BDSG, §§ 17 ff. UWG) erfassen die Weitergabe rechtswidrig erlangter Daten jedoch nur in Teilbereichen, da die Verkäufer und Käufer missbräuchlich erlangter Daten auf den weltweiten virtuellen Schwarzmärkten häufig weder die Täter sind, die die Daten zuvor ausgespäht haben, noch diejenigen, die sie später betrügerisch einsetzen. Zumindest ist diesen Datenhändlern entsprechendes oft nicht nachzuweisen.

Eine Beihilfe oder Anstiftung des Datenhändlers zur Vortat, beispielsweise zum Ausspähen von Daten (§ 202a StGB), liegt in aller Regel nicht vor, da die Vortat üblicherweise bereits beendet ist, wenn dem Datenhändler die Daten zum Kauf angeboten werden. Eine Beihilfe des Datenhändlers zum späteren widerrechtlichen Gebrauch ist noch nicht gegeben, solange die Daten in den Internetforen erst zum Verkauf angeboten werden und damit zu ihrem widerrechtlichen Gebrauch noch nicht unmittelbar angesetzt wird. Auch wenn die verkauften Daten später rechtswidrig verwendet werden, wird eine mögliche Anstiftung oder Beihilfe des Datenhändlers zu dieser Tat zumeist nicht verfolgbar sein, da nicht festgestellt werden kann, ob und von wem der Haupttäter die Daten angekauft hat.

Die Weitergabe der rechtswidrig erlangten Daten selbst wird aber nur in Teilbereichen von bestehenden Strafnormen erfasst. Der Tatbestand des Vorbereitens des Ausspähens oder Abfangens von Daten (§ 202c StGB) umfasst zwar in Absatz 1 Nummer 1 die Weitergabe von „Passwörtern“ oder „Sicherungscodes“. Strafbar ist das Sich-Verschaffen oder Weitergeben dieser Daten aber nur, wenn dies der Vorbereitung einer Tat nach § 202a StGB (Ausspähen von Daten) oder § 202b StGB (Abfangen von Daten) dient. Werden die Daten dagegen unmittelbar eingesetzt, wie z. B. Kreditkartendaten, so scheidet eine Strafbarkeit gemäß § 202c StGB aus. Auch die Fälle, in denen allein ein Computerbetrug (§ 263a StGB) vorbereitet wird, werden nicht erfasst.

Die strafrechtlichen Nebengesetze genügen ebenfalls nicht zur effektiven Verfolgung der Datenhehlerei. Die Strafvorschrift des § 44 Absatz 1 i. V. m. § 43 Absatz 2 Nummer 1 BDSG, die in Einzelfällen einschlägig sein könnte, bietet keine ausreichende Sanktionsmöglichkeit. Dieser Tatbestand erfasst unter anderem das vorsätzliche unbefugte Verarbeiten personenbezogener Daten gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht. Doch schon die Schutzrichtung des Bundesdatenschutzgesetzes, nämlich der Schutz personenbezogener Daten vor der unbefugten Preisgabe, bleibt deutlich hinter dem Ziel der Bekämpfung des illegalen Handels mit rechtswidrig erlangten Daten zurück. Dies zeigt sich auch an der vergleichsweise niedrigen Strafandrohung von bis zu zwei Jahren Freiheitsstrafe, während die Sachhehlerei nach § 259 StGB mit bis zu fünf Jahren Freiheitsstrafe bedroht ist, bei Gewerbsmäßigkeit sogar mit bis zu zehn Jahren. Zudem handelt es sich bei § 44 BDSG um ein reines Antragsdelikt ohne Möglichkeit der Verfolgung von Amts wegen. Die Daten juristischer Personen werden vom BDSG sogar überhaupt nicht geschützt.

Weder bei der rechtswidrigen Erlangung der sonstigen, nicht unmittelbar wahrnehmbaren Daten im Sinne des § 202a Absatz 2 StGB, noch beim späteren Handel mit diesen Daten handelt es sich jedoch um ein auf die Computernutzung beschränktes Phänomen. Da Daten auch auf anderen Wegen, zum Beispiel telefonisch oder brieflich, auf kriminelle Weise erlangt und dann auch weiter verkauft werden können, verlangt ein umfassender Schutz der Verfügungsbefugnis und des Geheimhaltungsinteresses des Verfügungsberechtigten über seine Daten, dass es nicht darauf ankommen darf, auf welchem rechtswidrigen Weg die Daten erlangt wurden. Auch der Weiterverkauf von Daten eines entwendeten Datenträgers muss über die gesamte Kette von Weiterveräußerungen von einer strafrechtlichen Norm erfasst werden.

Da es sich bei dem Handel mit rechtswidrig erlangten Daten grundsätzlich um ein ebenso strafwürdiges Verhalten handelt wie beim An- und Verkauf von gestohlenen körperlichen Gegenständen, zielt der Gesetzentwurf darauf ab, die beschriebene Strafbarkeitslücke zu schließen. Eine Gleichsetzung von Daten und körperlichen Sachen im Sinne des § 90 BGB hinsichtlich ihrer strafrechtlichen Behandlung ist zwar nicht möglich, jedoch ist eine Annäherung wegen der vergleichbaren Strafwürdigkeit verschiedener Fallkonstellationen erforderlich. Daten werfen wegen ihrer immateriellen Natur gegenüber körperlichen Gegenständen ganz eigene Fragestellungen auf, die nicht einfach dadurch gelöst werden können, dass die für körperliche Gegenstände entwickelten Normen auf Daten und Informationen angewandt werden (vgl. Sieber, a. a. O., C 14).

Maßstab für die Überschreitung der Grenze zur Strafbarkeit muss aufgrund der „Allgegenwärtigkeit“ von Daten die Betroffenheit von schutzwürdigen Daten sein. Der Tatbestand der Datenhehlerei bedarf daher einer Einschränkung in § 202d Absatz 2 StGB-E in Bezug auf sogenannte Alltagsdaten. Hierbei handelt es sich um Daten, deren Verwendung durch Dritte den Berechtigten „nicht weiter betrifft“ oder die sonst „frei zugänglich“ sind. § 202d Absatz 2 StGB-E eröffnet daher den Schutzbereich nur für solche Daten, an deren Nichtweiterverwendung der Berechtigte ein schutzwürdiges Interesse hat und die nicht aus allgemein zugänglichen Quellen entnommen werden können. Allgemein zugängliche Quellen sind beispielsweise Zeitungen, Rundfunk, Fernsehen oder auch der öffentliche Bereich des Internets. Unter § 202d Absatz 1 StGB-E subsumierbare Fallkonstellationen, die diese Art von Daten betreffen – mögen die Daten auch ursprünglich aus einer rechtswidrigen Tat herrühren -, sind nicht strafwürdig, so dass das Strafrecht als Ultima Ratio nicht zur Anwendung gebracht werden kann. Bei der Verwendung dieser „Alltagsdaten“ – auch wenn die Daten aus einer rechtswidrigen Tat stammen – dürfte dem Täter die Grenze fremder Zuständigkeit in vielen Fällen

nicht bewusst sein, da er davon ausgeht, dass er diese Daten auch auf andere Art und Weise hätte erlangen können und es sich möglicherweise sogar gerade um Daten handelt, bei denen eine Kenntnisnahme durch eine Vielzahl von Personen durch den Verfügungsberechtigten gewollt ist (zu denken wäre insoweit beispielsweise an Daten in Form einer Werbung für Sonderangebote). In solchen Fällen kann aus der Weiterverwendung entsprechender „Alltagsdaten" zum eigenen finanziellen Vorteil noch nicht auf ein ausreichendes Maß an krimineller Energie und ein vorhandenes Unrechtsbewusstsein beim Täter geschlossen werden, welches es rechtfertigen würde, ihn mit einer Strafsanktion zu belegen.

Um eine wirkungsvolle Strafverfolgung in Fällen des gewerbs- oder bandenmäßigen Handelns in den vorgenannten Fällen zu ermöglichen, sind Änderungen des Rechts der Telekommunikationsüberwachung (§ 100a StPO), der Maßnahmen ohne Wissen des Betroffenen (§ 100c StPO) sowie des Rechts der Untersuchungshaft (§ 112a StPO) erforderlich, da organisierte Kriminalität mit den für diese Fälle vorgesehenen Mitteln bekämpft werden sollte (vgl. Sieber, a. a. O., C 87).

Die Regelungen in der Strafprozessordnung über die Anschlussdelikte (§§ 3, 60 Nummer 2, § 68b Absatz 1 Satz 4 Nummer 1, § 97 Absatz 2 Satz 3, §§ 102, 138a Absatz 1 Nummer 3, § 160a Absatz 4 Satz 1 StPO) bedürfen ebenfalls der Anpassung, da die Datenhehlerei ein Anschlussdelikt ist.

II. Gesetzgebungskompetenz

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

III. Auswirkungen

Durch die Einführung eines neuen Straftatbestands und die Erweiterung bestehender Straftatbestände sowie strafprozessualer Eingriffsmöglichkeiten kann mehr Aufwand bei den Strafverfolgungsbehörden entstehen, dessen Umfang im gegenwärtigen Zeitpunkt nicht hinreichend genau abschätzbar ist. Im Übrigen wird das Vorhaben Bund, Länder, Gemeinden, die Wirtschaft und die Bürger nicht mit Mehrkosten belasten. Da sich der Gesetzentwurf auf Änderungen und Ergänzungen von Strafvorschriften und des Strafprozessrechts beschränkt, sind Auswirkungen auf das Preisniveau, insbesondere auf das Verbraucherpreisniveau, die Umwelt oder Auswirkungen von gleichstellungspolitischer Bedeutung nicht zu erwarten.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Strafgesetzbuchs)

Zu Nummer 1 (Inhaltsübersicht)

Es handelt sich um eine redaktionelle Folgeänderung im Hinblick auf die Einfügung des § 202d StGB-E (Artikel 1 Nummer 2).

Zu Nummer 2 und Nummer 3 (§ 202a Absatz 3 bis 6 StGB-E und § 202b Absatz 2 bis 5 StGB-E)

Der Schutz der Integrität von Computersystemen und -daten vor unberechtigtem Zugang in der Form des technischen Eindringens in fremde Systeme sowie des Abfangens von Daten erfolgt durch die Tatbestände der §§ 202a und 202b StGB, deren Strafrahmen jedoch nur Geldstrafen bzw. Freiheitsstrafen bis zu drei Jahren im Fall des § 202a StGB und bis zu zwei Jahren im Fall des § 202b StGB vorsehen. Bereits bei der Änderung des § 202a StGB und der Neuregelung des § 202b StGB im Rahmen des 41. Strafrechtsänderungsgesetzes vom 7. August 2007 war sich der Gesetzgeber der generellen Gefährlichkeit von Hacking-Angriffen (z. B. durch den Einsatz von Key-Logging-Trojanern, Sniffern oder Backdoorprogrammen) bewusst (vgl. Bundestagsdrucksache 16/3656, S. 9), weswegen er trotz Herabsetzung der Schwelle zur Tatbestandsverwirklichung den ursprünglichen Strafrahmen in § 202a StGB beibehielt. Nunmehr hat sich jedoch im Rahmen verschiedener Studien (vgl. Sieber, a. a. O., C 25 und C 27 m. w. N.) gezeigt, dass diese Strafrahmen zur Bekämpfung dieser Form der Kriminalität nicht mehr ausreichen.

Professionelle Straftäter werden in einer Vielzahl von Fällen ihre Hacking-Angriffe mit der Zielsetzung der eigenen Bereicherung bzw. mit dem Willen zu einer gezielten Schädigung anderer begehen. Diese unlauteren Absichten rechtfertigen es, mag auch die Schwelle zur Verwirklichung des Tatbestandes nicht allzu hoch angesetzt sein, den Strafrahmen deutlich nach oben anzupassen und statt einer Freiheitsstrafe von bis zu drei

bzw. bis zu zwei Jahren eine Obergrenze von bis zu fünf Jahren Freiheitsstrafe vorzusehen (§ 202a Absatz 3 StGB-E und § 202b Absatz 2 StGB-E). Das Tatbestandsmerkmal der Schädigungsabsicht ist erforderlich, um kriminelle Tätergruppierungen mit politischen Zielen zu erfassen.

Handeln die Täter gewerbsmäßig oder als Mitglied einer Bande, so erfordert diese Form der organisierten Kriminalität die Schaffung eigener Qualifikationstatbestände (§ 202a Absatz 4 und § 202b Absatz 3 StGB-E). Der Katalog der Bandentatbestände entspricht dem § 263 Absatz 5 und § 267 Absatz 4 StGB, ergänzt um die relevanten Tatbestände zur Bekämpfung der IT-Kriminalität. Durch den weiter erhöhten Strafrahmen wird der besonderen Gefährlichkeit sowie dem erhöhten Unrechts- und Schuldgehalt der gewerbs- und bandenmäßigen Begehungsweise Rechnung getragen. Das Vorbereitungsdelikt des § 202c StGB wurde, da das betroffene Rechtsgut nur abstrakt gefährdet wird, nicht in den Katalog mit aufgenommen. Der Unrechtsgehalt einer gewerbs- und bandenmäßigen Begehungsweise (des § 202c StGB) im Falle der eigenständigen Ausführung der Haupttat wird in der Regel über die §§ 202a, 202b StGB zu erfassen sein. Im Falle der gewerbs- und bandenmäßigen Vorbereitung fremder Taten wird der besondere Unrechtsgehalt über die Strafbarkeit der Teilnahme an der Haupttat nach den §§ 202a, 202b StGB erfasst werden können. Ein Bedürfnis für die Aufnahme des § 202c StGB in den Straftatenkatalog von § 202a Absatz 4 und § 202b Absatz 3 StGB-E besteht daher nicht.

Auch die Einführung einer Versuchsstrafbarkeit in diesen Fällen, die der Gesetzgeber des 41. Strafrechtsänderungsgesetzes noch explizit ausgeschlossen hatte (vgl. Bundestagsdrucksache 16/3656, S. 10 f.), ist zur Erfassung des vollständigen Unrechtsgehalts der Taten gerechtfertigt. Die Regelung des § 202c StGB ist insofern nicht ausreichend, da hierdurch nur abstrakte Gefährdungen erfasst werden, im Fall des Versuchs einer Tat nach § 202a StGB oder § 202b StGB jedoch bereits eine konkrete Rechtsgutgefährdung vorliegt. Ein systematischer Bruch liegt in der Normierung einer Versuchsstrafbarkeit daher nicht (vgl. Sieber, a. a. O., C 86).

Hinzu kommt, dass bereits Artikel 5 Absatz 2 des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme (ABl. L 69 vom 16.3.2005, S. 67) die Einführung einer Versuchsstrafbarkeit vorsah. Den Mitgliedstaaten war es jedoch freigestellt, diesbezüglich einen Vorbehalt geltend zu machen, wovon Deutschland Gebrauch gemacht hat. Einen solchen Vorbehalt sieht der nunmehr vorliegende Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates in Artikel 8 Absatz 2 nicht mehr vor. Es ist auch nicht zu erwarten, dass ein solcher Vorbehalt im Rahmen der Verhandlungen noch in den Richtlinienvorschlag aufgenommen wird. Die Anpassung im Vorgriff auf die kommende Richtlinie würde daher späteren Anpassungsbedarf vermeiden.

Um eine effektive Gewinnabschöpfung zu ermöglichen, sollten den Strafverfolgungsbehörden auch die hierfür notwendigen Mittel zur Verfügung gestellt werden. Fälle des gewerbs- oder bandenmäßigen Ausspähens oder Abfangens von Daten gemäß § 202a Absatz 4 bzw. § 202b Absatz 3 StGB-E stellen eine Form der organisierten Kriminalität dar. Um dieser organisierten Kriminalität die finanzielle Basis zu entziehen, sollte § 73d StGB, der erweiterte Verfall, anwendbar sein. § 73d StGB ermöglicht in Fällen, in denen die bei dem Täter vorgefundenen Vermögensgegenstände, deren rechtmäßiger Erwerb nicht festgestellt werden kann und bei denen sich die Herkunft aus rechtswidrigen Taten mit Blick auf die Situation des Täters und sein Vorleben einem objektiven Betrachter geradezu aufdrängt, eine Gewinnabschöpfung. Diese Vorgabe wird vom Bundesgerichtshof (Beschluss vom 22. November 1994 – 4 StR 516/94 -, NJW 1995, 470, bestätigt durch das BVerfG, Beschluss vom 14. Januar 2004 – 2 BvR 564/95 -, NJW 2004, 2073) in verfassungskonformer Weise dahingehend ausgelegt, dass die Anordnung des erweiterten Verfalls voraussetzt, dass „der Tatrichter auf Grund erschöpfender Beweiserhebung und -würdigung … die uneingeschränkte Überzeugung gewonnen hat, dass der Angeklagte die von der Anordnung erfassten Gegenstände aus rechtswidrigen Taten erlangt hat, ohne dass diese selbst im Einzelnen festgestellt werden müssten."

Zu Nummer 4 (§ 202d StGB-E)

Die vorgeschlagene Regelung soll als neuer § 202d StGB-E in den fünfzehnten Abschnitt des Besonderen Teils des Strafgesetzbuchs eingefügt werden. Für eine systematische Verortung an dieser Stelle spricht – ausgehend vom Schutzgut des § 202d StGB-E – die primäre Betroffenheit des persönlichen Lebens- und Geheimbereichs im Falle der Tatbestandsverwirklichung sowie die enge Orientierung am Datenbegriff des § 202a Absatz 2 StGB, der genauso in den §§ 202b und 202c StGB Verwendung findet.

Das von § 202d StGB-E geschützte Rechtsgut ist die auf das verfassungsrechtlich verankerte Recht auf informationelle Selbstbestimmung zurückgehende formelle Verfügungsbefugnis bzw. das formelle Datenge-

heimnis desjenigen, der aufgrund seines Rechts an dem gedanklichen Inhalt der Daten über deren Weitergabe oder Übermittlung entscheidet. Zwar ist zu dem Zeitpunkt, zu welchem der Tatbestand des § 202d StGB-E ansetzt, die formelle Verfügungsbefugnis des Einzelnen über seine Daten bereits verletzt, die Rechtsgutverletzung also bereits eingetreten, jedoch wird die Rechtsgutverletzung von dem Datenhändler, der diese Situation zumindest billigend in Kauf nimmt, perpetuiert und zum eigenen finanziellen Vorteil oder mit dem Ziel, dem Berechtigten Schaden zuzufügen, ausgenutzt. Dies gilt auch wenn die Daten – wie meist – nur kopiert werden und der Berechtigte weiterhin darüber verfügen kann. Aus dieser weiteren Vertiefung der Rechtsgutverletzung zum eigenen finanziellen Vorteil oder zum Schaden des Berechtigten rechtfertigt sich die Strafwürdigkeit des Datenhehlers. Aus dieser fortwirkenden Betroffenheit schutzwürdiger Daten des formell Verfügungsberechtigten folgt nicht nur die Rechtfertigung der Strafdrohung, sondern auch die Anbindung an das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Da das Datengeheimnis des formell Verfügungsbefugten jedoch nur in schützenswerter Weise betroffen sein kann, wenn dieser ein schutzwürdiges Interesse an der Nichtweiterverwendung der Daten hat und die Daten nicht allgemein zugänglich sind, sind diese Art von Daten vom Schutzbereich des § 202d StGB-E ausgenommen.

Durch die weite Fassung der möglichen Vortaten wird ein umfassender Schutz der formellen Verfügungsbefugnis des Einzelnen über seine Daten sowie des allgemeinen Rechts auf Nichtöffentlichkeit der Kommunikation gewährleistet. Da mit dem Verfügungsrecht über Daten häufig wirtschaftliche Interessen verbunden sind und aus dem vorhandenen kriminellen Absatzmarkt für rechtswidrig erlangte Daten oftmals der eigentliche Tatanreiz für den Vortäter resultieren wird, wird als Schutzreflex auch das Vermögen des Dateninhabers geschützt. Primäres Schutzgut ist das Vermögen jedoch nicht, da nicht jeder Art von Daten ein Vermögenswert innewohnt, die Vortaten keine Vermögensstraftaten sein müssen und die nicht befugte Verwendung bestimmter Daten nicht zwingend mit einer Vermögenseinbuße einhergeht. Dies verdeutlicht auch das subjektive Tatbestandsmerkmal der Schädigungsabsicht.

Zu § 202d Absatz 1 StGB-E

Tatobjekt sind – in Übereinstimmung mit den §§ 202a ff. StGB – die nicht unmittelbar wahrnehmbaren Daten gemäß § 202a Absatz 2 StGB. Auf die einschlägigen Kommentierungen und die hierzu ergangene Rechtsprechung kann insoweit Bezug genommen werden. Einer Ausdehnung des Datenbegriffs bedarf es nicht, da der Schutz der unmittelbar wahrnehmbaren Daten ausreichend gewährleistet ist (vgl. Graf in Münchener Kommentar, StGB, 2. Auflage, § 202a, Rn. 12 m. w. N.). Auch wenn die Formulierung von Daten in der Mehrzahl spricht, wird auch ein einzelnes Datum geschützt.

Als Vortaten, an welche die Datenhehlerei anknüpft, kommen insbesondere das Ausspähen oder Abfangen von Daten gemäß den §§ 202a, 202b StGB in Betracht. Um jedoch einen umfassenden Schutz der formellen Verfügungsbefugnis des Einzelnen über seine Daten zu gewährleisten, müssen auch weitere Straftaten, wie Diebstahl, Betrug oder Nötigung, als taugliche Vortaten normiert werden. Als taugliche Vortaten werden daher alle rechtswidrigen Taten erfasst, die der Erlangung von Daten dienen. Allein vertragswidrige oder ordnungswidrige Handlungen sind gemäß § 11 Absatz 1 Nummer 5 StGB vom Tatbestand ausgenommen. Die explizite Normierung der Daten als „fremde“ ist entbehrlich, da es sich hierbei um eine Selbstverständlichkeit handelt.

Wie sich aus der Überschrift des Tatbestandes des § 202d StGB-E ergibt, ist der Tatbestand der Datenhehlerei in seiner Gestaltung dem Tatbestand der Hehlerei gemäß § 259 StGB entlehnt. Auch bei § 202d StGB-E handelt es sich um eine Anschlusstat, deren Vortat abgeschlossen, d. h. zumindest vollendet sein muss, was sich aus dem Tatbestandsmerkmal „erlangt hat“ ergibt.

Die Tatbestandshandlungen des § 202d Absatz 1 StGB-E sind dem § 202c Absatz 1 StGB entnommen und bedürften keiner Erweiterung. Sie sind durch die Rechtsprechung und Literatur hinreichend konkretisiert. Allein das Tatbestandsmerkmal des Verkaufens wurde nicht in den Tatbestand des § 202d Absatz 1 StGB-E übernommen. In der strafrechtlichen Literatur ist insoweit umstritten, ob es in diesen Fällen auf die Erlangung der Verfügungsmacht über die Daten ankommt und damit das Verkaufen einen Unterfall des Verschaffens darstellt (vgl. Hilgendorf in Leipziger Kommentar, StGB, 12. Auflage, § 202c, Rn. 24), oder ob es ausreicht, dass es nur zu einem Vertragsabschluss gekommen ist (vgl. Fischer, StGB, 60. Aufl., § 202c, Rn. 7). Obergerichtliche Rechtsprechung liegt hierzu nicht vor. Aus der in der Cybercrime-Convention verwendeten englischen Bezeichnung „sale“ ergibt sich hierzu nichts Eindeutiges (vgl. Graf, a. a. O., § 202c, Rn. 20). Sollte das Tatbestandsmerkmal einen Unterfall der Verschaffensalternative darstellen, wäre es entbehrlich.

Im Fall des bloßen Weiterverkaufs, ohne Erlangung der Verfügungsmacht über die Daten, ist das Rechtsgut der formellen Verfügungsbefugnis nicht ausreichend strafwürdig beeinträchtigt. Bei Abschluss des Kaufvertrags wäre das zu diesem Zeitpunkt bereits verletzte Rechtsgut der formellen Verfügungsbefugnis nicht in der Art weitergehend beeinträchtigt, dass dies eine strafrechtliche Sanktionierung erfordern würde. Vor diesem Hintergrund ist diese Handlungsalternative in jedem Fall entbehrlich.

In subjektiver Hinsicht genügt im Hinblick auf das Tatobjekt und die rechtswidrige Vortat Eventualvorsatz. Welche rechtswidrige Vortat dies im konkreten Fall war, muss der Täter nicht wissen. Er muss weder wissen, mittels welcher strafbaren Handlung die Daten erlangt wurden, noch müssen ihm die näheren Umstände der Vortat wie Ort und Zeit der Tatbegehung, die Person des Vortäters, die Art seiner Beteiligung an der Vortat oder die Person des durch die Vortat Verletzten bekannt sein. Es genügt, dass sich sein bedingter Vorsatz darauf bezieht, dass die Sache aus irgendeiner rechtswidrigen Tat herrührt (vgl. Maier in Münchener Kommentar, 2. Aufl., § 259, Rn. 128 m. w. N.).

Zur Rechtfertigung der Strafandrohung bedarf es daneben – wie im Rahmen des § 259 StGB – jedoch noch eines weiteren subjektiven Elements. Hierzu dienen die alternativen Tatbestandsmerkmale der Bereicherungsabsicht und der Schädigungsabsicht, die der Regelung in § 44 Absatz 1 BDSG entsprechen. Das Tatbestandsmerkmal der Schädigungsabsicht ist erforderlich, um kriminelle Tätergruppierungen mit politischen Zielen, die regelmäßig keine Bereicherungsabsicht haben dürften, ebenfalls zu erfassen.

Aufgrund der Vielzahl der denkbaren Vortaten und der insoweit in Betracht kommenden Strafrahmen dieser Vortaten entspricht der Strafrahmen der Datenhehlerei – um eine angemessene Bestrafung je nach Vortat zu ermöglichen – dem der weiteren Anschlusstaten (§ 257 Absatz 1, § 258 Absatz 1, § 259 Absatz 1 StGB). Eine Anpassung des Strafrahmens an die Grundtatbestände des § 202a Absatz 1 StGB und § 202b Absatz 1 StGB-E ist nicht erforderlich. Da als Vortaten sämtliche rechtswidrigen Taten in Betracht kommen und damit das von der Vortat betroffene Rechtsgut vom betroffenen Rechtsgut der Datenhehlerei unabhängig ist, bedarf es keines mit § 202a Absatz 1 StGB oder § 202b Absatz 1 StGB-E übereinstimmenden Strafrahmens oder einer Strafrahmenlimitierung entsprechend § 257 Absatz 2, § 258 Absatz 3 StGB (vgl. insoweit auch die Kritik zu § 258 Absatz 3 StGB bei Fischer, a. a. O., § 258, Rn. 38 m. w. N.). Im Übrigen kann die Schwere der Vortat bei der konkreten Strafzumessung gemäß § 46 StGB noch ausreichend Berücksichtigung finden.

Überschneidungen im Anwendungsbereich mit anderen Strafvorschriften sind über die allgemeinen Konkurrenzregeln zu lösen.

Zu § 202d Absatz 2 StGB-E

Da Daten wegen ihrer immateriellen Natur gegenüber körperlichen Gegenständen eigene Fragestellungen aufwerfen, die nicht einfach dadurch gelöst werden können, dass die für körperliche Gegenstände entwickelten Normen auf Daten und Informationen angewandt werden (vgl. Sieber, a. a. O., C 14), bedarf der Datenbegriff des § 202a Absatz 2 StGB für die Fälle der Datenhehlerei einer weiteren Einschränkung, um die allein strafwürdigen Fälle zu erfassen. Dies erfordert eine Herausnahme sogenannter Alltagsdaten aus dem Anwendungsbereich der Norm.

Eine Strafwürdigkeit im Falle der Tatbestandsverwirklichung entsprechend § 202d Absatz 1 StGB-E ist anzunehmen, wenn der Berechtigte ein schutzwürdiges Interesse an der Nichtverwendung der Daten hat. Dies muss der Maßstab für die Überschreitung der Grenze zur Strafbarkeit sein.

Die Begrifflichkeit des schutzwürdigen Interesses entstammt dem BDSG. Der Bundesgerichtshof hat zum Begriff des schutzwürdigen Interesses unter anderem im Urteil vom 23. Juni 2009 (NJW 2009, 2888 zu § 29 BDSG) Folgendes ausgeführt:

'Der wertausfüllungsbedürftige Begriff des „schutzwürdigen Interesses“ verlangt eine Abwägung des Interesses des Betroffenen an dem Schutz seiner Daten und des Stellenwerts, den die Offenlegung und Verwendung der Daten für ihn hat, mit den Interessen der Nutzer, für deren Zwecke die Speicherung erfolgt, unter Berücksichtigung der objektiven Wertordnung der Grundrechte. Dabei sind Art, Inhalt und Aussagekraft der beanstandeten Daten an den Aufgaben und Zwecken zu messen, denen die Datenerhebung und -speicherung dient.'

Der Begriff der schutzwürdigen Interessen ist sehr weit. Grundsätzlich fallen hierunter alle von der Rechtsordnung anerkannten Interessen. Als Interessen kommen alle menschlichen Ziele in Betracht, das Streben nach Geld, Anerkennung, nach Privatheit wie nach Kommunikation. Hier ist jeder Mensch verschieden, die Interessen der jeweils Betroffenen können unterschiedlich und auch entgegengesetzt sein (vgl. von Lewinski in Beck'scher Online-Kommentar, BDSG, § 10, Rn. 13 ff.).

Unter Berücksichtigung des Grundrechts der Informationsfreiheit (Artikel 5 Absatz 1 Satz 1 des Grundgesetzes) ist die Schutzwürdigkeit im Rahmen einer Interessenabwägung (objektiv) zu ermitteln. Eine solche Interessenabwägung ist dem Täter nur möglich, wenn er die Schutzwürdigkeit aufgrund konkreter Angaben des Verfügungsberechtigten beurteilten kann, was oftmals nicht der Fall sein dürfte, oder für die Schutzwürdigkeit der Daten objektive Anhaltspunkte, in der Regel aufgrund der Art der Daten, bestehen, d. h. die Schutzwürdigkeit für ihn erkennbar ist. Die Erkennbarkeit sowie das subjektive Erkennen des Täters in Form des dolus eventualis werden regelmäßig im Rahmen einer tatrichterlichen Würdigung zu ermitteln sein.

Im Falle objektiver Anhaltspunkte für eine Schutzwürdigkeit der Daten wird eine „sichere Exkulpation“ regelmäßig nur bei entsprechender Einwilligung des Verfügungsberechtigten möglich sein, sofern der Täter ein schutzwürdiges Interesse des Verfügungsberechtigten an der Nichtweiterverwendung der Daten im Rahmen eines Eventualvorsatzes zumindest für möglich hält. Eine Überspannung der an den Täter gestellten Anforderungen liegt hierin jedoch nicht, da es sich nach § 202d Absatz 1 StGB um Daten handelt, die aus einer rechtswidrigen Tat stammen und der Täter dies zudem im Rahmen eines Eventualvorsatzes zusätzlich für möglich halten muss.

Ein mit den Mitteln des Strafrechts zu schützendes Interesse an der Nichtweiterverwendung der Daten ist aber ebenfalls nicht gegeben, wenn die Daten aus allgemein zugänglichen Quellen wie Zeitungen, Rundfunk oder Fernsehen entnommen werden können. Die Begrifflichkeit der allgemeinen Zugänglichkeit ist ebenfalls dem BDSG (z. B. § 28 Absatz 1 Satz 1 Nummer 3, § 29 Absatz 1 Satz 1 Nummer 2 BDSG) bzw. dem Grundrecht der Informationsfreiheit gemäß Artikel 5 Absatz 1 Satz 1 des Grundgesetzes entnommen.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine Informationsquelle allgemein zugänglich, wenn die Informationsquelle technisch geeignet und bestimmt ist, der Allgemeinheit, d. h. einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen (vgl. BVerfG, Beschluss vom 3. Oktober 1969 – 1 BvR 46/65 -, NJW 1970, 235). Hieraus ergibt sich, dass es demjenigen, der sich aus allgemein zugänglichen Quellen unterrichten darf, grundsätzlich auch gestattet sein muss, die dort zugänglichen Daten zu verwenden (vgl. Gola in Gola/Schomerus, BDSG, 11. Aufl., § 28, Rn. 32).

Zu den allgemein zugänglichen Quellen zählen insbesondere sämtliche veröffentlichten Printmedien, öffentliche Datenbanken, öffentliche Anschläge, der Rundfunk, öffentliche Veranstaltungen und auch das Internet, sofern es öffentlich zugänglich ist. Die Pflicht, ein Entgelt vor dem Zugriff auf die Information zu zahlen, nimmt einer Quelle nicht ihre allgemeine Zugänglichkeit. Die Daten müssen allgemein zugänglich, d. h. in diesen Quellen verfügbar sein. Nicht erforderlich ist, dass die verwendende Stelle sie unmittelbar aus einer öffentlichen Quelle entnommen hat. Die Möglichkeit genügt (vgl. Wolff in Beck'scher Online-Kommentar, BDSG, § 28, Rn. 81 ff.).

Ein wichtiger Anwendungsfall dieser Tatbestandseinschränkung sind die sogenannten Filesharing-Fälle, da diese Daten – regelmäßig Film- oder Musikdateien – dazu bestimmt und geeignet sind, der Allgemeinheit, d. h. einem nicht mehr bestimmbaren Personenkreis, Informationen – gegen Entgelt – zu verschaffen. Ein ausreichender strafrechtlicher Schutz dieser Fälle ist durch das Urheberrechtsgesetz gewährleistet.

Der Begriff der Verwendung ist § 3 Absatz 5 BDSG entnommen. Verwenden ist der Oberbegriff zu dem in § 3 Absatz 4 BDSG definierten Begriff der Verarbeitung und dem in § 3 Absatz 5 BDSG definierten Begriff des Nutzens. Hierdurch soll jede Art des „Umgangs“ mit Daten mit Ausnahme ihrer Erhebung beim Betroffenen im Sinne des § 3 Absatz 3 BDSG erfasst werden.

Da sämtliche Tatbestandsmerkmale des § 202d Absatz 2 StGB-E dem BDSG entnommen sind, kann zu ihrer Auslegung auf die einschlägigen Kommentierungen und die hierzu ergangene Rechtsprechung zurückgegriffen werden. Hiermit wird dem Bestimmtheitsgebot des Artikels 103 Absatz 2 des Grundgesetzes ausreichend Rechnung getragen.

In subjektiver Hinsicht muss sich der nach § 202d Absatz 1 StGB-E zumindest erforderliche bedingte Vorsatz des Täters auch auf das schutzwürdige Interesse des Berechtigen an der Nichtweiterverwendung der Daten und auf die Tatsache, dass die Daten nicht aus allgemein zugänglichen Quellen entnommen werden können, beziehen.

Zu § 202d Absatz 3, 4 und 6 StGB-E

Auch die gewerbs- und bandenmäßige Datenhehlerei ist eine Form der organisierten Kriminalität. Zur weiteren Begründung kann auf die Ausführungen unter Nummer 2 und Nummer 3 (§ 202a Absatz 3 bis 6 StGB-E und § 202b Absatz 2 bis 5 StGB-E) Bezug genommen werden.

Zu § 202d Absatz 5 StGB-E

Um eine ungewollte Kriminalisierung von Amtsträgern zu vermeiden, die sich allein dienstbezogen bemakelte Daten verschaffen, sieht § 202d Absatz 5 StGB-E eine Tatbestandsausschlussregelung für die Fälle vor, in denen ausschließlich in Erfüllung gesetzlicher Pflichten gehandelt wird. Die Tatbestandsausschlussregelung lehnt sich hierbei an § 184b Absatz 5 StGB (Besitz kinderpornografischer Schriften) an.

Ungeachtet der Frage, ob in solchen Fällen alle Tatbestandsmerkmale, v. a. in subjektiver Hinsicht erfüllt wären, soll dieser Tatbestandsausschluss die Straflosigkeit des Handelns in ausschließlich dienstlicher Pflichterfüllung verdeutlichen. Gedacht ist hierbei vor allem an die Fälle des Erwerbs von sogenannten Steuer-CDs. Hierzu enthält § 202d Absatz 5 Satz 2 StGB-E eine ausdrückliche Klarstellung des gesetzgeberischen Willens, dass Amtsträger beim Ankauf von Datenmaterial zur ausschließlichen Verwendung in einem Besteuerungsverfahren nicht mit Strafe bedroht werden dürfen.

Um der im Hinblick auf § 184b Absatz 5 StGB geäußerten Kritik (vgl. Fischer, a. a. O., § 184b, Rn. 26, welcher insoweit von einer tautologischen Zirkelregelung spricht) zu begegnen und zur präziseren Definition der dienstlichen Pflichten, verwendet der Gesetzentwurf den Begriff der gesetzlichen Pflichten.

Gesetzliche Pflichten sind beispielsweise das aus § 152 Absatz 2 und § 163 Absatz 1 StPO für Staatsanwaltschaft und Polizei folgende Legalitätsprinzip, d. h. die Verpflichtung zur Einleitung eines Ermittlungsverfahrens im Falle des Anfangsverdachts einer Straftat, was auch die sogenannten Vorermittlungen umfasst (vgl. Meyer-Goßner, StPO, 54. Aufl., § 152, Rn. 4a), die polizeirechtlichen Gefahrenabwehrvorschriften oder die Pflicht der Steuerfahndung zur Aufdeckung und Ermittlung unbekannter Steuerfälle gemäß § 208 Absatz 1 Nummer 3 AO. Durch den Zusatz in § 202d Absatz 5 Satz 2 StGB-E soll sichergestellt werden, dass unabhängig von der Diskussion über die Zulässigkeit des Datenankaufs unter verwaltungsrechtlichen Gesichtspunkten solche Handlungen von Amtsträgern bzw. ihrer Beauftragten jedenfalls im Strafrecht nicht relevant sind. Die im Schrifttum geäußerten Zweifel, ob in der Abgabenordnung bzw. der Strafprozessordnung eine Rechtsnorm existiert, die den Datenankauf ermöglicht oder ggf. sogar zum Ankauf von Daten verpflichtet, sind damit für das Strafrecht nicht relevant.

Der Begriff des Amtsträgers ist in § 11 Nummer 2 StGB legaldefiniert. Der Begriff des Beauftragten geht über den Begriff des Amtsträgers im Sinne des § 11 Nummer 2 Buchstabe c StGB hinaus und soll auch behördenexterne Personen erfassen, die allein aufgrund eines privatrechtlichen Auftrags im konkreten Einzelfall von einem Amtsträger beauftragt wurden (vgl. BGH, Urteil vom 15. Mai 1997 – 1 StR 233/96 -, NJW 1997, 3034 zu § 11 Nummer 2 Buchstabe c StGB).

Mit dem Ausschließlichkeitserfordernis soll sichergestellt werden, dass die gesetzliche Aufgabe der einzige Grund für die Tathandlung im Sinne des § 202d Absatz 1 StGB-E ist, da nur in diesem Fall ein strafwürdiges Verhalten nicht gegeben ist.

Eine weitere Ausdehnung auf Fälle des beruflichen Handelns, wie dies § 184b Absatz 5 StGB vorsieht, wäre nicht zielführend. Ein solcher Tatbestandsausschluss würde die Strafnorm in weiten Teilen leer laufen lassen, da die berufliche Beschäftigung mit Daten – anders als die Beschäftigung mit kinderpornografischen Schriften – einen unübersehbar großen Personenkreis betreffen würde. Eine Übertragung des Tatbestandsausschlusses des § 184b Absatz 5 StGB auf § 202d Absatz 5 StGB-E ist daher abzulehnen. Die freie Presse ist, ungeachtet der Frage, ob auch in diesen Fällen sämtliche Tatbestandsmerkmale erfüllt wären – was hinsichtlich der subjektiven Anforderungen oftmals nicht der Fall sein wird -, ausreichend durch die Regelungen zum Informantenschutz geschützt (z. B. § 53 Absatz 1 Satz 1 Nummer 5 StPO, § 97 Absatz 5 StPO, § 98 Absatz 1 Satz 2 StPO).

Zu Nummer 5 (§ 205 Absatz 1 Satz 2 und Absatz 2 Satz 1 StGB-E)

Für den Grundtatbestand des Ausspähens und des Abfangens von Daten (§ 202a Absatz 1 und § 202b Absatz 1 StGB-E) sieht § 205 StGB schon bisher ein Antragserfordernis vor, welches durch die Bejahung eines besonderen öffentlichen Interesses an der Strafverfolgung durch die Strafverfolgungsbehörden ersetzt werden kann. Die Einschränkung des Antragserfordernisses wird vor allem in den Fällen für eine effektive Verfolgung für erforderlich gehalten, bei denen Daten von Dritten betroffen sind. Solche Dritte sind nicht Verletzte und damit nicht Antragsberechtigte, da nach herrschender Meinung in den Fällen der §§ 202a und 202b StGB nur derjenige, der formell über die Daten verfügen darf, Verletzter sein kann (vgl. Lenckner in Schönke/Schröder, StGB, 28. Aufl., § 205 Rn. 4 m. w. N., Bundestagsdrucksache 16/3656, S. 12). Ein relatives Antragserfordernis in Fällen der Bagatellkriminalität zur Verhinderung von unnötigen Strafverfahren ist da-

rüber hinaus auch in den Fällen von § 202a Absatz 3 und § 202b Absatz 2 StGB-E, jeweils auch im Falle des Versuchs, gerechtfertigt.

Für § 202d Absatz 1 StGB-E kann insoweit nichts anderes gelten.

Zu Artikel 2 (Änderung der StPO)

Zu Nummer 1 (§ 100a Absatz 2 Nummer 1 Buchstabe g_1 -neu- StPO-E),
Nummer 2 (§100c Absatz 2 Nummer 1 Buchstabe e_1 -neu- StPO-E),
Nummer 3 (§ 112a Absatz 1 Satz 1 Nummer 2 StPO-E)

Weiteres Kernstück neben der Anpassung der materiellen Normen der §§ 202a und 202b StGB sowie der Einführung des neuen § 202d StGB-E sind Änderungen des Rechts der Telekommunikationsüberwachung (§ 100a StPO), der Maßnahmen ohne Wissen des Betroffenen (§ 100c StPO) sowie des Rechts der Untersuchungshaft (§ 112a StPO). Durch eine Ergänzung der Kataloge des § 100a Absatz 2 Nummer 1 StPO, des § 100c Absatz 2 Nummer 1 StPO und des § 112a Absatz 1 Satz 1 Nummer 2 StPO werden diese zur Bekämpfung der organisierten Kriminalität notwendigen Maßnahmen den Strafverfolgungsbehörden zur Verfügung gestellt. Infolge der Aufnahme der qualifizierten Tatbestände in den Katalog des § 100a Absatz 2 StPO wird ergänzend eine allgemeine Erhebungsbefugnis für Verkehrsdaten nach § 100g Absatz 1 Nummer 1 StPO bestehen. Insbesondere die Telekommunikationsüberwachung erscheint aufgrund der vielfach aus dem Ausland heraus tätigen gewerbs- und bandenmäßigen Datenhehler als entscheidendes Mittel, um eine effektive Strafverfolgung zu gewährleisten.

Zu Nummer 4 (§ 3, § 60 Nummer 2, § 68b Absatz 1 Satz 4 Nummer 1, § 97 Absatz 2 Satz 3, § 102, § 138a Absatz 1 Nummer 3, § 160a Absatz 4 Satz 1 StPO-E)

Da es sich bei der Datenhehlerei um ein Anschlussdelikt handelt, bedürfen die entsprechenden Regelungen in der Strafprozessordnung (§§ 3, 60 Nummer 2, § 68b Absatz 1 Satz 4 Nummer 1, § 97 Absatz 2 Satz 3, §§ 102, 138a Absatz 1 Nummer 3, § 160a Absatz 4 Satz 1 StPO) der Anpassung.

Zu Artikel 3 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.

Anlage

Der Bundesrat hat in seiner 920. Sitzung am 14. März 2014 folgende Entschließung gefasst:

Entschließung

Der Gesetzentwurf sieht vor, die mit Bereicherungs- oder Schädigungsabsicht vorgenommene Weitergabe von rechtswidrig erlangten Daten unter Strafe zu stellen und damit eine bisher grundsätzlich bestehende Strafbarkeitslücke zu schließen. Amtsträger, die sich allein dienstbezogen bemakelte Daten verschaffen, sollen von einer Bestrafung ausgeschlossen werden. In diesem Zusammenhang stellt der Bundesrat fest, dass der Ankauf sogenannter Steuer-CDs bereits nach dem geltenden Recht zulässig ist.

Anlage 2

Stellungnahme der Bundesregierung

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

Der Gesetzentwurf des Bundesrates enthält einen neuen Straftatbestand der Datenhehlerei (§ 202d des Strafgesetzbuches – StGB). Weiter sind vorgesehen die Aufnahme qualifizierter Begehungsweisen mit entsprechenden Strafschärfungen sowie von Versuchsstrafbarkeiten in den Straftatbeständen des Ausspähens von Daten und des Abfangens von Daten (§§ 202a, 202b StGB) und die Ausweitung der Ermittlungsmöglichkeiten der Telekommunikationsüberwachung, der akustischen Wohnraumüberwachung sowie der Untersuchungshaft durch die entsprechende Erweiterung der Straftatenkataloge in § 100a Absatz 2, § 100c Absatz 2 und § 112a der Strafprozessordnung um die in dem Entwurf vorgesehenen qualifizierten Begehungsweisen.

Der Handel mit rechtswidrig erlangten Daten, insbesondere auf einschlägigen Plattformen im Internet, stellt auch aus Sicht der Bundesregierung ein ernst zu nehmendes Problem dar. Die Bundesregierung teilt die Auffassung des Bundesrates, dass dem auch mit den Mitteln des Strafrechts entgegenzuwirken ist und Strafbarkeitslücken in diesem Bereich geschlossen werden sollten. Sie begrüßt daher die Gesetzesinitiative des Bundesrates. Die mit dem Gesetzentwurf vorgeschlagene Einführung eines neuen Straftatbestandes der Datenhehlerei erscheint grundsätzlich geeignet, die auch vom 69. Deutschen Juristentag 2012 in München befürwortete Stärkung des Geheimnis- und Datenschutzes im Internet durch das Strafrecht herbeizuführen.

Im Übrigen beabsichtigt die Bundesregierung – entsprechend den Vorgaben im Koalitionsvertrag – einen eigenen Gesetzentwurf zur Anpassung des Strafrechts an das digitale Zeitalter und insbesondere zur Strafbarkeit der Datenhehlerei vorzulegen.

Vor dem Hintergrund der verursachten Schäden, insbesondere im Hinblick auf höchstpersönliche Rechtsgüter, wird dabei die Aufnahme qualifizierter Begehungsweisen zu prüfen sein; darüber hinaus werden auch die vom Bundesrat ebenfalls vorgeschlagene Aufnahme von Versuchsstrafbarkeiten sowie die Ausweitung strafprozessualer Eingriffsbefugnisse geprüft werden.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333