Bundesrat **Drucksache** **……./..**

Gesetzesantrag
des Landes Hessen

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. Diese sind üblicherweise mit Passwörtern oder sonstigen Sicherungscodes gegen den Zugriff Dritter geschützt. Mittels des Einsatzes von Schadsoftware und unter Überwindung dieser Zugangshindernisse 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 oder Sicherungscodes 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 und Sicherungscodes aller Art statt. Die Erkenntnisse der nationalen und internationalen Strafverfolgungsorgane deuten darauf hin, dass die Fallzahlen und die daraus resultierenden Schäden in diesem Zusammenhang deutlich steigen.

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

B. Lösung

Der Entwurf trägt dem Anliegen, der Schließung bestehender Strafbarkeitslücken in Fällen des Handels mit Sicherungscodes bzw. mit ursprünglich gesicherten und rechtswidrig erlangten Daten, durch die Einführung eines neuen Straftatbestands der Datenhehlerei (§ 259a StGB-E) Rechnung. Nach Absatz 5 werden Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen, nicht vom Tatbestand der Datenhehlerei erfasst.

Zweites Kernstück sind Änderungen des Rechts der Telekommunikationsüberwachung (§ 100a StPO) und 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 die zur effektiven Bekämpfung der gewerbs- und bandenmäßigen Datenhehlerei notwendigen Ermittlungsmaßnahmen den Strafverfolgungsbehörden 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.

Davon Bürokratiekosten aus Informationspflichten:

Keine.

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. 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 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.

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 Artikel … des Gesetzes vom … (BGBl. I S. …) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 259 folgende Angabe eingefügt:
   „§ 259a Datenhehlerei“

2. Nach § 259 wird folgender § 259a eingefügt:

„§ 259a
Datenhehlerei

(1) Wer Passwörter oder sonstige Sicherungscodes, welche den Zugang zu Daten (§ 202a Abs. 2) ermöglichen und die ein anderer ausgespäht oder sonst durch eine rechtswidrige Tat erlangt hat, ankauft oder sich oder einem Dritten verschafft, sie absetzt oder absetzen hilft, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer Daten (§ 202a Abs. 2), die ein anderer ausgespäht oder sonst durch eine rechtswidrige Tat erlangt hat und welche von dem letzten befugten Inhaber durch Passwörter oder sonstige Sicherungscodes gesichert worden waren, ankauft oder sich oder einem Dritten verschafft, sie absetzt oder absetzen hilft, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.

(3) Die §§ 247, 260, 260a gelten sinngemäß.

(4) Der Versuch ist strafbar.

(5) Die Absätze 1 bis 4 gelten nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen.“

Artikel 2
Änderung der Strafprozessordnung

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

1. Dem § 100a Absatz 2 Nummer 1 Buchstabe l und § 100c Absatz 2 Nummer 1 Buchstabe k werden jeweils die Wörter „jeweils auch in Fällen der Datenhehlerei unter den in § 259a Absatz 3 in Verbindung mit § 260 oder § 260a genannten Voraussetzungen,“ angefügt.

2. In § 112a Absatz 1 Satz 1 Nummer 2 werden nach der Angabe „260“ die Wörter „auch in Verbindung mit § 259a Absatz 3" eingefügt.

3. In den §§ 3, 60 Nummer 2, § 68b Absatz 1 Satz 4 Nummer 1, § 97 Absatz 2 Satz 3, §§ 102, 138a Absatz 1 Nummer 3 und § 160a Absatz 4 Satz 1 werden die Wörter „oder Hehlerei“ jeweils durch ein Komma und die Wörter „Hehlerei oder Datenhehlerei“ ersetzt.

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 41. Strafrechtsänderungsgesetz 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 resultierenden Umsetzungsbedarf nachgekommen ist, wurden zuletzt Regelungen getroffen, um den Missbrauch der Informationstechnologie bekämpfen.

Diese genügen jedoch nicht, da die strafrechtliche Praxis gezeigt hat, dass weiterhin spürbare Strafbarkeitslücken bestehen. Grund hierfür ist, dass das Strafgesetzbuch in seiner gegenwärtigen Form weiterhin 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 (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ postuliert 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, Rz. 33 – juris – zur Geltung des Rechts auf informationelle Selbstbestimmung im Privatrechtsverkehr).

Eine Strafbarkeitslücke besteht beim Handel mit Sicherungscodes sowie beim Handel mit ursprünglich gesicherten und 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.

Diese ursprünglich gesicherten 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. zum Ganzen: Gutachten C von Prof. Dr. Ulrich Sieber zum 69. Deutschen Juristentag „Straftaten und Strafverfolgung im Internet“, B., I., 1., lit. c und d 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 deutlich steigen. Die polizeiliche Kriminalstatistik verzeichnet seit Jahren steigende Fallzahlen im Bereich der Delikte gegen die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme und Daten.

Die bestehenden Strafnormen (z.B. in §§ 202a ff., 263, 263a, 269 StGB, §§ 106 ff. UrhG, §§ 43, 44 BDSG, §§ 17 ff. UWG) erfassen die Weitergabe von Sicherungscodes sowie die Weitergabe ursprünglich gesicherter und rechtswidrig erlangter Daten jedoch nur in Teilbereichen, da die Verkäufer und Käufer der Sicherungscodes bzw. der missbräuchlich erlangten 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 oder Sicherungscodes in den Internetforen erst zum Verkauf angeboten werden und damit zu ihrem widerrechtlichen Gebrauch noch nicht unmittelbar angesetzt wird. Auch wenn die verkauften Daten oder Sicherungscodes 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 Sicherungscodes oder 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 Abs. 1 Nr. 1 die Weitergabe von „Passwörtern“ oder „Sicherungscodes“. Strafbar ist das Sich-Verschaffen oder Weitergeben dieser Daten aber nur, wenn dies der Vorbereitung einer

(zumindest in Umrissen konkretisierten) 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 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 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 Sicherungscodes oder mit ursprünglich gesicherten und rechtswidrig erlangten Daten zurück. Dies zeigt sich auch an der vergleichsweise niedrigen Strafandrohung von bis zu zwei Jahren Freiheitsstrafe, während die Hehlerei 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 Sicherungscodes bzw. der sonstigen nicht unmittelbar wahrnehmbaren Daten im Sinne des § 202a Abs. 2 StGB noch beim späteren Handel mit diesen Daten handelt es sich jedoch um ein auf die Computernutzung beschränktes Phänomen. Da Sicherungscodes und 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 Sicherungscodes und Daten, dass es nicht darauf ankommen darf, auf welchem rechtswidrigen Weg die Sicherungscodes und Daten erlangt wurden.

Die Grenze zur Strafbarkeit verläuft am Tatbestandsmerkmal der Sicherung der Daten. Insoweit hat das Bundesverfassungsgericht bereits einschränkend darauf hingewiesen, dass es dem Einzelnen im Rahmen seiner Kommunikationsprozesse regelmäßig möglich und zumutbar ist, geeignete Vorsorgemaßnahmen zu treffen, um seine Geheimhaltungsinteressen zu wahren (BVerfG, 1 BvR 2027/02, a.a.O., Rz. 32). Die Sicherung der Daten verleiht ihnen daher ihre besondere Schutzwürdigkeit. Die Überwindung einer Zugangssicherung bzw. deren konkrete Gefährdung indiziert die Bedeutung der geschützten Daten oder des geschützten Informationssystems für das Opfer, verdeutlicht dem Täter die Grenze fremder

Zuständigkeit, verlangt von ihm ein bestimmtes Maß an krimineller Energie und liefert auch ein Indiz für sein Unrechtsbewusstsein. (vgl. Sieber, a.a.O., C 86).

Weiterer Anpassungsbedarf hinsichtlich der §§ 100a Absatz 2 Nummer 1, 100c Absatz 2 Nummer 1 und 112a Absatz 1 Satz 1 Nummer 2 StPO ergibt sich daraus, dass der organisierte Handel mit Sicherungscodes und rechtswidrig erlangten Daten eine Form der organisierten Kriminalität darstellt, die mit den für diese Fälle vorgesehenen Mitteln bekämpft werden sollte.

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 Abs. 1 Nr. 1 GG.

III. Auswirkungen

Durch die Einführung eines neuen Straftatbestands sowie die Erweiterung der strafprozessualen 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 Entwurf 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 § 259a-E (Nummer 2).

Zu Nummer 2 (§ 259a-E)

Die vorgeschlagene Regelung soll als neuer § 259a StGB-E in den Einundzwanzigsten Abschnitt des Besonderen Teils des Strafgesetzbuchs eingefügt werden. Für eine systematische Regelung an dieser Stelle spricht die in enger Anlehnung an den Tatbestand der Hehlerei in § 259 StGB vorgeschlagene Ausgestaltung als Anschlussdelikt. Inhaltlich können Daten im weiteren Sinn zwar nicht pauschal den körperlichen Sachen im Sinne des § 90 BGB gleichgestellt werden, jedoch ist eine Annäherung im Hinblick auf die vergleichbare Strafwürdigkeit verschiedener Fallkonstellationen erforderlich. In Entsprechung zu dem Rechtsgut der formellen Verfügungsbefugnis, die aus dem Recht über den gedanklichen Inhalt der Information erwächst, sind Schutzobjekt allein gesicherte Daten. Im Einzelnen geschützt sind Passwörter und sonstige Sicherungscodes, welche den Zugang zu Daten (§ 202a Abs. 2 StGB) ermöglichen (Abs. 1) sowie die vormals vom letzten befugten Inhaber durch Passwörter und sonstige Sicherungscodes geschützten Daten (Abs. 2). Durch die weite Fassung der möglichen Vortaten wird insoweit ein umfassender Schutz der formellen Verfügungsbefugnis des Einzelnen über seine gesicherten Daten sowie des allgemeinen Rechts auf Nichtöffentlichkeit der Kommunikation gewährleistet. Da mit dem Verfügungsrecht über Daten häufig wirtschaftliche Interessen verbunden sind, soll als Schutzreflex auch das Vermögen des Dateninhabers geschützt werden.

Entscheidendes Tatbestandsmerkmal für die Überschreitung der Grenze zur Strafbarkeit ist der Umstand der Sicherung der Daten. Dieser Einschränkung auf besonders gesicherte Daten kommt maßgebliche Bedeutung für die Eingrenzung des Tatbestandes zu, da hierdurch die Grenzen fremder Zuständigkeit aufgezeigt sowie das Interesse des (formell) Berechtigten am Schutz seiner Verfügungsbefugnis und seines Geheimhaltungsinteresses dokumentiert wird. Erst dies rechtfertigt im Ergebnis die Anwendung des Strafrechts als Ultima Ratio.

Durch den Handel mit Sicherungscodes werden die entsprechend geschützten Daten erheblich gefährdet, da für den Handel mit Sicherungscodes, die den Zugang zu Daten anderer Personen ermöglichen, kaum ein zu rechtfertigender Anwendungsbereich denkbar ist und ein anderer Zweck als die missbräuchliche Verwendung nahezu nicht in Betracht kommt. Für Einzelfälle sowie eine mögliche Tätigkeit von IT-Sicherheitsunternehmen ist eine Tatbestandsausschlussregelung in § 259a Abs. 5 StGB vorgesehen.

Beim Handel mit ursprünglich gesicherten Daten wurde die Sicherung bereits durchbrochen, die formelle Verfügungsbefugnis des Einzelnen über seine Daten also bereits verletzt. Zwar ist die Sicherung im Falle des Handels mit diesen ursprünglich gesicherten Daten nicht mehr vorhanden, jedoch soll diese Sicherung insoweit fortwirken, wie der Täter diese ursprüngliche Sicherung in seinen Vorsatz aufgenommen hat. Durch die Verletzung der Verfügungsbefugnis und des Geheimhaltungsinteresses des letzten befugten Dateninhabers wird die Rechtsgutverletzung von dem Datenhändler, der diese Situation zumindest billigend in Kauf nimmt, perpetuiert und zum eigenen finanziellen Vorteil ausgenutzt. Aus dieser weiteren Vertiefung der Rechtsgutverletzung zum eigenen finanziellen Vorteil rechtfertigt sich die Strafwürdigkeit.

Der Tatanreiz für den Vortäter wird in der überwiegenden Anzahl der Fälle aus dem vorhandenen kriminellen Absatzmarkt für rechtswidrig erlangte Daten oder aus dem eigenen Willen zur rechtswidrigen Nutzung dieser Daten resultieren. Daher sieht der Tatbestand als subjektives Merkmal die Selbst- oder Drittbereicherungsabsicht vor. Darüber hinaus sind aber auch Fallkonstellationen denkbar, in welchen der Täter nicht eine finanzielle Bereicherung erstrebt, sondern beabsichtigt, dem Geschädigten einen materiellen oder immateriellen Nachteil zuzufügen. Dies ist gleichermaßen schutzwürdig.

Zu Absatz 1

Tatobjekt sind – in Anlehnung an § 202c Abs. 1 Nr. 1 StGB – Passwörter und Sicherungscodes, die den Zugang zu nicht unmittelbar wahrnehmbaren Daten ermöglichen. Der Schutz der unmittelbar wahrnehmbaren Daten ist ausreichend gewährleistet. Auch wenn die Formulierung von Daten in der Mehrzahl spricht, wird auch ein einzelnes gesichertes Datum geschützt (Graf, Münchner Kommentar, StGB, 1. Auflage, § 202a, Rn. 8).

Als Vortaten, an welche die Datenhehlerei anknüpft, kommen insbesondere das Ausspähen oder Abfangen von Daten gemäß §§ 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 jegliche rechtswidrige Taten erfasst, die der Erlangung von Passwörtern oder sonstigen Sicherungscodes dienen. Allein vertragswidrige oder ordnungswidrige Handlungen sind gemäß § 11 Abs. 1 Nr. 5 StGB vom Tatbestand ausgenommen. Die explizite Normierung der Passwörter oder sonstigen Sicherungscodes als „fremde“ ist entbehrlich, da es sich hierbei um eine Selbstverständlichkeit handelt.

Die Tatbestandshandlungen des § 259a Abs. 1 StGB-E sind dem § 259 Abs. 1 StGB entnommen und bedürften keiner Erweiterung. Sie sind durch die Rechtsprechung und Literatur hinreichend konkretisiert.

Zur Rechtfertigung der Strafandrohung wegen der für die geschützten Daten bestehenden Gefahr durch die Verschaffung von Passwörtern oder sonstigen Sicherungscodes bedarf es – neben dem notwendigen Dolus eventualis im Hinblick auf das Tatobjekt und die rechtswidrige Vortat – noch eines weiteren subjektiven Elements. Hierzu dienen die alternativen Tatbestandsmerkmale der Bereicherungsabsicht und der Schädigungsabsicht, die der Regelung in § 44 Abs. 1 BDSG entsprechen.

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 Abs. 1, 258 Abs. 1, 259 Abs. 1 StGB).

Zu Absatz 2

Der aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleiteten Schutzwürdigkeit des Tatobjekts Daten trägt Absatz 2 durch einen fortwirkenden Schutz einmal befugt gesicherter Daten Rechnung.

Tatobjekt sind Daten, also Informationen jeder Art. Zur Begrenzung auf die strafwürdigen Fälle und im Hinblick auf die Systematik der §§ 202a ff. StGB ist der Datenbegriff dahingehend beschränkt, dass nur die nicht unmittelbar wahrnehmbaren Daten erfasst werden. Die Anbindung an das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und damit die Rechtfertigung der Strafdrohung folgt aus der vom letzten befugten Inhaber vorgenommenen Sicherung der Daten, da diese die Grenze fremder Zuständigkeit markiert.

Der Tatbestand setzt daher in objektiver Hinsicht voraus, dass die Daten von dem letzten befugten Inhaber durch Passwörter oder Sicherungscodes gesichert gewesen sein müssen und mittels einer rechtswidrigen Tat erlangt worden sein müssen. Die Sicherung muss vor der Begehung der rechtswidrigen Vortat noch Bestand gehabt haben.

Die Tathandlungen entsprechen wiederum § 259 Abs. 1 StGB.

In subjektiver Hinsicht muss der Täter es zumindest für möglich halten, dass die erlangten Daten von dem letzten befugten Inhaber mit einer entsprechenden Sicherung versehen worden waren und auch einer rechtswidrigen Vortat stammen.

Zusätzlich muss der Täter aus Bereicherungs- oder Schädigungsabsicht gehandelt haben, wobei die Tatbestandsmerkmale der Regelung in § 44 Abs. 1 BDSG entsprechen.

Zu Absatz 3

In der Variante 1 des Absatzes 3 wird auf die auch in § 259 Abs. 2 StGB vorgesehene Verfahrensvoraussetzung des § 247 StGB verwiesen. Wurde eine Datenhehlerei im Haus- und Familienverband begangen, so ist es gerechtfertigt, zum Schutz des häuslichen Friedens die Strafverfolgung von einem Strafantrag abhängig zu machen.

Da es sich bei § 259a StGB-E nicht um ein Vermögens- oder Eigentumsdelikt handelt, sondern um eine Straftat gegen die formelle Verfügungsbefugnis des Einzelnen über seine Daten, kommt zur Kennzeichnung von Fällen der Bagatellkriminalität eine Bezugnahme auf das Geringwertigkeitsmerkmal des § 248a StGB nicht in Betracht. Fälle der Bagatellkriminalität sind daher über die allgemeinen Opportunitätsvorschriften der §§ 153, 153a StPO zu erfassen.

Die gewerbs- und bandenmäßige Datenhehlerei ist eine Form der organisierten Kriminalität. Aus diesem Grund enthält Absatz 3 in den Varianten 2 und 3 einen Verweis auf die Qualifikationstatbestände der §§ 260, 260a StGB. Dadurch wird der besonderen Gefährlichkeit sowie dem erhöhten Unrechts- und Schuldgehalt der gewerbs- und bandenmäßigen Begehungsweise Rechnung getragen.

Zu Absatz 4

Absatz 4 normiert die Versuchsstrafbarkeit, da nur hierdurch ein umfassender Schutz ermöglicht wird.

Zu Absatz 5

Um eine ungewollte Kriminalisierung von Personen zu vermeiden, die sich allein dienst- bzw. berufsbezogen bemakelte Sicherungscodes oder Daten verschaffen, sieht § 259a Abs. 5 StGB-E eine Tatbestandsausschlussregelung für die Fälle vor, in denen ausschließlich in Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten gehandelt wird. Die Tatbestandsausschlussregelung lehnt sich hierbei an § 184b Abs. 5 StGB (Besitz kinderpornographischer Schriften) an.

Dies würde beispielsweise Amtsträger umfassen, die rechtswidrig erlangte und ursprünglich gesicherte Daten erwerben, um ihre Amtspflichten zu erfüllen.

Weiterhin ist der Tatbestandsausschluss auch im Lichte der Pressefreiheit des Art. 5 Abs. 1 Satz 2 GG auszulegen. Der Erwerb rechtswidrig erlangter und ursprünglich gesicherter Daten durch Medienmitarbeiter zum Zweck der Veröffentlichung ist als Erfüllung rechtmäßiger beruflicher Pflichten nicht strafbar, sofern er ausschließlich der verfassungsrechtlich geschützten Funktion der freien Presse dient.

Ungeachtet der Frage, ob in solchen Fällen alle Tatbestandsmerkmale vorliegen, verdeutlicht dieser Tatbestandsausschluss die Straflosigkeit des Handelns in ausschließlich dienstlicher oder beruflicher Pflichterfüllung. Dabei wird durch das Ausschließlichkeitserfordernis sichergestellt, dass die dienstliche oder berufliche Aufgabe der einzige Grund für die Verschaffung, den Absatz oder die Absatzhilfe der Daten sein darf, da nur in diesem Fall ein strafwürdiges Verhalten nicht gegeben ist.

Zu Artikel 2 (Änderung der StPO)

Zu Nummer 1 und 2 (§§ 100a Absatz 2 Nummer 1 Buchstabe l, 100c Absatz 2 Nummer 1 Buchstabe k und 112a Absatz 1 Satz 1 Nummer 2 StPO):

Zweites Kernstück neben der Einführung des neuen § 259a StGB-E sind Änderungen des Rechts der Telekommunikationsüberwachung (§ 100a StPO), der Maßnahmen ohne Wis-

sen 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 entsprechend der Regelungen zur gewerbs- und bandenmäßigen (Sach-)Hehlerei werden diese zur Bekämpfung der organisierten Kriminalität notwendigen Maßnahmen den Strafverfolgungsbehörden zur Verfügung gestellt. Infolge der Aufnahme des qualifizierten Tatbestandes in den Katalog des § 100a Abs. 2 StPO wird ergänzend eine allgemeine Erhebungsbefugnis für Verkehrsdaten nach § 100g Abs. 1 Nr. 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 3 (§ 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):

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.