Ausufernd und fehlplatziert: Der Tatbestand der Datenhehlerei (§ 202d StGB) im System des strafrechtlichen Daten- und Informationsschutzes

Von Prof. Dr. **Tobias Singelnstein**, Berlin

Am 18. Dezember 2015 ist mit dem § 202d StGB der Tatbestand der Datenhehlerei in Kraft getreten.[1] *Damit schlägt der Gesetzgeber ein weiteres Kapitel in der Geschichte des strafrechtlichen Schutzes von Daten und Informationen auf – ohne diesen Bereich jedoch systematisch überzeugend in den Griff zu bekommen. Dieser Beitrag darüber sei der ZIS, ihren Herausgebern und der Redaktion mit den besten Glückwünschen zum 10jährigen Jubiläum gewidmet!*

I. Einführung

§ 202d Abs. 1 StGB erfasst – wie bereits der Titel „Datenhehlerei" nahelegt – den Umgang mit Daten, die ein Dritter durch eine rechtswidrige Tat erlangt hat. Damit reagiert der Gesetzgeber auf Entwicklungen im Bereich der Cyberkriminalität, dem allgemein eine stark zunehmende Bedeutung beigemessen wird. Eine wesentliche Rolle spielt dabei die (massenhafte) rechtswidrige Erlangung von Identitätsdaten, die sodann für Vermögensdelikte missbraucht werden.[2] Beispielhaft für diese Form der Cyberkriminalität sind das so genannte Phishing zur Erlangung von Konto- und Kreditkartendaten oder das Eindringen in entsprechende Datenspeicher.

Nach kriminologischen Erkenntnissen werden solche Taten nicht selten von verschiedenen Personen begangen. Zunächst macht sich ein technisch versierter Täter an die Beschaffung der Daten, verwendet diese aber nicht selbst, sondern veräußert sie weiter an andere Personen, die damit sodann die genannten Vermögensdelikte begehen oder die Daten weiterverkaufen.[3] Angesichts dessen sah sich der Gesetzgeber veranlasst, vor allem die zwischen der Beschaffung der Daten und ihrem Einsatz für weitere Delikte liegende Veräußerung gesondert unter Strafe zu stellen – auch und gerade, um Beweisproblemen zu begegnen.[4]

> *Fall 1*: T dringt über eine Telekommunikationsverbindung in den geschützten Datenserver des Unternehmens U ein und beschafft sich so die Identitäts- und Kreditkartendaten einer unbestimmten Zahl von Kunden des U. Anschließend verkauft und übermittelt er die Daten auf dem Schwarzmarkt an H, der diese zur Begehung von Vermögensdelikten verwenden möchte.

Der Gesetzgeber hat die neue Norm hinter den §§ 202a 202c StGB in den Abschnitt über die Verletzung des persönlichen Lebens- und Geheimbereichs eingefügt. Er macht damit deutlich, dass das Schutzgut des Tatbestandes nicht anders als beim Ausspähen und Abfangen von Daten im formellen Geheimhaltungsinteresse des Verfügungsberechtigten[5] sowie dessen Verfügungsbefugnis hinsichtlich der Daten zu sehen sein soll.[6]

II. Struktur und Merkmale des Tatbestandes

Den beabsichtigten Schutz setzt der Tatbestand mit zwei objektiven Merkmalen und – neben dem Vorsatz – einem besonderen subjektiven Merkmal um. Er ist damit jedenfalls von seiner Konstruktion her eng an die Sachhehlerei in § 259 StGB angelehnt. Tatobjekt sind alle Daten im Sinne der Legaldefinition des § 202a Abs. 2 StGB, also all solche Daten, die elektronisch oder magnetisch gespeichert sind oder übermittelt werden.[7] Damit gewährt der Tatbestand – wie schon die voranstehenden Normen der §§ 202a ff. StGB – einen sehr weitgehenden Schutz. Insbesondere findet keine Beschränkung auf besonders sensible oder wertvolle Inhalte statt, wie dies etwa die Tatbestände des Geheimnisschutzes tun.

Vielmehr nimmt § 202d Abs. 1 StGB hinsichtlich des Tatobjekts lediglich zwei Einschränkungen vor, die in der Natur der Sache liegen. Erstens dürfen die Daten nicht öffentlich zugänglich, also nicht über allgemein zugängliche zuverlässige Quellen zu erlangen sein,[8] da es in diesem Fall stets an der Strafwürdigkeit fehlt.[9] Zweitens muss ein anderer die Daten durch eine rechtswidrige Tat (§ 11 Abs. 1 Nr. 5 StGB) erlangt haben, was gerade das Wesen der Datenhehlerei als Anschlussdelikt ausmacht. Neben dem Ausspähen und Abfangen von Daten (§§ 202a, 202b StGB) sollen als Vortat auch allgemeine Delikte in Betracht kommen, wie der Diebstahl (§ 242 StGB) von Datenträgern oder die Nötigung

[1] BGBl. I 2015, S. 2227; dazu *Roßnagel*, NJW 2016, 533 (537).

[2] *Gercke*, ZUM 2013, 605 f.; *Hahn/Bußmann*, DRiZ 2012, 223; *Meier*, MschrKrim 2012, 184.

[3] *Bär*, DRiZ 2015, 432; *Sieber*, Gutachten C zum 69. Deutschen Juristentag, 2012, S. 22.

[4] BT-Drs. 18/5088, S. 24 ff.; *Hahn/Bußmann*, DRiZ 2012, 223 (223 f.); kritisch zum praktischen Bedarf etwa *Selz*, in: Taeger (Hrsg.), Internet der Dinge. Digitalisierung von Wirtschaft und Gesellschaft. Tagungsband DSRI-Herbstakademie, 2015, S. 915-931, 917 ff.

[5] Zum Berechtigtenbegriff BT-Drs. 18/5088, S. 46; *Neuhöfer*, jurisPR-Compl 4/2015, Anm. 6.

[6] BT-Drs. 18/5088, S. 26, 45; *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 28. Aufl. 2014, § 202a Rn. 1; *Weidemann*, in: v. Heintschel-Heinegg (Hrsg.), Beck'scher Online-Kommentar, Strafgesetzbuch, Stand: März 2016, § 202a Rn. 2.

[7] Dazu detailliert *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 6, 12. Aufl. 2009, § 202a Rn. 7 ff.

[8] BT-Drs. 18/5088, S. 45 f.; siehe auch § 10 Abs. 5 S. 2 BDSG; BGHSt 58, 268 (277); OLG Bamberg NStZ-RR 2011, 27; *Ambs*, in: Erbs/Kohlhaas (Hrsg.), Strafrechtliche Nebengesetze, 206. Lfg., Stand: Januar 2016, § 43 BDSG Rn. 17.

[9] *Neuhöfer*, jurisPR-Compl 4/2015, Anm. 6.

(§ 240 StGB).[10] Die Vortat muss – ebenso wie bei der Sachhehlerei – vollendet sein und tatsächlich die formelle Verfügungsbefugnis des Berechtigten beeinträchtigt haben, was im Einzelfall die genaue Bestimmung der Person des Berechtigten erforderlich macht.[11]

Als Tathandlung benennt der § 202d Abs. 1 StGB das Sichverschaffen sowie das Verschaffen oder Zugänglichmachen für einen Anderen und greift damit Teile der von § 202c Abs. 1 StGB erfassten Handlungen auf.[12] Ähnlich wie die Sachhehlerei erfasst damit auch die Datenhehlerei sehr umfassend die im Anschluss an eine Vortat in Betracht kommenden Handlungsweisen, vom eigenen Verschaffen bis hin zu allen Formen der Weitergabe an Dritte. Aus datenschutzrechtlicher Sicht sind damit alle Formen der Übermittlung der Daten an Dritte erfasst, aber auch solche eigenen Nutzungen der Daten, bei denen Dritte notwendig Kenntnis erlangen. Der Täter muss dabei die tatsächliche Verfügungsmacht über die Daten erlangen.[13]

Subjektiv verlangt der Tatbestand neben dem Eventualvorsatz, der die Vortat umfassen muss,[14] eine Bereicherungs- oder Schädigungsabsicht. Dies entspricht der parallelen Qualifikationsregelung für die Verletzung von Privatgeheimnissen in § 203 Abs. 5 StGB, für die nach richtiger Auffassung dolus directus 1. Grades zu verlangen ist.[15]

Zusammengenommen weist der Tatbestand des § 202d Abs. 1 StGB damit sowohl ein sehr breit formuliertes Tatobjekt, als auch sehr umfangreiche Tathandlungen auf. Eingrenzungen der Strafbarkeit werden vor allem durch zwei Merkmale umgesetzt: die Herkunft der Daten aus einer rechtswidrigen Vortat und das Erfordernis einer besonderen Absicht als überschießender Innentendenz. Erfasst sein können daher etwa auch die folgenden Fallkonstellationen:

> *Fall 2*: Der in einem Ministerium tätige Beamte B ist über die rechtswidrigen Praktiken mancher seiner Kollegen empört. Um Abhilfe zu schaffen, spielt er einschlägige geheime Daten dem Aktivisten A zu. Dieser geht damit zu dem Journalisten J und kopiert diesem die Daten, damit J daraus eine große Geschichte machen kann.
>
> *Fall 3*: O verliert seinen USB-Stick. Dies bemerkt T, der den Stick an sich nimmt, um ihn für sich zu behalten. Das auf dem Stick gespeicherte Spezialrezept für Omas Apfelkuchen, das O längst vergessen hatte, verkauft T für € 5,- an den Bäcker B, der mit dem leckeren Gebäck seinen Umsatz steigern möchte.

[10] BT-Drs. 18/5088, S. 46; *Golla/v. zur Mühlen*, JZ 2014, 668 (669); kritisch zu Delikten, die sich nicht (primär) auf die formelle Verfügungsbefugnis beziehen, *Selz* (Fn. 4), S. 926 f.
[11] *Neuhöfer*, jurisPR-Compl 4/2015, Anm. 6; dazu *Hilgendorf* (Fn. 7), § 202a Rn. 26 f.
[12] BT-Drs. 18/5088, S. 46 f.; *Franck*, RDV 2015, 180 (181).
[13] BT-Drs. 18/5088, S. 47.
[14] Vgl. zu den Anforderungen *Stree/Hecker*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 29. Aufl. 2014, § 259 Rn. 39.
[15] *Lackner/Kühl* (Fn. 6), § 203 Rn. 28.

III. § 202d StGB im System des strafrechtlichen Informationsschutzes

Daten und die in ihnen enthaltenen Informationen stellen für den Gesetzgeber ein Schutzgut dar, das offenbar schwer zu handhaben ist.[16] Im Schlepptau des technischen Fortschritts wurden zahlreiche verschiedene Tatbestände geschaffen, die zusammengenommen eher einen schwer überschaubaren Flickenteppich darstellen, als einem systematischen und schlüssigen Gesamtkonzept zu folgen. Wie ist der neue Tatbestand der Datenhehlerei in diesem Feld zu verorten?

1. Daten und Sachen

Daten und die in ihnen enthaltenen Informationen unterscheiden sich grundlegend von Sachen bzw. Eigentum und Gewahrsam als strafrechtlichem Schutzgut. Dies hängt insbesondere mit der fehlenden Verkörperung zusammen. Anders als Sachen sind Daten keine Einzelstücke und nicht fest lokalisiert. Sie lassen sich vielmehr perfekt kopieren und insofern beliebig vervielfältigen sowie sehr einfach auch über weite Strecken transferieren.[17] Dies führt zu divergierenden Schutzbedürfnissen für Eigentum und Gewahrsam an Sachen auf der einen Seite sowie Daten und Informationen auf der anderen Seite. Für den Eigentümer bzw. Gewahrsamsinhaber kommt es vor allem darauf an, dass die Sache unversehrt ist und ihm nach seinem Belieben zur Verfügung steht. Dies beides trifft zwar auch auf Informationen und Daten zu – allerdings in deutlich anderer Weise.

Erstens kann eine Sache in ihrer Verkörperung grundsätzlich nur einer Person zum gleichen Zeitpunkt zur Verfügung stehen. So kann etwa ein Mantel nur von einer Person getragen werden. Seine Wegnahme schließt daher den Eigentümer bzw. Gewahrsamsinhaber von der Nutzung aus. Daten hingegen können kopiert und anschließend zeitgleich von verschiedenen Personen genutzt werden.[18] Eine illegale Beschaffung von Daten schließt den Berechtigten daher nicht von der Nutzung aus, wenngleich er aus anderen Gründen schutzwürdig sein mag, womit der zweite wesentliche Unterschied angesprochen ist: Bei Sachen ist es dem Berechtigten für gewöhnlich egal, ob Dritte Kenntnis von seinem Besitz oder Eigentum und der Beschaffenheit der Sache haben. Anders ist es hingegen häufig bei Daten. Hier kommt es dem Berechtigten nicht selten darauf an, dass nur er Kenntnis oder Zugriff auf die in den Daten enthaltenen Inhalte hat. Dies gilt für Privat- und Geschäftsgeheimnisse ebenso wie für Passwörter und vergleichbare Zugangsdaten. Patientenkarteien, das private Tagebuch, das noch unveröffentlichte Gedicht eines Autors oder das Passwort für den Zugang zum privaten E-Mail-Account sind also insofern schützenswert, als nur der Berechtigte Kenntnis von diesen Informationen haben sollte. Dies gilt sowohl für Zugangsdaten, die einen erst dahinterstehenden Datenbestand schützen, als auch für Daten, die bereits wegen ihres eigenen Inhalts schützenswert sind, also etwa Privat- und Geschäftsgeheimnisse.

[16] Dazu allgemein *Golla*, ZIS 2016, 192 (192 ff.)
[17] *Golla/v. zur Mühlen*, JZ 2014, 668 (671).
[18] *Golla/v. zur Mühlen*, JZ 2014, 668 (671).

Kurz gesprochen lässt sich sagen: Was der Sache ihre Verkörperung ist, auf die der Berechtigte nach seinem Belieben Zugriff hat, ist den Daten ihr Inhalt, der je nach den Umständen nur einem begrenzten Personenkreis bekannt ist.

2. Konzepte des strafrechtlichen Daten- und Informationsschutzes

Bei der normativen Erfassung der damit skizzierten Schutzbedürfnisse hat der Gesetzgeber in der Vergangenheit verschiedene Konzepte verfolgt, die sich grundlegend in zwei Richtungen unterscheiden lassen.[19]

Auf der einen Seite finden sich zahlreiche Tatbestände, die jeweils besonders sensible und daher besonders schutzbedürftige Informationen betreffen, die zumindest auch in Form von Daten vorliegen können.[20] Dies gilt für Privatgeheimnisse und den höchstpersönlichen Lebensbereich, die durch die §§ 201, 201a, 202, 203, 204 StGB geschützt werden. Der Schutz von Dienst- und Geschäftsgeheimnissen ist in § 17 UWG sowie den §§ 203, 353b StGB geregelt. Ein Schutz personenbezogener Daten findet sich in § 44 BDSG und parallelen Vorschriften in den Landesdatenschutzgesetzen. Bei diesen Tatbeständen lässt sich von einem inhaltsbezogenen Schutzkonzept für Daten bzw. Informationen sprechen.

Auf der anderen Seite schützen bestimmte Tatbestände gespeicherte oder in Übermittlung befindliche Daten und Datenverarbeitungen unabhängig von ihrem Inhalt vor bestimmten Einwirkungen, so dass sich von einem formalen Schutzkonzept von Daten sprechen lässt. Dies gilt für die §§ 303a, 303b StGB, die die Veränderung und Beseitigung von Daten betreffen, sowie für die §§ 202a, 202b und 202c StGB, die die Verschaffung von besonders gesicherten oder in Übermittlung befindlichen Daten erfassen. Aber auch der neue § 202d StGB ist nach Auffassung des Gesetzgebers in diese Kategorie zu zählen. Dieses zweite Schutzkonzept, das gespeicherte Daten im Sinne des § 202a Abs. 2 StGB betrifft, ist ersichtlich an den strafrechtlichen Schutz von Sachen angelehnt. Vergleichsweise unproblematisch ist dies bei den §§ 303a, 303b StGB, die der Sachbeschädigung entsprechen[21] – denn der Berechtigte hat bei Daten nicht anders als bei Sachen ein schützenswertes Interesse daran, dass diese unversehrt erhalten bleiben. Deutlich anders stellt sich die Sachlage hingegen bei den §§ 202a ff. StGB dar. Hier wirken sich die eingangs benannten grundlegenden Unterschiede zwischen Sachen und Daten aus, die wie gezeigt zu divergierenden Schutzbedürfnissen führen. Während es bei Sachen im Wesentlichen um einen Schutz der Sachherrschaft geht, hat der Berechtigte bei Daten vor allem das Interesse, dass Dritte nicht Kenntnis vom Inhalt der Daten erlangen.

Diesen Unterschieden trägt der Gesetzgeber bei den §§ 202a, 202b StGB – die von ihrer Schutzrichtung her Diebstahl und Unterschlagung bei Sachen ähneln – zumindest noch insofern Rechnung, als der Kreis der Tathandlungen deutlich eingeschränkt ist. Beim Ausspähen von Daten (§ 202a StGB) muss der Täter eine Zugangssicherung überwinden, sind also nur besonders geschützte Daten erfasst.[22] Das Abfangen von Daten (§ 202b StGB) betrifft nur Daten, die sich in einer nichtöffentlichen Datenübermittlung befinden.[23] Hier sind die Daten also zum einen besonders schutzbedürftig, zum anderen erfordert der Zugriff einen erheblichen technischen Aufwand und somit auch besondere Tathandlungen. Wie aber fügt sich nun der neue Tatbestand des § 202d StGB in dieses Gefüge des strafrechtlichen Daten- und Informationsschutzes ein?

3. § 202d StGB als Element des formalen Schutzkonzepts

Zunächst scheint der Tatbestand tatsächlich eine relevante Lücke zu füllen, da gespeicherte Daten bislang nicht generell vor einer unbefugten Weitergabe geschützt sind.[24] In Anlehnung an die datenschutzrechtliche und verfassungsrechtliche Differenzierung zwischen Datenerhebung und Datenverarbeitung lassen sich zwei dem entsprechende Ebenen des strafrechtlichen Schutzes ausmachen: das Erheben bzw. Beschaffen und das Verarbeiten bzw. Nutzen. In diesem Sinne sind etwa Geheimnisse und andere Objekte des inhaltsbezogenen Schutzkonzeptes nicht nur vor einer unbefugten Beschaffung geschützt, sondern auch vor einer Weitergabe oder Verwendung. Ähnliches gilt für Sachen, die angesichts des § 259 StGB nicht nur vor Wegnahme und Unterschlagung, sondern ebenso vor weitergehendem Ankauf und Absetzen geschützt sind. Siehe die Tabelle auf S. 439.

Systematisch muss die Verortung der Datenhehlerei im formalen Schutzkonzept allerdings als verfehlt bezeichnet werden. Innerhalb dieses Konzepts werden gespeicherte Daten in einem formalen Sinn vor Zerstörung und Ausspähung geschützt. Im Vordergrund steht also nicht das inhaltsbezogene Interesse, dass die gespeicherten Inhalte Dritten nicht bekannt werden, sondern die Wahrung der Integrität des Datenbestandes.[25] Bei der Datenhehlerei geht es nun aber gerade um das inhaltsbezogene Interesse des Betroffenen und nicht um die im Rahmen des formalen Schutzkonzepts geschützte formale Verfügungsbefugnis des Berechtigten. Ganz streng genommen ist diese Verfügungsbefugnis der ursprünglich Berechtigten in den meisten Fällen der Datenhehlerei sogar gar nicht mehr betroffen. Es lässt sich nämlich vertreten, dass durch das Kopieren des Datenbestandes im Rahmen der Vortat – das zwar nicht immer, aber doch häufig erfolgt – ein neuer Datenbestand geschaffen wird, hinsichtlich dessen

[19] Allgemein zu den §§ 201 ff. StGB *Hoyer*, in: Wolter (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, 148. Lfg., Stand: Dezember 2014, Vor §§ 201 ff. Rn. 1 ff.; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 4. Aufl. 2013, Vor §§ 201 ff. Rn. 4 ff.

[20] *Hilgendorf*, in: Arzt/Weber/Heinrich/Hilgendorf, Strafrecht, Besonderer Teil, 3. Aufl. 2015, § 8 Rn. 24 ff., 37 ff.; *Popp*, in: Leipold/Tsambikakis/Zöller (Hrsg.), AnwaltKommentar StGB, 2. Aufl. 2015, § 203 Rn. 1 f.

[21] *Ernst*, DS 2007, 335 (338 f.); *Heinrich*, in: Arzt/Weber/Heinrich/Hilgendorf (Fn. 20), § 12 Rn. 41 ff.

[22] *Hilgendorf* (Fn. 7), § 202a Rn. 29 ff.

[23] *Bosch*, in: Satzger/Schluckebier/Widmaier (Hrsg.), Strafgesetzbuch, Kommentar, 2. Aufl. 2014, § 202b Rn. 2.

[24] *Klengel/Gans*, ZRP 2013, 16 (18).

[25] *Selz* (Fn. 4), S. 925 f.

nicht mehr der ursprünglich Berechtigte, sondern der kopierende Vortäter Verfügungsberechtigter ist.[26] Der formale Datenbestand, der als Kopie Gegenstand der Hehlerei wird, wäre danach gar nicht mehr ein solcher des Opfers der Vortat, so dass dessen Verfügungsbefugnis, die dem Gesetzgeber zufolge das Schutzgut darstellen soll, durch die Datenhehlerei gar nicht tangiert würde.[27]

Diese Befunde werden durch einen Vergleich mit der Sachhehlerei gemäß § 259 StGB untermauert, bei der der Unrechtsgehalt in der Perpetuierung der durch den Vortäter geschaffenen rechtswidrigen Vermögenslage begründet ist.[28] Der Eigentümer bzw. Gewahrsamsinhaber einer Sache wird grundsätzlich immer und unabhängig von Wert und Art der Sache Schutz vor Entziehung der Sachherrschaft begehren. Angesichts dessen schützt ihn § 259 StGB davor, dass eine ihm rechtswidrig entzogene Sache weiter von dem Berechtigten entfernt wird und dieser keine Zugriffsmöglichkeit mehr auf die Sache hat.[29] Bei Daten realisiert sich die Perpetuierung einer rechtswidrigen Lage hingegen nicht dadurch, dass ein Datenbestand dem Berechtigten nicht mehr zur Verfügung steht – er ist ja noch vorhanden. Eine Weitergabe gespeicherter Daten ist für den Berechtigten vielmehr nur im Hinblick auf die damit verbundene Weitergabe der *Inhalte* der Daten von Relevanz. Inwiefern sich hieraus eine Vertiefung der rechtswidrigen Lage ergeben kann, hängt aber stark von der Qualität der Daten ab. Da der Berechtigte die Daten in der Regel weiterhin selbst nutzen kann, ist für ihn vor allem von Bedeutung, ob sensible Daten einem weiteren Personenkreis bekannt oder zum Missbrauch genutzt werden.[30] Während der Berechtigte bei der Sachhehlerei somit unabhängig von der Art der Sache und der Form der Verfügung über diese schutzwürdig erscheint, liegen hinsichtlich Daten deutliche Abstufungen in Abhängigkeit von der Sensibilität der Daten und der Form ihrer Verarbeitung vor.

Schließlich steht das gesetzgeberische Konzept der Datenhehlerei auch in einem gewissen Widerspruch zu zivilrechtlichen Wertungen, die den grundlegenden Unterschieden zwischen Sachen und Daten Rechnung tragen. Während das Eigentum an Sachen durch die §§ 903, 985 BGB umfassend geschützt wird, ist der Zivilrechtsordnung eine dem entsprechende Regelung eines allgemeinen Ausschließlichkeitsrechts für Daten fremd. Ein solches nimmt der Gesetzgeber aber nun implizit an, wenn er die Datenhehlerei im Rahmen des formalen Schutzkonzeptes verortet und damit eine umfassende, ausschließliche „Datenherrschaft" schützt, die in der sonstigen Rechtsordnung gar nicht vorgesehen ist. Die inhaltlich differenzierenden Schutzkonzepte für Daten in verschiedenen Rechtsgebieten, etwa im Urheberrecht oder im Datenschutzrecht, werden von § 202d StGB ignoriert und nivelliert, der damit zugleich zu einer fragwürdigen Überkriminalisierung führt, die im Widerspruch zu den Vorgaben und Wertungen anderer Rechtsgebiete steht.

Vor diesem Hintergrund wäre eine Erfassung der Datenhehlerei im Rahmen des inhaltsbezogenen Schutzkonzepts angezeigt gewesen – wie dies etwa im Rahmen der Tatbestände des Geheimnisschutzes auch der Fall ist –, das eine Unterscheidung nach der Sensibilität des Inhalts der Daten vornimmt. Perspektivisch sollte der Gesetzgeber die Besonderheiten von Daten noch stärker berücksichtigen. Angesichts der bislang verfolgten Linie würde es sich hierfür anbieten, konsequenter zwischen dem formalen Schutz der Integrität von Datenbeständen einerseits und dem inhaltsbezogenen Schutzkonzept bezüglich der in den Daten enthaltenen Informationen andererseits zu differenzieren.[31]

IV. Reichweite des § 202d StGB

Die Verortung des § 202d StGB innerhalb des formalen Konzepts des strafrechtlichen Daten- und Informationsschutzes ist aus dogmatischer Sicht zwar nicht überzeugend. Sie ist angesichts des klaren Willens des Gesetzgebers aber hinzunehmen. Allerdings führt die systematisch verfehlte Fassung des Gesetzes zu einer erheblichen Weite der Strafbarkeit[32], die der Einschränkung bedarf.

1. Doppelte Entgrenzung

Der Schutz des § 202d Abs. 1 StGB betrifft – entsprechend dem formalen Schutzkonzept – alle Formen von gespeicherten Daten unabhängig von ihrem Inhalt (§ 202a Abs. 2 StGB), solange diese nicht allgemein zugänglich sind. Zugleich nimmt der objektive Tatbestand des § 202d StGB aber auch auf Seiten der Tathandlung kaum Einschränkungen vor. Anders als andere Tatbestände innerhalb des formalen Schutzkonzepts, wie die §§ 202a, 202b StGB, die die Überwindung von Zugangssicherungen oder den Zugriff auf eine nicht-öffentliche Datenübermittlung verlangen, genügt für die Datenhehlerei ausweislich des Wortlauts jedes Verschaffen oder Zugänglichmachen.[33]

Damit weist der Tatbestand im Vergleich zu benachbarten Normen eine doppelte Entgrenzung auf – sowohl hinsichtlich des Tatobjekts wie auch der Tathandlung. Dies führt zu einer problematischen Reichweite der Norm. Während andere Tatbestände entweder besonders sensible Daten umfassend vor Handlungen schützen – vor allem solche des inhaltsbezogenen Schutzkonzepts – oder umgekehrt alle gespeicherten Daten vor bestimmten besonderen Eingriffen bewahren wollen, erfasst § 202d StGB praktisch alle Verfügungen über gespeicherte Daten im Anschluss an eine Vortat. Die damit zu konstatierende undifferenzierte Weite des Tatbestandes des § 202d Abs. 1 StGB, der Sachverhalte mit stark variie-

[26] Allgemein zur Bestimmung des Berechtigten *Hilgendorf* (Fn. 7), § 202a Rn. 26 f.
[27] So *Selz* (Fn. 4), S. 925 f.
[28] *Ruhmannseder*, in: v. Heintschel-Heinegg (Fn. 6), § 259 Rn. 3.
[29] *Maier*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 2. Aufl. 2012, § 259 Rn. 2.
[30] Siehe auch *Golla/v. zur Mühlen*, JZ 2014, 668 (671); *Meinicke/Eidam*, K & R 2016, 315 (315).
[31] Siehe auch *Gercke*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl. 2015, § 202a StGB Rn. 1; *Golla*, ZIS 2016, 192 (196 f.).
[32] *Selz* (Fn. 4), S. 929.
[33] *Golla/v. zur Mühlen*, JZ 2014, 668 (669).

rendem Unrechtsgehalt erfasst, ist hinsichtlich der ultima ratio-Funktion des Strafrechts und den Bestimmtheitsanforderungen des Art. 103 Abs. 2 GG problematisch.[34]

2. Tatbestandsausschluss für Erfüllung beruflicher Pflichten (§ 202d Abs. 3 StGB)

Vor diesem Hintergrund ist eine gewisse Restriktion des Tatbestands der Datenhehlerei erforderlich. Dieses Problem hat auch der Gesetzgeber erkannt und in § 202d Abs. 3 StGB einen Tatbestandsausschluss für Handlungen bestimmter Berufsgruppen vorgesehen, wie sie in ähnlicher Weise auch bereits von den Tatbeständen zur Kinderpornographie bekannt sind.[35] Namentlich genannt sind zum einen in § 202d Abs. 3 Nr. 1 StGB Handlungen von Amtsträgern zur Beschaffung von Daten für die Verwertung in einem Steuer-, Straf- oder Ordnungswidrigkeitenverfahren, womit insbesondere die Beschaffung so genannter Steuer-CDs von der Strafbarkeit ausgenommen werden soll.[36] Zum anderen wurde im Laufe des Gesetzgebungsverfahrens § 202d Abs. 3 Nr. 2 StGB in den Tatbestand mit aufgenommen, der berufliche Handlungen von Journalisten von der Strafbarkeit nach Abs. 1 ausnimmt.

Allerdings macht das Wort „insbesondere" in § 202d Abs. 3 S. 2 StGB deutlich, dass die Nennung dieser beiden Berufsgruppen keine abschließende Aufzählung darstellen soll. Es handelt sich lediglich um Beispiele für die in § 202d Abs. 3 S. 1 StGB zu findende allgemeine Regelung, derzufolge alle Handlungen vom Tatbestand ausgenommen sind, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Diese Regelung ähnelt stark der Bestimmung in § 184b Abs. 5 Nr. 3 StGB, die einen entsprechenden Tatbestandsausschluss für das Verschaffen von kinderpornographischen Schriften vorsieht. Diese Regelung soll etwa Rechtsanwälte, Amtsträger der Strafverfolgungsbehörden, Sachverständige, Ärzte und Wissenschaftler erfassen, soweit die Handlungen konkret mit der beruflichen Tätigkeit in Verbindung stehen.[37] Dementsprechend ist auch für § 202d Abs. 3 S. 1 StGB anzunehmen, dass ein derartiger dienstlicher und beruflicher Umgang mit Daten, die aus einer rechtswidrigen Vortat stammen, tatbestandslos sein soll, der in (ansonsten) rechtmäßiger Weise und nur zu diesem Zweck erfolgt.

Dieser Ausschluss beruflicher Tätigkeiten von der Strafbarkeit wegen Datenhehlerei ist einerseits folgerichtig. Die wenig detaillierte und unklare Regelung in § 202d Abs. 3 S. 1 StGB führt andererseits aber zu einer erheblichen Rechtsunsicherheit für die genannten Berufsgruppen. Weder kann als geklärt angesehen sein, welche beruflichen Tätigkeiten tatsächlich von dem Tatbestandsausschluss umfasst sind, noch ist hinreichend klar, welche Rechtmäßigkeitsanforderungen jeweils für die in Rede stehende Handlung gelten sollen bzw. was sich überhaupt hinter dem Terminus „rechtmäßiger Pflichten" verbirgt.[38] In diesem Sinne hat etwa bei § 184b Abs. 5 StGB in der jüngeren Vergangenheit ein Fall für Aufsehen gesorgt, in dem ein Rechtsanwalt einem Sachverständigen kinderpornographische Schriften zur Begutachtung überlassen hatte und deswegen verurteilt wurde.[39]

Weiterhin muss die enge Anlehnung des Tatbestandsausschlusses an die Regelung in § 184b Abs. 5 StGB als wenig geglückt bezeichnet werden – die Sachlage ist dort eine grundlegend andere als hier. Anders als bei kinderpornographischen Schriften bestehen bezüglich rechtswidrig erlangter Daten kaum detailliert bestimmte Pflichten für einen beruflichen Umgang. Ebenso kann das Kriterium der Ausschließlichkeit der beruflichen Pflichterfüllung[40] nicht einfach übertragen werden, da ein paralleles persönliches Interesse an der Kenntnisnahme von bestimmten Daten – anders als bei kinderpornographischen Schriften – unschädlich sein sollte. Eine verfassungskonforme Auslegung muss hier jedenfalls für Medien und Wissenschaft einen breiten Raum der Straflosigkeit ergeben.

Vor diesem Hintergrund muss etwa das Medienprivileg des § 202d Abs. 3 Nr. 2 StGB weit verstanden werden, so dass journalistische Tätigkeit umfassend geschützt ist. Bei der an § 353b Abs. 3a StGB angelehnten Regelung ist zum einen ein weiter Begriff journalistischer Tätigkeit anzulegen, der Blogger und nicht hauptberuflich tätige Journalisten einschließt,[41] wie schon der Verweis auf § 53 Abs. 1 Nr. 5 StPO deutlich macht.[42] Zum anderen sollten – anders als dies bei § 184b Abs. 5 StGB angesichts der dort anderen Sachlage angenommen wird[43] – nicht alleine Handlungen privilegiert sein, die unmittelbar im Zusammenhang mit einer konkreten Veröffentlichung erfolgen.[44] Vielmehr muss es genügen, dass der Umgang mit den Daten ausschließlich der Ausübung der privilegierten Tätigkeit dient, auch wenn eine konkrete Veröffentlichung noch nicht in Planung ist.

Mit der gewählten Regelungstechnik – umfassender Tatbestand, wenig konkreter Tatbestandsausschluss – wälzt der Gesetzgeber zum einen das Risiko einer Fehlbewertung umfassend auf den Berufstätigen ab und ermöglicht zunächst einmal die Aufnahme strafrechtlicher Ermittlungen, begleitet

[34] So auch *Golla/v. zur Mühlen*, JZ 2014, 668 (670); *Schramm*, AnwBlBln 2015, 272.
[35] BT-Drs. 18/5088, S. 48.
[36] BT-Drs. 18/5088, S. 48.
[37] *Eisele*, in: Schönke/Schröder (Fn. 14), § 184b Rn. 16; *Ziegler*, in: v. Heintschel-Heinegg (Fn. 6), § 184b Rn. 16a.
[38] *Meinicke/Eidam*, K & R 2016, 315 (315 f.); *Roßnagel*, NJW 2016, 533 (537); *Selz* (Fn. 4), S. 929; allgemein zur Kritik schon *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 63. Aufl. 2016, § 184b Rn. 42.
[39] OLG Frankfurt NJW 2013, 1107.
[40] Zu diesem *Hörnle*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 2. Aufl. 2012, § 184b Rn. 41; *Lackner/Kühl* (Fn. 6), § 184b Rn. 9.
[41] Siehe zu § 353b Abs. 3a StGB *Graf*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 2. Aufl. 2014, § 353b Rn. 59 ff.
[42] *Neuhöfer*, jurisPR-Compl 4/2015, Anm. 6; vgl. auch *Perron*, in: Schönke/Schröder (Fn. 14), § 353b Rn. 21c.
[43] *Hörnle* (Fn. 40), § 184b Rn. 41.
[44] *Franck*, RDV 2015, 180 (182); siehe aber BT-Drs. 18/5088, S. 48; skeptisch auch *Dix/Kipker/Schaar*, ZD 2015, 300 (305).

von entsprechenden Eingriffsmaßnahmen.[45] Dies wirkt sich bei der Datenhehlerei noch deutlich schwerwiegender aus, als bei § 184b StGB. Während der Umgang mit kinderpornographischen Schriften im beruflichen Kontext selten ist und die diesbezüglichen rechtlichen Anforderungen vergleichsweise klar sind, ist dies bei aus einer rechtswidrigen Vortat stammenden Daten nicht der Fall. Der Umgang mit diesen dürfte praktisch wesentlich häufiger sein; zugleich können – anders als bei kinderpornographischen Schriften – nicht ganz selten berechtigte Interessen für einen Umgang mit solchen Daten streiten.[46]

Schließlich begegnet die Gleichbehandlung von staatlichen Amtsträgern auf der einen und privaten Berufsgruppen auf der anderen Seite im Rahmen des Tatbestandsausschlusses grundlegenden Bedenken. Einerseits steht zu befürchten, dass die genannten Unklarheiten des Gesetzes für Amtsträger in der Praxis eher zu deren Gunsten, für andere Betroffene aber je nach Lage des Einzelfalles und gemäß den Bewertungen des Rechtsanwenders genutzt werden. Bezüglich Amtsträgern begründet dies zum einen die Gefahr, dass deren Handlungsbefugnisse weniger klar sind; auch ist das Verhältnis zu deren Amtsbefugnissen ungeklärt.[47] Zum anderen berücksichtigt die Gleichbehandlung nicht die divergierende Machtposition und daraus resultierende Gefährdungen zwischen Amtsträgern auf der einen und Privaten auf der anderen Seite, die grundsätzlich eine strengere rechtliche Bindung staatlichen Handelns verlangt.[48] Dies gilt auch und gerade im vorliegenden Kontext, wo die neue Regelung des § 202d Abs. 3 Nr. 1 StGB unter Umständen nicht nur die Strafbarkeit nach § 202d Abs. 1 StGB betrifft, sondern auch eine solche nach anderen Tatbeständen und somit eine Art Sperrwirkung entfaltet. Je nachdem, wie weit man diese ziehen will – was angesichts der divergierenden Schutzgüter der in Betracht kommenden Tatbestände unterschiedlich beurteilt werden mag – kann § 202d Abs. 3 Nr. 1 StGB damit gar eine umfassende Legalisierung des Ankaufs rechtswidrig erlangter Daten durch die Strafverfolgungsbehörden bedeuten.[49] Angesichts dessen treten verschiedene Autoren der Privilegierung von Amtsträgern zu Recht bereits im Grundsatz entgegen.[50]

3. Restriktive und sachhehlerspezifische Auslegung des Tatbestandes

Vor diesem Hintergrund – doppelte Entgrenzung des Tatbestandes, wenig klarer Tatbestandsausschluss für berufliche Tätigkeiten – kommt einer weitergehenden restriktiven Auslegung des Tatbestands Bedeutung zu. Diese könnte auf Seiten des objektiven Tatbestandes an zwei Punkten ansetzen: dem Tatobjekt oder der Tathandlung. Aus teleologischer Sicht spräche nach den vorstehenden Ausführungen vieles dafür, die Geltung des Tatbestandes auf bestimmte, besonders sensible Daten zu beschränken. Hierfür würde auch das Ziel des Gesetzgebers sprechen, der vor allem die eingangs genannten besonderen Formen der Cyberkriminalität vor Augen hatte. Indes ist dieser Weg durch den klaren Wortlaut des Tatbestandes wie auch seine systematische Einordnung versperrt. § 202d Abs. 1 StGB nimmt eindeutig Bezug auf den formellen Datenbegriff in § 202a Abs. 2 StGB.

Damit verbleibt auf objektiver Seite alleine noch ein restriktives Verständnis der genannten Tathandlungen, wie es für das formale Schutzkonzept typisch ist. Ausweislich seines Wortlauts erfasst § 202d Abs. 1 StGB alle Handlungen, mittels derer sich eine Person die bemakelten Daten selbst verschafft oder sie einem Dritten verschafft oder zugänglich macht, einschließlich der Zugänglichmachung durch Verbreitung. Nicht anders als bei der Sachhehlerei nach § 259 StGB[51] ist dafür ein einverständliches Zusammenwirken mit dem Vortäter und also ein derivativer Erwerb zu fordern. Eine Übernahme der Verfügungsmacht gegen oder ohne den Willen des Vortäters ist danach nicht erfasst.[52] Eine solche sachhehlerspezifische Auslegung ist sowohl für die Erwerbs-, wie auch für die Absatzhehlerei zu fordern, wobei letztere im Fall des § 202d Abs. 1 StGB zutreffender mit dem Begriff der Übermittlungshehlerei erfasst ist. Eine weitergehende Einschränkung des Tatbestandes ist hingegen nur schwer zu begründen.

Im subjektiven Bereich ist eine Restriktion alleine über die überschießende Innentendenz denkbar. Während die Variante der Bereicherungsabsicht[53] vergleichsweise klar ist, ist die Reichweite der Schädigungsabsicht nicht abschließend geklärt. Bei § 203 Abs. 5 StGB verstehen Teile der Literatur diese eng und verlangen mit gewichtigen, vor allem systematischen Argumenten einen Vermögensbezug.[54] Nach anderer Auffassung sollen hingegen auch immaterielle Schäden von der Regelung erfasst sein,[55] wofür insbesondere der Wortlaut spricht. Dieses starke Argument gibt auch im Kontext des § 202d Abs. 1 StGB den Ausschlag, so dass auch immaterielle Schäden erfasst sind. Dabei ist aber zu beachten, dass der beabsichtigte Schaden über das hinausgehen muss, was ohnehin bereits vom objektiven Tatbestand erfasst wird.[56] Zudem ist der Begriff der Schädigungsabsicht nach den vorstehenden Ausführungen restriktiv auszulegen. Dabei ist nach

[45] *Schramm*, AnwBlBln 2015, 272 (274).
[46] *Schramm*, AnwBlBln 2015, 272 (274).
[47] *Dix/Kipker/Schaar*, ZD 2015, 300 (304 f.).
[48] Siehe zu Amtsdelikten im Allgemeinen nur *Heinrich*, Der Amtsträgerbegriff im Strafrecht, 2001, S. 279 ff.
[49] *Klengel/Gans*, ZRP 2013, 16 (18); zur möglichen Strafbarkeit dessen siehe etwa *Kelnhofer/Krug*, StV 2008, 660 (661 f.); *Seitz*, Ubg 2014, 380 (385 f.); *Spernath*, NStZ 2010, 307 (308); *Trüg/Habetha*, NJW 2008, 887 (888); *Trüg*, StV 2011, 111 ff.
[50] *Dix/Kipker/Schaar*, ZD 2015, 300 (304 f.).
[51] *Ruhmannseder* (Fn. 28), § 259 Rn. 3.
[52] So auch die Gesetzesbegründung BT-Drs. 18/5088, S. 47.
[53] Zu diesen *Ambs* (Fn. 8), § 44 BDSG Rn. 2; *Golla*, ZIS 2016, 192 (192 f.); *Kargl* (Fn. 19), § 203 Rn. 82 f.
[54] *Bosch* (Fn. 23), § 203 Rn. 49; *Hoyer* (Fn. 19), § 203 Rn. 64; *Kargl* (Fn. 19), § 203 Rn. 84.
[55] *Ambs* (Fn. 8), § 44 BDSG Rn. 2; siehe auch *Cierniak/Pohlit*, in: Joecks/Miebach (Fn. 29), § 203 Rn. 135; *Lackner/Kühl* (Fn. 6), § 203 Rn. 28; *Schünemann*, in: Laufhütte/Rissing-van Saan/Tiedemann (Fn. 6), § 203 Rn. 164.
[56] Vgl. *Cierniak/Pohlit* (Fn. 55), § 203 Rn. 135; *Hoyer* (Fn. 19), § 203 Rn. 64 zu § 203 StGB.

hier vertretener Auffassung eine Interessenabwägung vorzunehmen, die im Fall altruistischer Motivation bei der Verbreitung von Inhalten, nicht hingegen beim Missbrauch von Identitätsdaten, zu einer Verneinung der Schädigungsabsicht führen kann, indem der Begriff der Schädigung eng ausgelegt wird.

Für die eingangs genannten Fälle führt dies zu folgenden Ergebnissen:

Fall 1: T macht sich als Vortäter nicht nach § 202d Abs. 1 StGB strafbar, wohl aber H, der sich die Daten verschafft.

Fall 2: B kann selbst über die Daten verfügen, macht sich also nur nach § 353b StGB strafbar. Diese Tat ist erst mit der Übermittlung der Daten an A vollendet, so dass A sich durch die Entgegennahme mangels Vollendung der Vortat noch nicht gemäß § 202d Abs. 1 StGB strafbar macht. Anderes gilt für die Weitergabe an den Journalisten. J ist zwar selbst durch das Medienprivileg geschützt. Dieses betrifft jedoch nicht den A, der daher nur durch eine restriktive Auslegung der Schädigungsabsicht einer Strafbarkeit entgehen könnte.

Fall 3: T hat den Stick unterschlagen. Das somit rechtswidrig erlangte Rezept verschafft sich der B durch den Ankauf. Sofern B die Herkunft des Rezeptes kennt, kann auch er sich nach § 202d Abs. 1 StGB strafbar machen.

V. Zusammenfassung und Fazit

Zusammenfassend betrachtet begegnet der neue Tatbestand des § 202d StGB erheblichen Bedenken. Erstens ist die damit geschlossene Strafbarkeitslücke klein: Sowohl die Entwendung von Identitätsdaten, als auch deren Nutzung für weitere Straftaten – insbesondere Vermögensdelikte – stehen recht umfassend unter Strafe.[57] Den beklagten Strafbarkeitslücken hätte deutlich einfacher auch durch eine punktuelle Veränderung bestehender Tatbestände begegnet werden können[58], die den Handel mit Identitätsdaten unter Strafe stellen.[59]

Zweitens werden durch den Tatbestand sehr viel mehr Sachverhalte pönalisiert als diejenigen, mit denen seine Einführung begründet wurde. Dies ist insbesondere durch die systematisch verfehlte Verortung des Tatbestandes innerhalb des formalen anstelle des inhaltsbezogenen Schutzkonzeptes bedingt, die zu einer doppelten Entgrenzung des Tatbestandes führt – sowohl hinsichtlich des Tatobjekts, wie auch der Tathandlungen. Damit erfasst der Tatbestand undifferenziert alle Verfügungen über alle Arten von gespeicherten Daten, solange diese aus einer rechtswidrigen Vortat stammen und mit der vom Tatbestand vorausgesetzten Absicht gehandelt wird. Dies führt dazu, dass auch solche Handlungen dem Tatbestand unterfallen, deren Strafwürdigkeit äußerst zweifelhaft ist. Angesichts dessen ist der Tatbestand des § 202d Abs. 1 StGB auch über die Einschränkungen in Abs. 3 hinaus restriktiv auszulegen.

Drittens schließlich ist die Einschränkung des Tatbestandes in § 202d Abs. 3 StGB wenig klar und begründet für die einschlägigen Berufsgruppen die Gefahr einer strafrechtlichen Verfolgung. Selbst wenn es am Ende nicht zu einer Verurteilung kommt, stellt sich bereits die Einleitung eines Strafverfahrens und die Durchführung von Ermittlungs- und Zwangsmaßnahmen beispielsweise gegenüber Journalisten oder Wissenschaftlern als erhebliche Gefahr für den freien Informationsfluss in der Gesellschaft dar.

[57] *Franck*, RDV 2015, 180 (182); *Selz* (Fn. 4), S. 917 ff.; siehe auch *Sieber* (Fn. 3), S. 59 f.
[58] *Golla*, ZIS 2016, 192 (196 ff.); eingehend dazu *Golla/v. zur Mühlen*, JZ 2014, 668 (671 ff.); siehe auch *Meinicke/Eidam*, K & R 2016, 315 (315).
[59] Dazu *Gercke*, ZUM 2013, 605 (607).

Tabelle

	Erheben, Beschaffen	*Verarbeiten, Nutzen*
Inhaltsbezogener Schutz (Geheimnisse, personenbezogene Daten u.ä.)	§§ 201 Abs. 1, Abs. 2, 201a Abs. 1, 202 StGB, § 17 UWG, § 44 BDSG	§§ 201, 201a, 203, 204, 353b StGB, § 17 Abs. 1, Abs. 2 UWG, § 44 BDSG
Formaler Schutz (Daten i.S.v. § 202a Abs. 2 StGB)	§§ 202a, 202b StGB	§§ 202d StGB
Sachen	§§ 242, 246 StGB	§ 259 StGB