Der missratene Tatbestand der neuen Datenhehlerei (§ 202d StGB)

Von Prof. Dr. **Carl-Friedrich Stuckenberg**, LL.M., Bonn

Die mit dem Gesetz zur Wiedereinführung der Vorratsdatenspeicherung vom 10.12.2015 in das StGB eingefügte Vorschrift der Datenhehlerei (§ 202d) soll als Analogon zu § 259 StGB die Tatbestände der §§ 202a ff., 303a ff. StGB ergänzen und ist aus Versatzstücken dieser Normen zusammengesetzt. Während § 259 StGB bestimmte Formen der Verletzung der zivilrechtlichen Rechtspositionen Eigentum und Besitz unter Strafe stellt, ist das Schutzgut der Computerstraftatbestände des StGB bis heute unklar, weil es keine entsprechende primäre Normenordnung für Daten gibt. Der Gesetzgeber hat es sich zu leicht gemacht, indem er dieses grundsätzliche Problem ignorierte und aufgrund falscher Verallgemeinerungen und falscher Analogien den Unrechtstyp falsch bestimmte und somit einen Straftatbestand schuf, der imaginäre Rechte schützt. War zuvor schon zweifelhaft, ob Bedarf für die Pönalisierung der Weitergabe illegal erlangter Daten besteht, so erweist sich die nun getroffene Regelung in gleichem Maße als handwerklich fehlerhaft.

I. Einleitung

Am 16.10.2015 hat der Deutsche Bundestag das „Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“ beschlossen,[1] dem der Bundesrat am 6.11.2015 zugestimmt[2] hat. Das am 10.12.2015 verkündete Gesetz[3] führt eine neue Version der Vorratsdatenspeicherung ein und ist dementsprechend umstritten. Gleichsam im Windschatten dieser rechtspolitischen Großkontroverse und an etwas versteckter Stelle zwischen Änderungen des Justizvergütungsgesetzes (Art. 4) und Erfüllung des Zitiergebots (Art. 6) hat das Artikelgesetz auch (in Art. 5) eine Vorschrift über die Datenhehlerei in das Strafgesetzbuch eingefügt. Sie lautet:

> „§ 202d Datenhehlerei
> (1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer 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 drei Jahren oder mit Geldstrafe bestraft.
> (2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.
> (3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere
> 1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
> 2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.“

Die Vorschrift hat bisher nur wenig Beachtung gefunden, die neben Zweifeln an der Existenz der behaupteten Strafbarkeitslücke vor allem dem jetzigen Abs. 3 galt,[4] der die Straflosigkeit des Ankaufs von Steuer-CDs durch Finanzverwaltungen sowie von Whistleblower-Informationen durch Journalisten gewährleisten soll. Dabei handelt es sich jedoch um bloße Folgeprobleme; Thema dieses Beitrags ist vielmehr die Tatbestandsfassung des § 202d Abs. 1 StGB, die nicht nur rechtspolitisch zweifelhaft, sondern auch dogmatisch in mehrfacher Hinsicht misslungen erscheint.

Der Tatbestand steht gleich für mehrere Entwicklungstendenzen: Zum einen für die zunehmende Anpassung des StGB an die Herausforderungen des digitalen Zeitalters, mithin den Ausbau dessen, was als „Computerstrafrecht“, „Daten-“ oder „Informationsstrafrecht“ firmiert, zum anderen kulminiert hierin die notorische Unklarheit über das dogmatische Fundament dieser Tatbestandsgruppe, die immer noch auf der Suche nach einem eigenen Rechtsgut im analytischen Sinne oder Schutzgut ist. Schließlich ist § 202d StGB ein Beispiel für einen bestimmten Gesetzgebungsstil, nämlich der Schließung von Strafbarkeitslücken durch „cut and paste“, der aus Versatzstücken geltender Normen einen neuen Tatbestand zusammennäht und sich dabei durch falsche Analogien, unbedachte Verallgemeinerungen und dogmatische Unbekümmertheit leiten lässt. Mit Verkündung im Bundesgesetzblatt wurde diesem legislativen Patchwork normatives Leben – Geltung – eingehaucht, doch ob der Tatbestand wirklich nötig ist, seine Aufgabe erfüllen kann und sich in die Systematik des StGB einfügt, ist ausgesprochen fragwürdig.

Vor der kritischen Betrachtung sei der normative Zusammenhang, in dem § 202d StGB steht, kurz umrissen:

II. Zur Entstehungsgeschichte

1. Die Entwicklung der Tatbestände des „Computerstrafrechts“

Die überkommenen Tatbestände des StGB können das zumeist als „Computerkriminalität“ bezeichnete sozialschädliche Verhalten, das mittels elektronischer Datenverarbeitung

[1] BT-Prot. 18/131, S. 12779A; BR-Drs. 492/15; damit ist der Regierungsentwurf BT-Drs. 18/5088 unverändert angenommen worden.
[2] BR-Prot. 938, S. 415 f.
[3] BGBl. I 2015, S. 2218 (2227).

[4] Zu den Entwürfen *Hahn/Bußmann*, DRiZ 2012, 223; *Klengel/Gans*, ZRP 2013, 16; *Golla/v. zur Mühlen*, JZ 2014, 668; *Franck*, RDV 2015, 180; *Wefing*, DRiZ 2015, 212; *Dix/Kipker/Schaar*, ZD 2015, 300 (304 f.); *Buermeyer*, SZ v. 5.10.2015, http://www.sueddeutsche.de//digital/netzpolitik-datenhehlerei-1.2676184; *Selz*, in: Taeger (Hrsg.), Internet der Dinge, Digitalisierung von Wirtschaft und Gesellschaft, 2015, S. 915; zum Gesetz *Roßnagel*, NJW 2016, 533 (537); *Golla*, ZIS 2016, 192 (198); *Singelnstein*, ZIS 2016, 432.

begangen wird oder diese zum Angriffsziel nimmt, nur zum Teil zu erfassen. Zum einen fallen die in Computersystemen verarbeiteten „Daten" als Tatobjekte nicht unter den Sachbegriff, da sie unkörperlich sind. Was „Daten" sind, ist zwar bislang nicht gesetzlich definiert,[5] doch verweist die herrschende Meinung auf DIN 44300 und geht von einem weiten Datenbegriff aus, der „Gebilde aus Zeichen oder kontinuierliche Funktionen, die auf Grund bekannter oder unterstellter Abmachungen Informationen darstellen", umfasst; kurz: Daten sind codierte Informationen. Informationen sind Angaben über einen Gegenstand, einen Zustand oder ein Ereignis der realen oder irrealen Welt.[6] Wer sich unbefugt Daten verschafft oder sie verändert, begeht dadurch weder Diebstahl noch Sachbeschädigung. Zum anderen lassen sich automatisierte Vorgänge des Rechtsverkehrs nicht durch Vorschriften schützen, die die Täuschung von Menschen voraussetzen. Wer einen Automaten mit falschen Daten füttert, um sich zu bereichern, ist weder wegen Betruges noch Urkundenfälschung strafbar.

Der deutsche Gesetzgeber hat vor fast genau 30 Jahren erstmals auf die technische Entwicklung reagiert und mit dem 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität 1986[7] mehrere auf „Computerkriminalität" zugeschnittene Tatbestände in das StGB eingefügt, namentlich das Ausspähen von Daten (§ 202a), den Computerbetrug (§ 263a), die Fälschung beweiserheblicher Daten (§§ 269, 270), die Datenveränderung (§ 303a) und die Computersabotage (§ 303b).

Computer- und Internetkriminalität ist längst auch Gegenstand von Rechtsakten der Europäischen Union[8] sowie des Europarates, unter dessen Ägide 2001 in Budapest die „Convention on Cybercrime" geschlossen wurde,[9] die derzeit in 48 Staaten in Kraft ist und in vielem das Vorbild für den Rahmenbeschluss des Rates der Europäischen Union von 2005 über Angriffe auf Informationssysteme[10] wurde, welcher nun durch die Richtlinie vom 12.8.2013[11] ersetzt worden ist.

Die Aktivitäten des deutschen Gesetzgebers in diesem Bereich dienten im letzten Jahrzehnt stets der Umsetzung des europäischen Rechts, z.B. durch das 35. Strafrechtsänderungsgesetz von 2003[12] und das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität von 2007,[13] das u.a. die Vorschriften der § 202b (Abfangen von Daten) und das gemeinsame Vorbereitungsdelikt des § 202c StGB einfügte. Die durch die neue Richtlinie geforderte Erhöhung des Strafrahmens des § 202c StGB ist durch das am 26.11.2015 in Kraft getretene Korruptionsbekämpfungsgesetz[14] erfolgt.

Im Gegensatz dazu ist die Datenhehlerei ein deutsches Eigengewächs, das weder auf europäische Vorgabe noch Anregung zurückgeht und, soweit ersichtlich, auch keine Vorbilder im europäischen Ausland hat. Erstaunlicherweise sind auch die umfangreichen Aktivitäten der seit 2007 bestehenden und beim United Nations Office on Drugs and Crime (UNODC) angesiedelten Expertengruppe der Vereinten Nationen zu „identity-related crime"[15] ebenso wenig berücksichtigt worden wie die diesbezüglichen Resolutionen des Wirtschafts- und Sozialrats (ECOSOC)[16].

2. Die Genese der Datenhehlerei

Die Vorgeschichte des § 202d StGB beginnt mit einem Beschluss der 83. Konferenz der Justizministerinnen und Justizminister vom Juni 2012,[17] der Strafbarkeitslücken beim Handel mit rechtswidrig erlangten Daten feststellte und das Land Hessen mit der Formulierung eines Gesetzentwurfs beauftragte. Einen entsprechenden Beschluss hat auch der 69. Deutsche Juristentag im September 2012 gefasst,[18] obschon

[5] BT-Drs. 10/5058, S. 29; zur Kritik siehe *Hilgendorf*, ZStW 113 (2001), 650 (656); *Scheffler/Dressel*, ZRP 2000, 514 (516 f.).

[6] *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 6, 12. Aufl. 2011, § 202a Rn. 7.

[7] 2. WiKG v. 15.5.1986 = BGBl. I 1986, S. 721, dazu RegE BR-Drs. 150/83; BT-Drs. 10/318, Bericht des Rechtsausschusses BT-Drs. 10/5058.

[8] Nachweise bei *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, Rn. 93 ff.

[9] Convention on Cybercrime, done at Budapest, on 23 November 2001, ETS No. 185, in Kraft seit dem 1.7.2004; von Deutschland mit Wirkung vom 1.7.2009 ratifiziert = BGBl. II 2008, S. 1242. Zur Entstehungsgeschichte siehe *Schwarzenegger*, in: Donatsch/Forster/Schwarzenegger (Hrsg.), Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag, 2002, S. 305; zur Umsetzung in deutsches Recht siehe *Gercke*, MMR 2004, 728 ff., 801 ff.; *Hilgendorf/Valerius* (Fn. 8), Rn. 119 ff.

[10] Rahmenbeschluss des Rates der Europäischen Union (2005/222/JI) v. 24.2.2005 über Angriffe auf Informationssysteme = ABl. EU 2005 Nr. L 69/67.

[11] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates v. 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates = ABl. EU 2013 Nr. L 218/8.

[12] Art. 1 Nr. 10 des 35. StÄG v. 22.12.2003 = BGBl. I 2003, S. 2838.

[13] BGBl. I 2007, S. 1786; dazu *Borges/Stuckenberg/Wegener*, DuD 2007, 275; *Ernst*, NJW 2007, 2661; *Cornelius*, CR 2007, 682; *Popp*, Medien und Recht International 2007, 84; *Vahle*, DSB 10/2007, 14; *Stuckenberg*, Ad Legendum 2008, 82; *ders*., wistra 2010, 41; *Goeckenjan*, wistra 2009, 47.

[14] Gesetz zur Bekämpfung der Korruption v. 20.11.2015, Art. 1 Nr. 5 = BGBl. I 2015, S. 2025.

[15] Vgl. nur UNODC, Handbook on Identity-related Crime, 2011.

[16] Dazu *Stuckenberg*, in: Borges/Schwenk/Stuckenberg/Wegener (Hrsg.), Identitätsdiebstahl und Identitätsmissbrauch im Internet, 2009, S. 325 ff. m.w.N.

[17] 83. Konferenz der Justizministerinnen und Justizminister am 13. und 14.6.2012 in Wiesbaden.

[18] Verhandlungen des 69. DJT, Bd. 2/1, 2013, L 56, Beschluss II.3.

im vorbereitenden Gutachten von *Sieber*[19] von Datenhehlerei nirgends die Rede ist.

In einer ersten, im Januar 2013 bekannt gewordenen Fassung des hessischen Gesetzentwurfs trägt die Vorschrift die Nummer „§ 259a" und bezieht sich nur auf ausgespähte oder sonst rechtswidrig erlangte „Passwörter oder sonstige Sicherungscodes" sowie auf dadurch gesicherte Daten als Tatobjekte; die Tathandlungen wurden aus der Sachhehlerei des § 259 StGB übernommen.[20] Das sozialschädliche Phänomen, auf das der Entwurf zielt, ist der auch in *Siebers* Gutachten beschriebene,[21] in nicht öffentlichen Internetforen betriebene schwunghafte Handel mit bündelweise angebotenen Kreditkarten- und Bankdaten sowie sonstigen „digitalen Identitäten". Bei dieser Form der Arbeitsteilung seien die Datenhändler weder personenidentisch mit den Tätern, die die Datensätze erlangt haben, noch mit denen, die diese dann etwa für einen Computerbetrug einsetzen, weshalb die Datenweitergabe bisher weder von den Vorschriften des StGB noch des UrhG, BDSG oder UWG zureichend erfasst werde. Zwar bestrafe § 202c StGB das Sichverschaffen und Weitergeben von Passwörtern und Sicherungscodes, jedoch nur, wenn dies der Vorbereitung einer einigermaßen konkretisierten Tat des Ausspähens oder Abfangens von Daten diene, greife also nicht bei anderen Taten wie einem Computerbetrug und auch nicht, wenn die künftigen Taten noch nicht konkretisiert sind.[22] Die Strafvorschrift des § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 1 BDSG könne zwar im Einzelfall erfüllt sein, schütze aber z.B. juristische Personen nicht und biete mit maximal zwei Jahren Freiheitsstrafe keine ausreichende Sanktionsmöglichkeit, weshalb der Entwurf die Strafdrohungen der Sachhehlerei von bis zu fünf, bei gewerbs- oder bandenmäßiger Begehung bis zu zehn Jahren Freiheitsstrafe übernimmt.[23]

Der im Juni 2013 vom Bundesrat als neuer „§ 202d" eingebrachte Gesetzentwurf bezeichnet die Tatobjekte hingegen allgemeiner als „Daten im Sinne von § 202a Abs. 2", also nur nicht unmittelbar wahrnehmbare Daten, weil die unmittelbar wahrnehmbaren Daten ausreichend geschützt seien,[24] obgleich zuvor dargelegt wurde, dass sich der Schutz nicht nur auf Computerdaten beschränken dürfe[25]. Der Entwurf behauptet unumwunden, dass 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, […]".[26]

Die Problematik einer Analogie zum Sacheigentum wird unter Berufung auf *Siebers* Gutachten erkannt, gleichwohl aber eine Annäherung für nötig gehalten:

„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]."[27]

Als „Maßstab für die Überschreitung der Grenze zur Strafbarkeit", mithin als Analogon zur Eigenschaft von Sachen, in fremdem Eigentum zu stehen, kreiert der Entwurf die ebenso zutreffende wie inhaltslose Kategorie der „schutzwürdigen Daten". Absatz 2 des Entwurfs führt zwei Kriterien an: Zum einen dürfen die Daten nicht allgemein zugänglich sein, zum anderen müsse der Berechtigte wie bei § 29 BDSG ein „schutzwürdiges Interesse" an deren Nichtverwendung durch andere haben, das im Wege einer Interessenabwägung zu ermitteln sei.[28] Die Tathandlungen entsprechen jetzt denen

[19] *Sieber*, Gutachten C zum 69. DJT.

[20] Gesetzesantrag des Landes Hessen, veröffentlicht auf Netzpolitik.org am 15.1.2013: https://netzpolitik.org/wp-upload/Gesetzentwurf-Datenhehlerei.pdf, S. 4 (5.5.2016):
„§ 259a StGB-E
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."

[21] Vgl. *Sieber* (Fn. 19), C 23.

[22] Gesetzesantrag des Landes Hessen (Fn. 20), S. 8 f.; so auch der Referentenentwurf des BMJV: Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, Fassung v. 22.5.2015, S. 27, verfügbar unter: http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Hoechstspeicherfrist.pdf;jsessionid=C3A45FDB72FCCF27F45E5EC4782607B2.1_cid297?__blob=publicationFile&v=6 (5.5.2016).

[23] Gesetzesantrag des Landes Hessen (Fn. 20), S. 8 f.

[24] BT-Drs. 17/14362, S. 13 mit Verweis auf *Graf*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 2. Aufl. 2012, § 202a Rn. 12, der seinerseits BT-Drs. 10/5058, S. 29, zitiert, wo davon ausgegangen wurde, dass u.a. §§ 201, 202 StGB ausreichend seien. Diese 30 Jahre alte Einschätzung sollte überdacht werden.

[25] BT-Drs. 17/14362, S. 11.

[26] BT-Drs. 17/14362, S. 11.

[27] BT-Drs. 17/14362, S. 11.

[28] BT-Drs. 17/14362, S. 14.

des § 202c: „sich oder einem anderen verschaffen, einem anderen überlassen, verbreiten oder sonst zugänglich machen". Die Bereicherungsabsicht wird aus § 259 StGB, die alternative Schädigungsabsicht aus § 44 BDSG übernommen.[29] Der Gesetzentwurf verfiel der Diskontinuität und wurde 2014 erfolglos erneut eingebracht.[30]

Der jetzt Gesetz gewordene Entwurf der großen Koalition vom Juni 2015 lehnt sich an den Bundesratsentwurf an, verzichtet auf das reichlich vage Kriterium des „schutzwürdigen Interesses" und übernimmt auch die Tathandlungen aus § 202c StGB mit Ausnahme des dort genannten „Verkaufens",[31] das auf das europäische Vorbild zurückgeht, aber wegen des deutschen Abstraktionsprinzips schlecht passt. Gegenüber den Vorgängerentwürfen wird die Strafobergrenze deutlich gesenkt auf drei Jahre und damit an § 202a StGB angepasst, schwere Fälle wurden gestrichen. Die Ausnahmeregelungen des Absatzes 3 sind teils an § 184b Abs. 5, teils an § 353b Abs. 3a StGB angelehnt.[32]

III. Das Regelungskonzept des § 202d StGB

Nach der Gesetzesbegründung schützt der neue § 202d StGB „[…] das formelle Datengeheimnis, das durch die Vortat bereits verletzt worden ist, vor einer Aufrechterhaltung und Vertiefung dieser Verletzung. Bereits mit der Erlangung der Daten durch den Vortäter sind die formelle Verfügungsbefugnis desjenigen, der aufgrund seines Rechts an dem gedanklichen Inhalt über eine Weitergabe und Übermittlung der Daten entscheidet […], und damit das Interesse an der Aufrechterhaltung des Herrschaftsverhältnisses über eine Information […] beeinträchtigt worden. Dem Berechtigten wird mit der Vortat die ihm zustehende Entscheidung, wem seine Daten zugänglich sein sollen, aus der Hand genommen.

Diese Rechtsgutsverletzung wird aufrechterhalten und vertieft, wenn sich im Anschluss daran ein Dritter die gestohlenen Daten verschafft und damit die Daten weiterverbreitet werden. Mit dem Datenhehler erhält eine weitere Person die Möglichkeit, über die Zugänglichmachung der Daten anstelle des Berechtigten zu entscheiden. Zugleich kann es für den Berechtigten schwieriger werden, seine Daten nachzuverfolgen und die alleinige Verfügungsbefugnis über sie zurückzugewinnen."[33]

Wie bei der Sachhehlerei würden durch die Datenhehlerei aber auch allgemeine Sicherheitsinteressen beeinträchtigt, nämlich „durch den von der Hehlerei geschaffenen Anreiz zur Verübung von Vortaten".[34]

Taugliche Tatobjekte des § 202d StGB sind nur Daten, die „elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden" im Sinne des § 202a Abs. 2 StGB. Ausgeschlossen sind ferner „allgemein zugängliche" Daten, worunter mit § 10 Abs. 5 S. 2 BDSG solche Daten verstanden werden sollen, „die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann", weshalb bei ihnen ein „formelles Datengeheimnis" fehle.[35] Sonstige Einschränkungen gibt es nicht: Die fraglichen Informationen müssen weder zum persönlichen Lebens- oder Geheimbereich gehören noch ein Geschäftsgeheimnis im Sinne des UWG noch personenbezogene Daten im Sinne des Datenschutzrechts darstellen.[36]

Diese Daten muss ein anderer als der Täter durch eine „rechtswidrige Tat" erlangt haben. Als Vortaten kommen daher gem. § 11 Abs. 1 Nr. 5 StGB nur Straftaten in Betracht, mögen sie auch schuldlos begangen sein, namentlich Ausspähen und Abfangen von Daten gem. §§ 202a, 202b StGB, aber auch Diebstahl (§ 242 StGB) von Datenträgern, Betrug (§ 263 StGB), Computerbetrug (§ 263a StGB), Nötigung (§ 240 StGB), Fälschung technischer Aufzeichnungen (§ 269 StGB) oder Fälschung von Zahlungskarten (§ 152b StGB) usw.[37]

„Entsprechend der Rechtslage bei der Sachhehlerei" sei es nötig, aber auch ausreichend, dass die Vortat unabhängig von ihrer systematischen Einordnung in ihren praktischen Auswirkungen die „formelle Verfügungsbefugnis des Berechtigten" verletze.[38] Als Berechtigter sei derjenige anzusehen, „der über die Daten verfügen darf […], also grundsätzlich derjenige, der die Daten gesammelt und abgespeichert hat oder auf dessen Veranlassung die Speicherung erfolgt ist".[39]

Nicht ausreichend sei die bloße Verletzung öffentlicher Interessen, auch auf datenschutzrechtliche Betroffenheit komme es nicht an.[40] Nicht „durch eine rechtswidrige Tat erlangt" und somit ausgeschieden sind laut Gesetzesbegründung solche Daten, „die dem Vortäter bereits zur Verfügung stehen und die er unter Verletzung des Urheberrechts vervielfältigt. Ebenso wenig erlangt der Vortäter Daten durch eine rechtswidrige Tat, wenn er lediglich eine Vertragsverletzung, ein Disziplinarvergehen oder eine Ordnungswidrigkeit begeht. Als Vortat ist es daher nicht ausreichend, wenn in einem berechtigt genutzten System Daten lediglich unter Verletzung von vertraglichen Zugriffsbeschränkungen erlangt werden."[41]

Dieser Ausschluss nicht strafbarer Vortaten soll sich aus dem erwähnten Schutz „allgemeiner Sicherheitsinteressen"[42] ergeben. Nicht erfasst sind damit die typischen Steuer-CD- und Whistleblower-Fälle, in denen Personen, die etwa von Berufs wegen Zugriff auf Datensätze haben, diese vertrags- oder dienstrechtswidrig weitergeben, also gleichsam „Datenunterschlagung" begehen. Rechtspolitisch ist das kurios, weil diese Fallgruppen die Debatte um die Datenhehlerei erst ausgelöst haben.

[29] BT-Drs. 17/14362, S. 13.
[30] BR-Drs. 70/14.
[31] BT-Drs. 18/5088, S. 46 f.
[32] BT-Drs. 18/5088, S. 48.
[33] BT-Drs. 18/5088, S. 26.
[34] BT-Drs. 18/5088, S. 26.
[35] BT-Drs. 18/5088, S. 45.
[36] BT-Drs. 18/5088, S. 45 f.
[37] BT-Drs. 18/5088, S. 46.
[38] BT-Drs. 18/5088, S. 46.
[39] BT-Drs. 18/5088, S. 46.
[40] BT-Drs. 18/5088, S. 46.
[41] BT-Drs. 18/5088, S. 46.
[42] BT-Drs. 18/5088, S. 26.

Wie bei der Sachhehlerei müsse der Datenhehler mit dem Vortäter einvernehmlich zusammenwirken. Wie bei der Sachhehlerei scheide eine Straftat aus, „wenn der durch die Vortat verletzte Berechtigte die ihm gestohlenen Daten zurückkauft", wohingegen der bloß datenschutzrechtliche Betroffene sich strafbar mache.[43]

IV. Kritik

Dieser Überblick über die Tatbestandsstruktur dürfte deutlich gemacht haben, dass § 202d StGB eine Reihe von Fragen aufwirft. Auf die am grundlegendsten erscheinenden sei hier eingegangen.

1. Falsche Verallgemeinerungen und imaginäre Rechte: „Formelles Datengeheimnis" und „Recht am gedanklichen Inhalt"?

In gleicher Weise wie es bei den §§ 202a, 202b und §§ 303a, 303b StGB schon seit bald 30 Jahren moniert wird,[44] ist auch das Schutzgut des § 202d StGB problematisch. Für gewöhnlich knüpft das Strafrecht, wenn es wie hier um Individualinteressen geht, an Rechtspositionen wie Leben, Gesundheit, Vermögen, Eigentum an, die in den anderen Teilen der Rechtsordnung, vor allem im Zivilrecht, konturiert werden. Eigentum und Besitz sind die klassischen subjektiven Rechte, die an körperlichen Gegenständen bestehen können und einem Rechtsträger definierte Befugnisse im Umgang mit den Rechtsobjekten zuweisen. Die Verletzung dieser Berechtigungen durch Beschädigung oder Entziehung lösen Schadensersatz- und Rückgewähransprüche aus und das Strafrecht verstärkt die zivilrechtlichen Verbote durch die Sanktionsdrohung für Sachbeschädigung, Unterschlagung, Diebstahl und Hehlerei.

Für beliebige Daten, also codierte Informationen, gibt es, ungeachtet einzelner Vorschläge im Schrifttum,[45] bislang[46] keine entsprechenden zivilrechtlichen oder sonstigen Regeln, die einem Rechtsträger bestimmte Befugnisse zuweisen.

Für bestimmte Arten von Informationen gibt freilich es seit langem rechtliche Regelungen, die Schutz und auch Strafe vorsehen, nämlich

a) für Geheimnisse verschiedener Art, d.h. Informationen, die nur einem beschränkten Personenkreis zugänglich sein sollen. Hierzu zählen Staats- und sonstige Dienstgeheimnisse, private Geheimnisse als Ausprägung des allgemeinen Persönlichkeitsrechts, dem auch die Kommunikationsgeheimnisse sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[47] entspringen, sowie Betriebs- und Geschäftsgeheimnisse, die das Recht gegen den unlauteren Wettbewerb auch mit Strafnormen schützt (vgl. § 17 Abs. 2 Nr. 2 UWG zur „Geheimnishehlerei");

b) für das sog. „geistige Eigentum", also Informationen, die die Kriterien des Urheberrechts, Patent-, Marken-, Gebrauchs- oder Geschmacksmusterrechts erfüllen und dann dessen auch strafrechtlichen Schutz genießen;

c) schließlich für personenbezogene Daten, deren Regulierung in Fortentwicklung des allgemeinen Persönlichkeitsrechts zum Grundrecht auf informationelle Selbstbestimmung Gegenstand des Datenschutzrechts ist (§§ 43, 44 BDSG[48]).

Alle sonstigen Informationen sind allenfalls mittelbar geschützt, zumeist durch das Eigentum am Informationsträger, die vertrauliche Art der Übermittlung usw. Wenn jemand die Geheimzahl seiner Bankkarte auf einen Zettel schreibt, den er in seiner Schreibtischschublade aufbewahrt, so ist diese Information nur dadurch geschützt, dass sein Zettel nicht weggenommen oder zerstört werden darf und dass das Hausrecht verhindert, dass interessierte Personen des Zettels ansichtig werden.

Es ist zwar möglich, dass die Tatobjekte des § 202d StGB auch in eine der genannten drei Kategorien geschützter Informationen fallen, insbesondere personenbezogene Daten i.S.d. § 3 Abs. 1 BDSG darstellen, nötig ist das aber nicht. Vielmehr erfasst der Tatbestand jede beliebige Information, sofern sie nur weder unmittelbar wahrnehmbar noch allgemein zugänglich ist, also die digitale Einkaufliste ebenso wie die Datei mit den Wetteraufzeichnungen eines Hobbymeteorologen. Die noch im Bundesratsentwurf behauptete Fundierung durch das Grundrecht auf informationelle Selbstbestimmung bzw. das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[49] hat der Regierungsentwurf aufgegeben.

---

[43] BT-Drs. 18/5088, S. 47; krit. *Franck*, RDV 2015, 180 (182: „völlig irregeleitet").

[44] Siehe nur *Graf* (Fn. 24), § 202a Rn. 2; *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 3, 4. Aufl. 2013, § 303a Rn. 4 ff. m.w.N.

[45] Ein „Dateneigentum" schlägt *Hoeren*, MMR 2013, 486, vor, der an § 303a StGB anknüpft, womit die Suche nach den Primärnormen in einen Zirkel gerät. *Zech*, CR 2015, 137 (143), billigt dem Strafrecht beim Schutz von Daten zwar eine „echte Pionierfunktion" zu, sieht aber, dass das „entscheidende Problem, wem die entsprechenden Handlungsbefugnisse zugewiesen sein sollen", auch im StGB unbeantwortet bleibt.

[46] Es besteht in der Industrie ein erhebliches Interesse an quasi-dinglichen Nutzungsrechten („data ownership") am „neuen Gold" oder „neuen Öl" der Anwenderdaten, so dass langfristig der wirtschaftliche Wert von „Big Data" ein solches Primärnormengefüge entstehen lassen könnte. Zu den konzeptionellen Ansätzen in der aktuellen Diskussion siehe neben den in Fn. 45 Genannten noch *Dorner*, CR 2014, 617; *Zech*, GRUR 2015, 1151; *Schwartmann/Hentsch*, RDV 2015, 221; *Heun/Assion*, CR 2015, 812; *Sahl*, RDV 2015, 236; *Hornung/Goeble*, CR 2015, 265; *Hofmann*, JurPC Web-Dok. 158/2015; siehe auch OLG Celle NJW-RR 2011, 1047 f.; OLG Naumburg VRS 2014, 174 m. Anm. *Assion*, CR 2016, 84 f.

[47] BVerfGE 120, 274.

[48] Zur problematischen Fassung der Tatbestände siehe *Golla*, ZIS 2016, 192 (193 ff.).

[49] BR-Drs. 284/13, S. 6 f., 14 f.; zu Recht kritisch *Golla/v. zur Mühlen*, JZ 2014, 668 (670).

Das Problem, dass es keine generelle primäre Normenordnung des Umgangs mit beliebigen „Informationen“ gibt, die einen dem Sacheigentum entsprechenden Zuweisungsgehalt hätte, plagt die Vorschriften über die Computerkriminalität seit ihrer Einführung 1986, namentlich die Datenveränderung des § 303a StGB, die deshalb von manchen Autoren wegen Unbestimmtheit für verfassungswidrig gehalten wird.[50] Während der Bundesratsentwurf mit der Leerformel, an der Nichtverwendung der Daten müsse ein „schutzwürdiges Interesse“ bestehen, versucht hat, das Problem auf den Rechtsanwender abzuwälzen, hat sich der Gesetzgeber die Verlegenheitslösung der herrschenden Meinung zu eigen gemacht, wenn er das „formelle Datengeheimnis“ als Schutzgut ansieht.

„Formell“ heißt dieses Datengeheimnis, weil es auf den Inhalt der Informationen nicht ankommt. Dieses angebliche Rechtsgut ist ein merkwürdiges Ding, denn es existiert offenbar nur im Strafrecht, und soll auf einem „Recht an dem gedanklichen Inhalt“ einer Information beruhen, das im „Interesse an der Aufrechterhaltung des Herrschaftsverhältnisses über eine Information“ zur Entscheidung über die Weitergabe und Übermittlung der Daten befugt.[51] „Recht am gedanklichen Inhalt“ klingt nach einer Art geistigen Eigentums, das aber offenbar an jeder beliebigen Information begründet werden kann.

Noch merkwürdiger wird es, wenn man liest, wie ein solches – um den von *Amelung* in anderem Kontext geprägten Ausdruck[52] zu entleihen – Informationsbeherrschungsrecht entstehen soll, nämlich dadurch, dass man Daten sammelt und speichert oder speichern lässt. Diese von *Welp* begründete Skripturakttheorie[53] erinnert an *Lockes* Arbeitstheorie des Eigentumserwerbs:[54] Indem man etwas mit einer Information macht, sie speichert, gewinnt man das Recht an ihr. Das kann nicht ernstlich so gemeint sein wie es formuliert ist: Wenn jemand in sein Notebook hineintippt und speichert, dass am Ostersonntag, dem 27.3.2016, in Bonn eine Temperatur von 12 Grad herrschte und der Himmel grau war, gewönne er dann die rechtliche Herrschaft über diesen gedanklichen Inhalt? Aber was soll „rechtliche Herrschaft“ heißen? Dass sonst danach niemand mehr diesen Satz über das Bonner Wetter sagen oder speichern darf? Wenn es doch jemand tut, könnte er das gerichtlich nach § 1004 BGB untersagen lassen und gem. § 823 BGB Schadensersatz verlangen? Von einem „Recht am gedanklichen Inhalt“ im Wortsinne, d.h. mit Zuweisungsgehalt und Ausschlussfunktion, kann offensichtlich nicht die Rede sein, es sei denn der Gesetzgeber wollte en passant ein neues Immaterialgüterrecht[55] erschaffen, das im Rechtsverkehr einiges Chaos anrichten dürfte. Verwechselt wird hier der semantische Gehalt der ortlosen Information mit ihrer physikalischen Existenz als syntaktische Codierung[56] in bestimmter Hardware. In §§ 202a ff., 303a ff. StGB geht es nicht um die Information als solche, egal, wo und wie sie gespeichert ist, sondern darum, dass bestimmte physikalisch realisierte Informationen, die bestimmten Personen zwar bislang ohne klaren Rechtsgrund, aber jedenfalls in oft im Ergebnis einsehbarer Weise[57] zugeordnet werden, unbefugt aus Hardware oder Transmissionen extrahiert oder darin verändert werden.

Wenn es wirklich um ein Recht am gedanklichen Inhalt ginge, wäre es zudem nicht schlüssig, nur nicht unmittelbar wahrnehmbare Verkörperungen dieses Inhalts zu schützen.[58] Derjenige, der neugierig auf den Zettel mit der Geheimzahl starrt, den der Bankkunde leichtsinnigerweise in der Hand hält, während er die Zahlen gerade in die Tastatur des Bankautomaten eingibt, würde dieses Recht ebenso verletzen. Ein solches „Recht am gedanklichen Inhalt“ beliebiger Informationen gibt es bisher indes nicht. Ein Interesse an der Herrschaft über beliebige Daten, also verkörperte Informationen, mag gewiss bestehen, Interessen begründen aber nicht ohne weiteres auch subjektive Rechte. Eine „formelle Verfügungsbefugnis“ über selbst gespeicherte Informationen hängt ebenso in der Luft; was es stattdessen gibt, ist die aus dem Eigentumsrecht folgende Befugnis zum Umgang mit dem informationsverarbeitenden Gerät.

2. Falsche Analogien: Die „formelle Verfügungsbefugnis“ als Quasi-Besitz?

Die Vorschrift krankt weiterhin am unsachgemäßen und notgedrungen zum Scheitern verurteilten Versuch einer Parallelisierung zur Sachhehlerei. Dabei erfüllt die mit dem formellen Datengeheimnis einhergehende formelle Verfügungsbefugnis des Berechtigten über die von ihm gespeicherten Daten in der Gesetzesbegründung eine analoge Funktion wie der Besitz bei den Zueignungsdelikten. So wie das Unrecht der Sachhehlerei in der Perpetuierung der durch die

[50] *Tolksdorf*, in: Jähnke/Laufhütte/Odersky (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 8, 11. Aufl. 2005, § 303a Rn. 7 m.w.N.; *Zaczyk* (Fn. 44), § 303a Rn. 4 f., § 303b Rn. 1.

[51] BT-Drs. 18/5088, S. 26 im Anschluss an *Graf* (Fn. 24), § 202a Rn. 2; siehe ferner nur *Lenckner/Eisele*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 29. Aufl. 2014, § 202a Rn. 1; *Heger*, in: Lackner/Kühl, Strafgesetzbuch, Kommentar, 28. Aufl. 2014, § 202a Rn. 1, jeweils m.w.N.

[52] *Amelung*, Informationsbeherrschungsrechte im Strafprozeß: dogmatische Grundlagen individualrechtlicher Beweisverbote, 1990.

[53] *Welp*, iur 1988, 443 (447); siehe auch *Hilgendorf* (Fn. 6), § 202a Rn. 26; *Stree/Hecker*, in: Schönke/Schröder (Fn. 51), § 303a Rn. 3, jeweils m.w.N.; dem folgend BayObLGSt 1993, 86 (89) m. Anm. *Hilgendorf*, JR 1994, 478; OLG Naumburg VRS 2014, 174 (176 f.).

[54] *Locke*, Two Treatises of Government, 1698, II § 27 f.

[55] Vgl. *Sieber* (Fn. 19), C 151, 153, der von „neuen immateriellen Rechtsobjekten“ spricht, ohne diese näher zu bestimmen, dagegen zu Recht skeptisch *Hilgendorf*, JZ 2012, 825 (831).

[56] Zur Unterscheidung von semantischer und syntaktischer Ebene und zum Begriff der Codierung siehe nur *Zech*, Information als Schutzgegenstand, 2012, S. 35 ff.

[57] Vgl. die Fallgruppen bei *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 63. Aufl. 2016, § 303a Rn. 5 ff.

[58] Vgl. Gesetzesantrag des Landes Hessen (Fn. 20), S. 9; so schon wortgleich BT-Drs. 17/14362, S. 11.

Vortat geschaffenen widerrechtlichen Besitzlage gesehen wird,[59] soll die Datenhehlerei die durch die Vortat begangene Verletzung der formellen Verfügungsbefugnis aufrechterhalten und vertiefen.[60]

Die Analogie funktioniert indessen nicht:[61] Körperliche Gegenstände sind dem Berechtigten, der ein Recht auf Rückgabe hat, womöglich auf Dauer entzogen, wenn sie verhehlt werden. Daten erlangt man dadurch, dass man sie kopiert.[62] Trotz der Ausspähung hat der Berechtigte seine Daten in aller Regel – wenn nicht noch eine Datenveränderung hinzutritt – noch und kann sie weiter nutzen.[63] Im Gegensatz zu Sachen sind Daten also „nicht-rivalisierende" Güter, d.h. wegen der beliebigen Kopierbarkeit ist ihre tatsächliche Nutzerzahl nicht oder weniger[64] begrenzt, überdies nutzen sie sich im Gegensatz zu Sachen auch nicht ab.[65] Es geht somit weder um Enteignung noch um Erschwerung oder Vereitelung eines Restitutionsrechts, auch wenn die Gesetzesbegründung das andeutet, denn wie sollte so eine „Datenrückgabe" zur Wiedererlangung der „alleinigen Verfügungsbefugnis" aussehen? Sachen kann man zurückgeben, Informationen kaum. Soll der Datendieb versprechen, die fremden Kontodaten auf seinem Rechner und aus seinem Gedächtnis zu löschen? Lebensfremd wirkt daher das in der Gesetzesbegründung angesprochene Szenario, dass der Berechtigte straflos sei, wenn er seine Daten vom Dieb zurückkaufe.

Tatsächlich ist das „formelle Datengeheimnis" verloren, wenn Unbefugte Kenntnis von den Daten erlangt haben. Ein gelüftetes Geheimnis ist kein Geheimnis mehr. Wiederherstellen kann man ein Geheimnis – die tatsächliche Exklusivität der Datennutzung – nur, indem die Zahl der unbefugt Wissenden auf null zurückgeführt wird, was aus diversen Gründen offensichtlich ausscheidet. Anders als die Gesetzesbegründung meint, hilft hier auch keine Rückgabe mehr, sondern nur noch die Ersetzung des verratenen Geheimnisses durch ein neues, nämlich durch Änderung der Passwörter etc.

Wenn man Datenhehlerei schon als Verschiebungsdelikt konzipiert, so geht die Parallele an anderer Stelle nicht weit genug: Unterschlagung ist taugliche Vortat der Sachhehlerei, aber unbefugte Weitergabe von Daten durch Zugriffsberechtigte soll für Datenhehlerei nicht genügen – das liegt freilich daran, dass man für Daten noch kein Pendant zum bei der Unterschlagung verletzten dinglichen Recht des Eigentums gefunden hat und „bloße" Pflichtwidrigkeit nicht genügen lassen will, was durchaus zweifelhaft erscheint.

3. Abstrakte Gefährdung statt Perpetuierung

Schließlich erscheint die Einstufung des Datenhandels als Perpetuierungsunrecht noch aus einem weiteren Grunde verfehlt im Hinblick auf die Fallgruppe, die Anlass zum Bundesratsentwurf gab, also den Handel mit digitalen Identitäten, insbesondere Zugangsdaten. Diese Daten haben als Handelsware nur einen einzigen und zwar kriminellen Verwendungszweck,[66] aus dem sich ihr wirtschaftlicher Wert ergibt, nämlich die Möglichkeit, finanzielle Transaktionen durchzuführen oder sich sonst interessante Daten zu verschaffen, um Straftaten nach §§ 202a ff., 263a, 269 usw. StGB zu begehen. Es handelt sich bei den fraglichen Datensätzen also um potentielle Tatwerkzeuge, Tatmittel, vergleichbar gestohlenen oder kopierten Tresor-, Haus- und Wohnungsschlüsseln. Die Sozialschädlichkeit des Handels damit liegt nicht darin, dass man den Berechtigten etwas vorenthält, sondern dass man deren künftige Schädigung ermöglicht. Die einschlägige Norm ist daher § 202c StGB, dessen Tathandlungen ja auch in § 202d stecken, der jedoch die zwei benannten Mängel aufweist, nämlich einmal die Unklarheit, ob es sich um die Vorbereitung konkreter Taten oder um ein abstraktes Gefährdungsdelikt handelt,[67] und zum zweiten die Beschränkung auf die Vorbereitung oder Gefahr lediglich von Taten nach §§ 202a und 202b StGB.

Es hätte demnach genügt, den § 202c StGB zu erweitern, indem man den Bezug auf bestimmte Durchführungstaten streicht. Die praktische Relevanz dieses Tatbestands bleibt freilich genauso zweifelhaft wie die des § 202d, denn oft sind die Datenhändler unbekannt oder sitzen für deutsche Strafverfolgungsbehörden kaum erreichbar im Ausland. Relevanter dürfte sein, dass ein Tatverdacht nach § 202d Ermittlungsmaßnahmen einschließlich der Telekommunikationsüberwachung erlaubt.

Eine Änderung des § 202c StGB reicht natürlich nicht aus, wenn man „Datenhehlerei" aller Art bestrafen will. Welche Verhaltensweisen der Gesetzgeber aber sonst noch im Auge hatte, bleibt unklar, da der Regierungsentwurf dazu nichts sagt. Insoweit fehlt es jedenfalls an der „empirischen Analyse der Rechtswirklichkeit"[68] als Voraussetzung jeglicher rationaler Kriminalpolitik.

V. Fazit

Die Datenhehlerei soll insbesondere ein Phänomen erfassen, das durchaus als strafwürdig durchgehen mag, nämlich den Handel mit unbefugt erlangten Zugangsdaten, deren einzige Verwendungsmöglichkeit die Begehung weiterer Computerstraftaten ist. Dazu hätte eine Erweiterung des § 202c StGB

[59] BT-Drs. 7/550, S. 252; weitere Nachweise bei *Altenhain*, in: Kindhäuser/Neumann/Paeffgen (Fn. 44), § 259 Rn. 3.
[60] Oben bei Fn. 33.
[61] Siehe auch *Golla/v. zur Mühlen*, JZ 2014, 668 (671); *Singelnstein*, ZIS 2016, 432 (433, 434 f.).
[62] Eine echte „Übertragung" von Daten im Sinne einer Ortsverschiebung von Objekten gibt es nicht, es gibt nur Kopiervorgänge, *Hoppen*, CR 2015, 802 (803).
[63] So auch BT-Drs. 17/14362, S. 12; BT-Drs. 18/5088, S. 27.
[64] Es kommt natürlich auf die konkreten Zugriffs- und Nutzungsformen an, etwa beim gleichzeitigen Zugriff auf eine Online-Publikation, vgl. *Schwartmann/Hentsch*, RDV 2015, 221 (225), jedenfalls ist die Rivalität von Daten typischerweise deutlich geringer als die körperlicher Gegenstände.
[65] Zur Begrifflichkeit *Zech*, CR 2015, 137 (139); *Schwartmann/Hentsch*, RDV 2015, 221 (224 f.).
[66] Zutreffend Gesetzesantrag des Landes Hessen (Fn. 20), S. 12.
[67] Dazu *Borges/Stuckenberg/Wegener*, DuD 2007, 275 (276); *Stuckenberg*, wistra 2010, 41 (45 m.w.N.).
[68] Vgl. *Sieber* (Fn. 19), C 18.

zu einem abstrakten Gefährdungsdelikt genügt, das die Weitergabe von zu Gefahrgut gewordenen Datensätzen bestraft. Dann hätten sich auch die misslichen Folgeprobleme des Abs. 3 erübrigt.

Stattdessen wird § 202d StGB in Analogie zur Sachhehlerei zu Unrecht als Perpetuierungsdelikt verstanden, das an den Strafrahmen der Vortat angebunden wird, obwohl dem Opfer hier nichts vorenthalten wird, was es wiedererlangen könnte. Der Tatbestand perpetuiert hingegen das vom 2. WiKG geschaffene Problem der Unbestimmtheit des Schutzguts der Computerdelikte, weil der Gesetzgeber über die klare Fallgruppe der Zugangsdaten hinaus beliebige Daten als Tatobjekte erfassen will, obschon es immer noch keine primäre Normenordnung des allgemein erlaubten und verbotenen Umgangs mit Daten gibt. Das vom Gesetzgeber ersatzweise herangezogene „formelle Datengeheimnis“ aufgrund eines durch Speicherung erworbenen „Rechts am gedanklichen Inhalt einer Information“ ist nicht konsistent als subjektive Rechtsposition darstellbar.