2. Assistententagung Grüner Bereich

Freiburg 2017

Hennemann | Sattler [Hrsg.]

Immaterialgüter und Digitalisierung

Junge Wissenschaft zum Gewerblichen Rechtsschutz, Urheber- und Medienrecht

Nomos

2. Assistententagung Grüner Bereich

Freiburg 2017

Moritz Hennemann | Andreas Sattler [Hrsg.]

Immaterialgüter und Digitalisierung

Junge Wissenschaft zum Gewerblichen Rechtsschutz, Urheber- und Medienrecht

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8487-4102-1 (Print)
ISBN 978-3-8452-8411-8 (ePDF)

1. Auflage 2017
© Nomos Verlagsgesellschaft, Baden-Baden 2017. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

Vorwort

Unter dem Generalthema *Immaterialgüter und Digitalisierung* fand am 21. und 22. Juni 2017 die Tagung „Junge Wissenschaft – Kolloquium zum Gewerblichen Rechtsschutz, Urheber- und Medienrecht“ an der Albert-Ludwigs-Universität in Freiburg im Breisgau statt. Die Tagung folgte auf entsprechende Veranstaltungen in München 2015 (hierzu Hofmann/Raue, GRUR 2015, 1088) und in Köln 2016 (hierzu Specht, GRUR Newsletter, Sonderausgabe 2016 – 125 Jahre GRUR, S. 22).

Die Veranstaltung richtete sich vornehmlich an PostDocs und Promovierende sowie alle wissenschaftlich interessierten Praktikerinnen und Praktiker, die auf den Gebieten des Immaterialgüter-, IT- und Medienrechts tätig sind. Diskutiert wurden Fragestellungen aus dem Urheber- und Medienrecht, dem Daten- und Datenschutzrecht sowie dem Kartellrecht. Die Referentinnen und Referenten aus Deutschland, Österreich und Großbritannien nutzten diese Gelegenheit zu anregenden Diskussionen über den Schutz von Daten und die Gewährleistung eines Zugangs zu Daten, aktuelle Gesetzesvorhaben sowie der Suche nach wirksamen Regulierungsinstrumenten im Zeitalter der Digitalisierung. Wir freuen uns sehr, dass die Beiträge zur Tagung nunmehr in dem vorliegenden Tagungsband als Band 2 der Reihe „Assistententagung Grüner Bereich“ einer breiteren Öffentlichkeit zugänglich gemacht werden können.

Gefördert wurde die Tagung von der Deutschen Vereinigung für Gewerblichen Rechtsschutz und Urheberrecht e.V. (GRUR), durch die Kanzlei Hengeler Mueller und durch den Nomos Verlag. Erst durch diese großzügige Unterstützung konnte die Veranstaltung und die Publikation dieses Tagungsbandes realisiert werden. Ihnen allen gebührt unser besonderer Dank. Herrn Dr. Marco Ganzhorn danken wir für die engagierte verlagsseitige Betreuung des Tagungsbandes. Unser herzlicher Dank gilt schließlich auch den Mitarbeiterinnen und Mitarbeitern des Instituts für Medien- und Informationsrecht, Abt. I: Privatrecht (Lehrstuhl Paal), deren vorbildliches Engagement den reibungslosen Ablauf der Veranstaltung erst ermöglicht hat.

Erfreulicherweise ist es auch gelungen, die Zukunft dieser Plattform zum Austausch zwischen junger Wissenschaft und Praxis zu sichern. Die nächste Tagung wird im Sommer 2018 an der TU München stattfinden.

Moritz Hennemann *Andreas Sattler*

Inhalt

Das Strafrecht als schlechtes Vorbild – Betrachtung zum „Dateneigentum“ und § 202d StGB

Sebastian J. Golla[*] und Sebastian Thess[**]

A. Wem gehören die Daten?

Am Vorabend der Eröffnung der CeBIT 2017 bezog Bundeskanzlerin *Angela Merkel* Stellung dazu, wie die Gesetzgebung auf die zunehmende Bedeutung der Prozessierung und Sammlung von Daten im Automotivbereich reagieren werde: Es seien unter anderem „eigentumsrechtliche Fragen“ zu klären. Man befände sich „noch mitten in der Diskussion“, es sei aber „natürlich wichtig, ob dem Autohersteller die Dinge gehören, oder ob dem Softwarehersteller die Daten gehören. Denn mit den Daten über die Nutzer wird man natürlich wieder neue Produkte und Anwendungen herstellen können.“[1] Provoziert von *Merkels* Äußerung präsentierte der Satiriker *Dietmar Wischmeyer* darauf in seinem „Logbuch der Bekloppten und Bescheuerten“ in der heute-show eine „ganz verrückte“ Idee: „Wie wäre es denn, wenn dem Kunden seine Daten gehören würden?“[2] Der Nutzer des Automobils war in Merkels Liste potentieller „Dateneigentümer“ nicht aufgetaucht.

---

* Dr. jur. Der Autor ist wissenschaftlicher Mitarbeiter an der Johannes Gutenberg-Universität Mainz. Er hat an der unter dem Aktenzeichen 1 BvR 2821/16 anhängigen Verfassungsbeschwerde gegen § 202d StGB mitgewirkt.

** Der Autor ist wissenschaftlicher Mitarbeiter an der Humboldt-Universität zu Berlin. Er hat an der unter dem Aktenzeichen 1 BvR 2821/16 anhängigen Verfassungsbeschwerde gegen § 202d StGB mitgewirkt.

1 Video-Podcast der Bundeskanzlerin #10/2017 vom 18.3.2017, abrufbar unter https://www.bundeskanzlerin.de/Webs/BKin/DE/Mediathek/Einstieg/mediathek_einstieg_podcasts_node.html?id=2138524 (zuletzt abgerufen am 22.6.2017).

2 heute-show vom 28.4.2017, Wischmeyer seine Daten, abrufbar unter https://www.zdf.de/comedy/heute-show/wischmeyer-seine-daten-102.html (zuletzt abgerufen am 22.6.2017).

Auch diverse andere Spitzenpolitiker haben sich bereits unterschiedlich zum „Dateneigentum“ geäußert.[3] Dieses Thema und die kontroverse Diskussion darüber, wem Daten „gehören“, sind damit im Mainstream angekommen. Konkrete Lösungen zu den aufgeworfenen Fragen sind weder in dem – sich rasch mehrenden – juristischen Schrifttum,[4] noch auf Ebene der Gesetzgebung in kurzer Zeit zu erwarten.[5] Die gesellschaftliche Relevanz des Themas wird jedoch zunehmend klar, auch weit über das „Lieblingsspielzeug“ Automobil hinaus. Die Journalistin *Christiane Schulzki-Haddouti* verglich etwa die Situation der Digital Natives in der heutigen Zeit angesichts des Versuches, eine neue Eigentumskategorie des „Dateneigentums“ einzuführen, mit der Situation der „Ureinwohner des amerikanischen Kontinents, als europäische Siedler ihnen anhand von Papierzetteln den Begriff des ‚Landeigentums‘ erklären wollten“.[6] Die Frage, ob und wie ein „Dateneigentum“ geregelt wird, könnte für den Umgang mit Informationen in vielen Bereichen richtungsweisend sein. Eine nicht ausreichend bedachte Neuregelung von Verfügungsrechten über Daten könnte sich als ebenso großer Fehlgriff herausstellen wie der Tausch beträchtlicher Territorien gegen Glasperlen und Feuerwasser.

Die Diskussion darüber, ob (Quasi-)Immaterialgüterrechte an bestimmten Arten von Daten bestehen oder durch den Gesetzgeber neu geschaffen

---

3 Jüngst etwa kritisch zu dem u. a. von Renate Künast geprägten Slogan „Meine Daten gehören mir“ *de Maizière*, Datenschutz ist kein Selbstzweck, Tagesspiegel vom 16.2.2017, abrufbar unter http://www.tagesspiegel.de/politik/data-debates-datenschutz-ist-kein-selbstzweck/19391956.html (zuletzt abgerufen am 22.6.2017); vgl. für einen Überblick die Statements von Politikern großer Parteien bei *Härting/Golla*, Drei Fragen zum „Dateneigentum“, PinG Spezial, abrufbar unter http://www.pingdigital.de/blog/wp-content/uploads/2016/06/PinG_2016-04_Leseprobe_Haerting_komplett.pdf (zuletzt abgerufen am 22.6.2017).

4 Vgl. nur *Berberich/Golla*, PinG 2016, 165 ff.; *Dorner*, CR 2014, 617 ff.; *Fezer*, ZD 2017, 99 ff.; *Härting*, CR 2016, 646 ff.; *Heun/Assion*, CR 2015, 812 ff.; *Heymann*, CR 2016, 650 ff.; *Kerber*, GRUR Int. 2016, 989 ff.; *Malgieri*, PinG 2016, 133 ff.; *Paal/Hennemann*, NJW 2017, 1697, 1698; MüKo/*Wagner,* BGB, 8. Aufl. 2017, § 823 BGB Rn. 294 ff.; *Specht/Rohmer*, PinG 2016, 127 ff.; *Zech*, GRUR 2015, 1151 ff.

5 Allerdings führte die Europäische Kommission jüngst in einem Arbeitspapier diverse mögliche Regelungsansätze für ein neues Data producer's right auf; Comission Staff Working Document on the free flow of data and emerging issues of the European data economy vom 10.1.2017, SWD (2017) 2 final, S. 33.

6 *Schulzki-Haddouti*, Wem gehören „meine Daten", iRIGHTS.info vom 24.3.2016, abrufbar unter: https://irights.info/artikel/wem-gehoeren-meine-daten/27159 (zuletzt abgerufen am 22.6.2017).

werden sollten, hat ihren Hauptschauplatz im Zivilrecht, das für die Zuordnung von Daten als Wirtschaftsgütern am ehesten in Betracht kommt. Allerdings werden im Diskurs bisweilen auch bestehende Regelungen des Strafrechts herangezogen, um Verfügungsrechte an Daten zu begründen oder diese zumindest als Modell für eine mögliche zivilrechtliche Regelung anzuführen. Dieser Beitrag zeigt die Grenzen der Orientierung an den strafrechtlichen Regelungen in der Diskussion um neue Rechte an Daten auf. Dabei legt er einen Schwerpunkt auf die neue Regelung zur „Datenhehlerei" in § 202d StGB und betrachtet auch dessen (Un-)Vereinbarkeit mit dem Grundgesetz.

B. Die strafrechtliche Regelung als schlechtes Vorbild

Die Idee, ein „Dateneigentum" für das Zivilrecht nach dem Vorbild strafrechtlicher Regelungen zu konstruieren, hat prominente Fürsprecher.[7] In dieser Diskussion scheinen sogar eingefleischte „Zivilisten" mit Blick auf die scheinbar fortschrittliche Regelung in den §§ 202a ff., 303a f. StGB eine neue Leidenschaft für das Strafrecht zu entdecken. Die Heranziehung der strafrechtlichen Regelungen ist jedoch kaum gewinnbringend für die Fortentwicklung des Rechts in diesem Bereich. Aus ihnen lässt sich kein stringentes Konzept eines „Dateneigentums" ableiten, das dazu geeignet wäre, auf das Zivilrecht übertragen zu werden.

I. § 202a und § 303a StGB als Regelungen zum Integritätsschutz

§ 202a und § 303a StGB liegt ein formelles Schutzkonzept von Daten zugrunde.[8] Die Vorschriften sind in ihrer Konzeption aber nicht geeignet, um als Referenz oder Quelle für ein „Dateneigentum" zu dienen. Sie zielen auf spezifische Gefährdungen und schützen zuvorderst die Integrität von Daten.

---

7 *Hoeren*, MMR 2013, 486, 487 ff.; vgl. auch MüKo/*Wagner*, BGB, 8. Aufl. 2017, § 823 Rn. 296.

8 *Singelnstein*, ZIS 2016, 432, 434.

§ 202a StGB (Ausspähen von Daten) zielt unter anderem darauf ab, Fälle des Hacking zu kriminalisieren.[9] Die Regelung wurde ursprünglich geschaffen, um als Daten dargestellte Informationen gegen Spionage zu schützen und das unbefugte Eindringen in Datenverarbeitungssysteme[10] unter Strafe zu stellen.[11] Dabei wurde die Neuregelung in einer besonderen Nähe zu § 202 StGB (Verletzung des Briefgeheimnisses) gesehen. Auch aus dieser Verwandtschaft lässt sich herleiten, dass § 202a StGB eher eine eng formal begrenzte Geheimsphäre als eine umfassende Verfügungsbefugnis schützt.

§ 303a StGB (Datenveränderung), der als Ergänzung zu § 303 StGB konzipiert ist,[12] könnte sich noch eher als Basis eines „Dateneigentums" eignen. Jedoch liefert auch § 303a StGB allenfalls Stoff für einen Schutz der Integrität und Verfügbarkeit von Daten. Dies zeigt schon die Anlehnung an das Delikt der Sachbeschädigung. Beim Sacheigentum im Sinne von § 903 BGB ist zwischen dem Schutz der Integrität sowie der freien Nutzung und Verwertung von Sachen zu unterscheiden. Nur erstere lässt sich bei Daten ohne besondere Feinjustierungen ähnlich wie bei Sachen schützen. Hier besteht ein vergleichbares Interesse an Unversehrtheit und Verfügbarkeit. Nutzung und Verwertung von Daten unterscheiden sich allerdings gravierend von jener von Sachen. Daten sind nicht an den Ort ihrer Verkörperung gebunden, können beliebig oft vervielfältigt werden und dem parallelen Zugriff beliebig vieler Personen ausgesetzt sein. Mit einer Nutzung von Daten ist, anders als regelmäßig bei Sachen, auch keine Abnutzung im Sinne der Beeinträchtigung ihrer Integrität verbunden. Es wäre widersinnig, die Verfügungsrechte hier gleichlaufend zu regeln. Daher ist auch die jüngste Ankündigung des Bundesministeriums für Verkehr und digitale Infrastruktur, Daten im Wege einer gesetzlichen Regelung „im Ergebnis mit Sachen gleichstellen" zu wollen, alarmierend.[13] Eine

9 BT-Drs. 16/3656, S. 9 f., 16; vgl. auch NK/*Kargl* StGB, 4. Aufl. 2013, § 202a Rn. 1 ff.

10 Daher wird die Regelung zum Teil auch als „elektronischer Hausfriedensbruch" bezeichnet; Schönke/Schröder/*Lenckner/Eisele*, StGB, 29. Aufl. 2014, § 202a Rn. 18 m.w.N.

11 BT-Drs. 10/5058, S. 28.

12 BT-Drs. 10/5058, S. 34; vgl. auch MüKo/*Wieck-Noodt,* StGB, 2. Aufl. 2014, § 303a Rn. 1.

13 BMVI, Strategiepapier Digitale Souveränität, abrufbar unter: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html (zuletzt abgerufen am 22.6.2017).

Gleichstellung im Hinblick auf die Verfügungsrechte an Daten würde die genannten grundlegenden Unterschiede vernachlässigen.

Es steht außer Frage, dass gerade die wirtschaftliche Weiterverwendung sowie die Transaktionsfähigkeit von Daten und damit die Verfügungsrechte an ihnen für ein privates „Datenverkehrsrecht" relevant sind. Gerade hier helfen allerding die § 202a und § 303a StGB zugrundeliegenden Konzepte nicht weiter. Dies gilt unter anderem für das Konzept des Skripturaktes. Demnach ist im Zusammenhang mit den §§ 202a f., 303a f. StGB derjenige zur Verfügung über Daten befugt, der diese gespeichert hat (Skribent). Die Zuordnung von Eigentumsrechten an Daten ist eine der wichtigsten Fragen bei der möglichen Regelung eines „Dateneigentums". Doch es dürfte schwierig sein, eine sachgerechte Lösung dafür zu finden, Daten stets „eindeutig natürlichen oder juristischen Personen als ‚Eigentum'" zuzuweisen. Auf den ersten Blick erscheint es einleuchtend, angelehnt an das Strafrecht durch die Skriptur bzw. „Herstellung" von Daten die Verfügungsberechtigung an diesen zu bestimmen. Der Teufel liegt hier jedoch im Detail. Schon für bewegliche Sachen ist die Frage nach dem Hersteller bei arbeitsteiligen Wertschöpfungsprozessen oft schwierig zu beantworten und bisweilen Gegenstand komplexer vertraglicher Regelungen. Bei Daten kommen weitere Probleme hinzu, wenn man die Skriptur als Kriterium für die Zuordnung heranzieht. Wenn Daten kopiert und damit neu geschrieben werden, entsteht nach dem strafrechtlichen Konzept die Verfügungsbefugnis an diesen bei dem Kopierenden neu. Dies gilt nach einhelliger Ansicht auch dann, wenn der Kopierende sich die ursprünglichen Daten unbefugt verschaffte.[14] §§ 202a f., 303a f. StGB schützen Daten als konkrete Repräsentation von Informationen also von dem Zeitpunkt an, zu dem diese konkret geschrieben werden, vor einem unbefugten Zugriff oder einer Beeinträchtigung. Der Schutz der Daten endet aber dann, wenn sie neu geschrieben werden. Eine immaterialgüterrechtsähnliche Zuweisung der in den Daten enthaltenen Informationen ist mit dem Schutz der formellen Verfügungsbefugnis an Daten nicht verbunden. Auch für die Verkehrsfähigkeit und Handelbarkeit von Daten ist dieses Konzept nicht ergiebig, da die Verfügungsrechte durch einen faktischen und nicht einen rechtsgeschäftlichen Vorgang neu entstehen.

---

14 OLG Nürnberg v. 23.1.2013 – 1 Ws 445/12, CR 2013, 213, 214; *Hoeren*, MMR 2013, 486, 488; Schönke/Schröder/*Stree/Hecker*, StGB, 29. Aufl. 2014, § 303a Rn. 3; *Selz*, in: Taeger, Internet der Dinge, 2015, S. 915, 925 m.w.N.

II. Die „Datenhehlerei" als Fehlkonstruktion

Auch der neue Straftatbestand der Datenhehlerei (§ 202d StGB) taugt nicht als Blaupause für die Anerkennung eines „Dateneigentums". Er zeigt im Gegenteil sogar noch deutlicher als die bisherigen Regelungen, dass der Schutz der Verkehrsfähigkeit bzw. Handelbarkeit von Daten im Wirtschaftsverkehr über die existierenden Konzepte des Strafrechts nicht in den Griff zu bekommen ist. Der Straftatbestand kann die als Schutzgut ausgerufene Verfügungsbefugnis an Daten[15] bzw. das formelle Datengeheimnis[16] nämlich gar nicht wirksam schützen.[17] § 202d StGB soll typischerweise in Dreierkonstellationen Anwendung finden, in denen ein „Datendieb" dem ursprünglichen Inhaber der Daten diese entwendet und sie an einen „Datenhehler" weiterleitet. In diesen Konstellationen wird die formelle Verfügungsbefugnis des ursprünglichen Dateninhabers aber nur in den seltensten Fällen durch den „Datenhehler" gebrochen bzw. verletzt. Der „Datendieb" bricht zwar zunächst durch unbefugten Zugriff die Verfügungsmacht des ursprünglichen Inhabers und macht sich regelmäßig nach § 202a f. StGB strafbar. Sobald er die Daten aber kopiert, entsteht die Verfügungsbefugnis bei ihm neu. Zwar enthält der durch Kopie neu entstandene Datensatz des „Datendiebs" die gleichen Informationen wie der ursprüngliche Datensatz des Dateninhabers, technisch gesehen handelt es sich aber um eine neue Repräsentation dieser Informationen.[18] Die formelle Verfügungsbefugnis des über die ursprünglichen Daten Verfügungsberechtigten erstreckt sich gerade nicht auf Kopien dieser Daten, mag er auch Rechte an den Inhalten haben.[19] Gibt er sie dann an den „Datenheh-

15 BT-Drs. 18/5088, S. 3, S. 26 f. und S. 46.

16 BT-Drs. 18/5088, S. 26, S. 45 ff.

17 *Selz*, in: Taeger, Internet der Dinge, 2015, S. 915, 926.

18 Das Entwenden, Kopieren und Weitergeben von Daten aus einem Computersystem lässt sich insofern grob vergleichen mit dem Fall, in dem eine Person in ein Gebäude einbricht, dort ein Blatt aus einem Aktenordner auf selbst mitgebrachtem Papier kopiert und diese Kopie einem Dritten verkauft. Zwar liegen ein Hausfriedensbruch und möglicherweise Delikte nach BDSG und UWG vor, das Eigentum an der neuen Kopie des Blattes Papier liegt aber bei dem Einbrecher. Es wäre kein tauglicher Tatgegenstand einer Hehlerei; vgl. *Berberich/Golla*, PinG 2016, 165, 172.

19 Die Frage des inhaltlichen Schutzes ist von §§ 202 a ff. StGB getrennt zu betrachten und kann u. a. zu Strafbarkeiten nach §§ 43, 44 BDSG oder § 17 UWG führen.

ler“ weiter, kann letzterer die Verfügungsbefugnis des Dateninhabers damit im Ergebnis nicht mehr brechen.

Die Datenhehlerei vermag die formelle Verfügungsbefugnis des Dateninhabers damit nie zu schützen, wenn die Daten zuvor durch den „Datendieb“ kopiert werden. Da aber die Weitergabe von Daten auf elektronischem Wege letztlich stets mit einem Kopiervorgang verbunden ist, verfehlt die Norm in den vom Gesetzgeber als Anlass der Einführung proklamierten Fällen – dem Handel mit rechtswidrig erlangten digitalen Identitäten wie z. B. Kreditkartendaten oder Zugangsdaten zu Onlinebanking, E-Mail-Diensten oder sozialen Netzwerken auf Webportalen und in Foren[20] – ihren Schutzzweck.

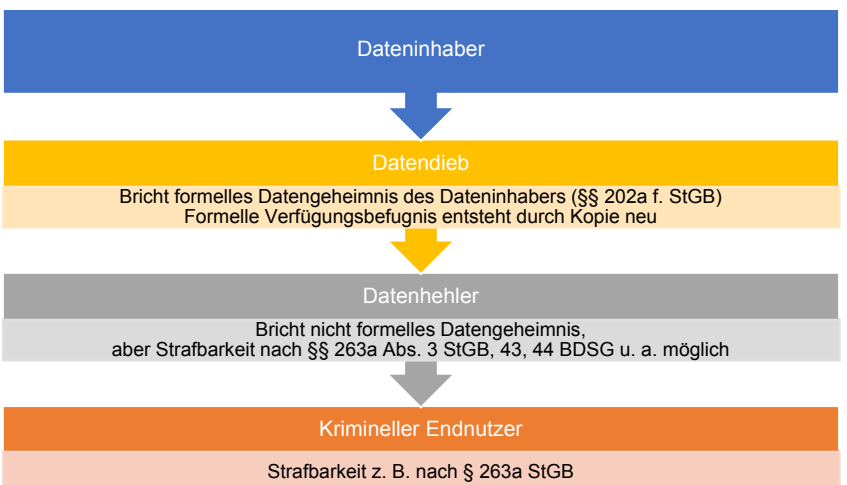

Abbildung: Formelle Verfügungsbefugnis und Datenhehlerei

Aufgrund des verfehlten Schutzzwecks und der uferlosen Weite des Tatbestandes, der Daten unabhängig von einschränkenden Kriterien wie beispielsweise einem Personenbezug oder einem zumindest schützenswerten Interesse[21] einbezieht und auch nicht ausdrücklich einen Bruch der for-

20 BT-Drs. 17/14362, S. 1.

21 So waren nach der Erstfassung des § 202d Abs. 2 StGB nur solche Daten im Sinne des Absatzes 1 erfasst, an deren Nichtweiterverwendung der Berechtigte ein schutzwürdiges Interesse hat (BT-Drs. 17/14362, S. 14 f.); diese Einschränkung wurde im weiteren Gesetzgebungsverfahren aufgegeben.

mellen Verfügungsbefugnis verlangt, schützt die Datenhehlerei de facto beliebige Daten. Damit scheint der Tatbestand ein strafbewehrtes Ausschließlichkeitsrecht an (auch wertlosen) in Daten manifestierten Informationen als Selbstzweck zu begründen.[22]

C. Verfassungswidrigkeit von § 202d StGB

Neben den aufgezeigten Schwächen der an den Strafnormen angelehnten Herleitung des „Dateneigentums" ergeben sich bei § 202d StGB noch weitere Probleme. Die Vorschrift ist wegen Verletzung der Pressefreiheit, der Berufsfreiheit sowie des Bestimmtheitsgrundsatzes verfassungswidrig.[23]

I. Verletzung der Pressefreiheit (Art. 5 Abs. 1 Satz 2 Alt. 1 GG)

1. Eingriff in den Schutzbereich durch Strafbarkeit von Pressetätigkeiten

§ 202d StGB stellt Verhaltensweisen unter Strafe, die unter den Schutzbereich der Pressefreiheit fallen und greift damit in deren Schutzbereich ein. Die Pressefreiheit gewährleistet in umfassender Weise die „Berichterstattung von der Beschaffung der Information bis zur Verbreitung der Nachricht und der Meinung".[24] Dabei ist auch der „prinzipiell ungehinderte Zugang zu Informationen" geschützt, denn nur dieser „versetzt die Medien in den Stand, die ihnen in der freiheitlichen Demokratie zukommende Funktion wahrzunehmen".[25] Zur Gewährleistung der der Presse zukommenden Kontroll- und Mittlerfunktion[26] muss sich der Schutz auch auf rechtswidrig erlangte Informationen erstrecken.[27]

---

22 *Stuckenberg*, ZIS 2016, 526, 530 f. („Recht am gedanklichen Inhalt" beliebiger Daten).

23 Unter dem Aktenzeichen 1 BvR 2821/16 ist eine Verfassungsbeschwerde gegen § 202d StGB anhängig, an der die Autoren dieses Beitrages als Mitverfasser mitgewirkt haben; vgl. dazu näher https://freiheitsrechte.org/datenhehlerei/ (zuletzt abgerufen am 22.6.2017).

24 BVerfGE 103, 44, 59.

25 BVerfGE 103, 44, 59.

26 Siehe bereits BVerfGE 20, 162, 175.

27 Vgl. BVerfGE 66, 116, 137 f. bzgl. der Meinungsfreiheit.

a. Strafbarkeit von Pressetätigkeiten

§ 202d Abs. 1 StGB sieht einen extrem weiten Tatbestand vor, der eine Vielzahl geschützter Tätigkeiten tatbestandlich erfasst. Bereits der objektive Tatbestand des § 202d Abs. 1 StGB beinhaltet mit Ausnahme des Ausschlusses von nicht allgemein zugänglichen Daten keine wirksamen Beschränkungen. Zwar muss nach §§ 202d Abs. 2 StGB i. V. m. § 11 Abs. 1 Nr. 5 StGB eine strafbare Vortat vorliegen.[28] Anders als bei der Sachhehlerei (§ 259 StGB), die als Vortat lediglich gegen das Vermögen gerichtete Straftaten erfasst, genügt für § 202d StGB jede strafbare Vortat. Brisante Informationen, die Journalisten von Whistleblowern und sonstigen Quellen erhalten, sind regelmäßig durch eine solche erlangt. Insbesondere Verstöße gegen §§ 44 Abs. 1 i. V. m. 43 Abs. 2 Nr. 1 BDSG, §§ 17 Abs. 1, 2 UWG oder §§ 202a, 203, 353b StGB kommen in Betracht. Weitere mögliche Vortaten sind Straftaten, die sich tatbestandlich nicht auf den Umgang mit Daten oder Informationen beziehen – etwa Diebstahl, Betrug oder Nötigung.[29] Auch die an § 202c Abs. 1 StGB angelehnten Tathandlungen des (Sich-)Verschaffens, des Überlassens sowie sonstigen Zugänglichmachens[30] in § 202d StGB erfassen praktisch jede Form des Umgangs mit Daten, die taugliche Tatobjekte sind.

Lediglich im subjektiven Tatbestand begrenzt § 202d StGB die Strafbarkeit auf mit Bereicherungs- oder Schädigungsabsicht vorgenommene Tathandlungen.[31] Eine (Dritt-)Bereicherungsabsicht liegt vor, wenn nach der Vorstellung des Täters die Tat auf die Erlangung eines (nicht notwendigerweise rechtswidrigen)[32] Vermögensvorteils für sich selbst oder einen Dritten gerichtet ist.[33] Erforderlich ist dolus directus 1. Grades.[34] Von der Pressefreiheit geschützte Personen handeln oftmals mit Bereicherungsab-

---

28 So auch einhellige Ansicht zu § 259 StGB, vgl. nur Müko/*Maier*, StGB, 2. Aufl. 2012, § 259 Rn. 19.

29 BT-Drs. 17/14362, S. 13; *Golla/von zur Mühlen*, JZ 2014, 668, 669.

30 Siehe umfassend LK/*Hilgendorf*, StGB, 12. Aufl. 2010, § 202c Rn. 22.

31 Die Merkmale sind entsprechend jenen in § 44 Abs. 1 BDSG auszulegen; BR-Drs. 249/15, S. 52.

32 Ganz h.M. bzgl. des wortgleichen Merkmals in § 203 Abs. 5 StGB, siehe *Lackner/Kühl,* StGB, 28. Aufl. 2014, § 203 Rn. 28; MüKo/*Cierniak*, StGB, 2. Aufl. 2012, § 203 Rn. 135 m.w.N.; a.A. NK/*Kargl*, StGB, 4. Aufl. 2013, § 203 Rn. 83.

33 BeckOK/*Holländer*, Datenschutzrecht (BDSG), 6. Edition 2013, § 44 Rn. 9; BR-Drs. 249/15, S. 52.

34 BR-Drs. 249/15, S. 52; *Singelnstein*, ZIS 2016, 432, 433.

sicht: Einem Journalisten oder anderen freien Mitarbeiter, der bei Recherche oder Publikationen auf Honorarbasis tätig wird, kommt es gerade darauf an, durch seine Tätigkeit einen Vorteil im Vermögenssaldo zu erzielen, sodass eine Absicht zur Selbstbereicherung vorliegt. Bei angestellten Journalisten kommt eine Drittbereicherungsabsicht in Betracht, wenn ein anderer Beteiligter (regelmäßig der Verlag) unmittelbare Vermögensvorteile aus Publikation oder Recherche zieht.[35]

Mit Schädigungsabsicht handelt eine Person, der es darauf ankommt, einem anderen durch die Verwirklichung des Tatbestandes einen Nachteil zuzufügen. Hierfür genügt es, dass die Schädigung ein notwendiges – wenn auch vom Täter nicht erstrebtes – Zwischenziel darstellt,[36] solange er die Schädigung nicht lediglich als „peinliche oder lästige Folge seines Handelns“[37] hinnimmt, weil er glaubt, sonst sein anderes Ziel zu verfehlen.[38] Ausreichend ist dolus directus 2. Grades. Als Schädigung genügen auch immaterielle Nachteile[39] wie beispielsweise Ehrverletzungen oder Bloßstellungen.[40] Investigative Presseveröffentlichungen decken oftmals reputationsschädigendes, weil rechtswidriges oder doch wenigstens sittlich missbilligtes, Verhalten auf und machen dieses bekannt. Die Veröffentlichung führt daher unweigerlich zu immateriellen Nachteilen der betroffenen Personen. Häufig werden Veröffentlichungen überdies auch nachteilige Vermögensauswirkungen mit sich ziehen, gerade wenn die Publikation Missstände bei gewerblich betriebenen Tätigkeiten betrifft.

b. Unzureichender Tatbestandsausschluss in § 202d Abs. 3 StGB

Die tatbestandliche Weite des § 202d StGB wird bzgl. presserechtlich geschützter Tätigkeiten durch den Tatbestandsausschluss in § 202d Abs. 3 StGB nur unzureichend begrenzt.

---

35 Vgl. Auernhammer/*v. Lewinski*, BDSG, 4. Aufl. 2014, § 44 Rn. 15 f.
36 Vgl. MüKo/*Hefendehl*, StGB, 2. Aufl. 2014, § 263 Rn. 792.
37 BGHSt 16, 1 f.
38 BeckOK/*Holländer*, Datenschutzrecht (BDSG), 6. Edition 2013, § 44 Rn. 11; vgl. BR- Drs. 249/15, S. 52.
39 Vgl. BR-Drs. 249/15, S. 52.
40 *Golla*, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, 2015, S. 183.

aa. Mangelnder Anwendungsbereich spezieller Ausschlusstatbestände

Nach § 202d Abs. 3 Satz 2 Nr. 2 StGB sind berufliche Handlungen der in § 53 Abs. 1 Nr. 5 StPO genannten Personen straflos. An diesem Verweis wird die gesetzgeberische Motivation deutlich, einen Gleichlauf zwischen dem vom Schutzbereich der Pressefreiheit erfassten und dem vom Tatbestandsausschluss erfassten Personenkreises herzustellen. Der verfassungsrechtliche Schutzbereichsmaßstab des BVerfG sieht einen Schutz der Pressefreiheit für diejenigen Personen und Verhaltensweisen vor, die einen inhaltlichen Bezug zum Presseergebnis aufweisen, der allerdings im Falle presseinterner Hilfstätigkeiten durch den organisatorischen Zusammenhalt des Presseunternehmens regelmäßig gegeben ist.[41]

Davon ausgehend sind diejenigen vom Tatbestandsausschluss erfasst, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken oder mitgewirkt haben. Hiervon werden alle in einem Pressebetrieb beruflich tätigen Personen erfasst.[42] Auch freiberufliche Journalisten sind umfasst, sofern und soweit sie dauerhaft dem Journalismus nachgehen.[43] Insoweit ist die vom Gesetzgeber bezweckte Kongruenz gewahrt. Rechtlich bedenklich verbleibt die in der Gesetzesbegründung vorgesehene Beschränkung des Tatbestandsausschlusses auf Handlungen, die „in Vorbereitung einer konkreten Veröffentlichung" erfolgen.[44] Nach diesem Kriterium wären Hintergrundrecherchen sowie Verifizierungen von Material, die der Entscheidung, ob eine konkrete Veröffentlichung überhaupt erfolgen soll, dienen, von dem Tatbestandsausschluss nicht erfasst.

Nebenberufliche Pressetätigkeiten sind nur erfasst, wenn die Absicht besteht „sie in gleicher Art zu wiederholen und sie dadurch, wenn auch

---

41 Siehe BVerfGE 77, 346, 354; den Schutz kraft organisatorischer Verknüpfung annehmend BVerfGE 25, 296, 304 bzgl. der Buchhaltung und BVerfGE 64, 108, 114 f. bzgl. des Anzeigenteils.

42 Satzger/Schluckebier/Widmaier/*Eschelbach*, StPO, 2. Aufl. 2016, § 53 Rn. 32; ähnlich Löwe/Rosenberg/*Ignor/Bertheau*, StPO, 26. Aufl. 2012, § 53 Rn. 54; *Meyer-Goßner/Schmitt*, StPO, 59. Aufl. 2016, § 53 Rn. 31.

43 Vgl. nur Löwe/Rosenberg/*Ignor/Bertheau*, StPO, 26. Aufl. 2012, § 53 Rn. 54; *Meyer-Goßner/Schmitt*, StPO, 59. Aufl. 2016, § 53 Rn. 31.

44 BT-Drs. 18/5088, S. 48 unter Verweis auf MüKo/*Hörnle*, StGB, 12. Aufl. 2012, § 184b Rn. 41.

nicht zu einer dauernden, so doch zu einer wiederkehrenden Beschäftigung zu machen".[45] Dadurch werden externe Hilfspersonen, die einem nicht pressebezogenen Beruf nachgehen und nur im Einzelfall unterstützend tätig werden, nicht von dem einfachrechtlichen Tatbestandsausschluss erfasst, obwohl die Tätigkeit nach verfassungsrechtlichen Maßstäben kraft Inhaltsbezugs zum Presseerzeugnis geschützt ist. Genau in diesen Fallgruppen zeigt sich die verfassungswidrige Divergenz zwischen dem auf Verfassungsebene geforderten und dem mangels Anwendbarkeit des Tatbestandsausschlusses auf einfachrechtlicher Ebene verwehrten Schutz. Diese Fallgruppe ist kein theoretisches Konstrukt, sondern betrifft eine erhebliche Anzahl von Personen.[46] So wenden sich Presseangehörige beispielsweise oft an externe Spezialisten, um vor einer geplanten Veröffentlichung Informationen zu erhalten, von Quellen erhaltene Informationen zu verifizieren oder technische Gegebenheiten auszuloten.

Insgesamt ist der Ausschluss damit besonders für nicht hauptberufliche Unterstützer von Pressetätigkeiten zu eng. Er genügt den Anforderungen der Pressefreiheit nicht und müsste zumindest verfassungskonform extensiv ausgelegt werden.

bb. Mangelnder Anwendungsbereich des allgemeinen Ausschlusstatbestands

Neben den in § 202d Abs. 3 Satz 2 StGB vorgesehenen speziellen Ausschlussgründen sieht § 202d Abs. 3 Satz 1 StGB einen Ausschlussgrund für Handlungen vor, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Nach der Gesetzesbegründung soll § 202d Abs. 3 StGB inhaltlich dem Tatbestandsausschluss in § 184b Abs. 5 StGB (Besitz kinderpornografischer Schriften) entsprechen.[47] Bei Berücksichtigung der dortigen Auslegung und Anwendung zeigt sich, dass die vom Gesetzgeber ausdrücklich vorgesehene Übertragung der einschränkenden Voraussetzungen des § 184b Abs. 5 StGB auf § 202d Abs. 3

45 BGHZ 7, 129, 130 mit Verweis auf RG DR 1943, 764 Nr. 30.

46 Siehe als Beispiel die Tätigkeit eines „Software-Reverse-Engineers", in: Heise Security, c't deckt auf: Kreditkarten-Betrug trotz Chip+PIN, abrufbar unter: https://www.heise.de/security/meldung/c-t-deckt-auf-Kreditkarten-Betrug-trotz-Chip-PIN-3080702.html (zuletzt abgerufen am 22.6.2017).

47 BT-Drs. 18/5088, S. 48.

StGB zu verfassungswidrigen Konsequenzen führt: Mag die dezidiert restriktive Formulierung und Handhabung des Ausschlusstatbestandes dort durchaus ihre Berechtigung haben, so führt sie im Kontext des § 202d StGB zu einer erheblichen Beschränkung der Pressefreiheit.

Für das aus § 184b Abs. 5 StGB übernommene Merkmal der „beruflichen Pflichtenerfüllung" gilt ein sehr enges Verständnis. Ein bloßer Zusammenhang zwischen Handlung und beruflicher Tätigkeit genügt nicht. Vielmehr muss eine – konkret normativ ableitbare – Pflicht zur Handlung bestehen.[48] Die Entscheidung über das „ob" und „wie" einer presserelevanten Tätigkeit ist aber ein verfassungsrechtlich verbürgtes Recht – diese Entscheidung kann nicht im Sinne einer beruflichen Pflicht vorgegeben sein.[49] Weiter einschränkend muss die Handlung der beruflichen Pflichterfüllung „dienen". Dies wird in § 184b Abs. 5 StGB restriktiv verstanden, sodass die Handlung zur Erfüllung der beruflichen Pflichten erforderlich sein muss. Übertragen auf § 202d StGB führt dies dazu, dass ein Journalist zur Inanspruchnahme der Straffreiheit substantiiert darlegen und begründen müsste, warum eine konkrete Materialbeschaffung und -sichtung für eine Veröffentlichung erforderlich (und nicht nur förderlich) war. Dafür müsste er in vielen Fällen Informationen über seine Quellen preisgeben. Ferner stellt sich oft erst nach der Datenbeschaffung und -sichtung und somit nach bereits vorgenommener tatbestandlicher Handlung heraus, ob die Daten genutzt werden können und mithin für eine Veröffentlichung erforderlich waren. Insoweit genügt der Tatbestandsausschluss nicht dem verfassungsrechtlichen Schutz der Pressefreiheit.

2. Eingriff durch Einschüchterungseffekte

Darüber hinaus ergibt sich ein weiterer, eigenständiger Eingriff in die Pressefreiheit daraus, dass § 202d StGB in mehrfacher Hinsicht Einschüchterungseffekte („chilling effects") hervorruft und dadurch die für

48 So LG Karlsruhe v. 28.5.2010, 2 KLs 310 Js 323/09, - juris - Rn. 13 unter Rekurs auf den verfassungsrechtlichen Aufgaben- und Pflichtenkreises eines Abgeordneten sowie bei OLG Frankfurt v. 2.11.2012, 2 Ws 114/12, - juris - Rn. 28 wo die berufliche Pflichtenerfüllung in Form der Weitergabe von tatbestandlich relevantem Material durch einen Anwalt an einen Gutachter zwecks Überprüfung eines zuvor erstellten Gutachtens unter Verweis auf die in § 147 StPO normierten anwaltlichen Rechte und Pflichten verneint wurde.

49 Vgl. BVerfGE 10, 118, 121; BVerfGE 91, 125, 134; BVerfGE 103, 44, 59.

die journalistische Tätigkeit unerlässliche und deshalb verfassungsrechtlich geschützte Beschaffung sowie eigenständige Prüfung von Informationen erschwert. Das BVerfG hat anerkannt, dass bereits die Möglichkeit, Adressat einer in die Grundrechte eingreifenden staatlichen Maßnahme zu sein, einen erheblichen und verfassungsrechtlich relevanten Einschüchterungseffekt haben kann.[50]

Einen solchen Einschüchterungseffekt hat § 202d StGB auf Journalisten, da ein Tatverdacht als Türöffner für strafprozessuale Ermittlungsmaßnahmen – insbesondere Durchsuchungen, Sicherstellungen und Beschlagnahmen – genutzt werden kann. Die Kombination aus weitem Tatbestand und engem Tatbestandsausschluss ist besonders brisant. Wegen des weiten Tatbestands lässt sich ein Anfangsverdacht leicht begründen. Der Tatbestandsausschluss hingegen wird in der Praxis kaum geeignet sein, Ermittlungsmaßnahmen abzuwenden. Ermittler können sich zu Recht darauf berufen, dass sich ohne Ermittlungsmaßnahmen gar nicht feststellen lässt, ob eine Handlung ausschließlich der Erfüllung beruflicher Pflichten gedient habe.[51]

Zusätzlich bewirkt § 202d StGB eine doppelte Einschüchterung von Informanten und Hilfspersonen und damit einen zusätzlichen Eingriff in die Pressefreiheit. Erstens können „potentielle Informanten durch die begründete Befürchtung, bei einer Durchsuchung (von Presseräumen) könnte ihre Identität festgestellt werden, davon abgehalten werden, Informationen zu liefern, die sie nur im Vertrauen auf die Wahrung ihrer Anonymität herauszugeben bereit sind.“[52] Zweitens wirkt sich die Gefahr der eigenen Strafbarkeit von nicht berufsmäßig handelnden Informanten und Hilfspersonen nach § 202d StGB negativ auf den Informationsfluss aus. Beide Einschüchterungseffekte betreffen unmittelbar die Pressefreiheit, denn diese soll gerade das Vertrauensverhältnis zwischen den Informanten/Hilfsper-

50 Allgemein BVerfGE 65, 1, 42; BVerfGE 113, 29, 46; BVerfGE 125, 260, 335: „diffuse Bedrohlichkeit“; näher zu Einschüchterungseffekten durch die Überwachung einer Versammlung auf potentiell Teilnahmewillige (BVerfGE 122, 342, 369), durch die Überwachung der Kommunikation zwischen Anwalt und Mandant auf zukünftige Mandanten (BVerfG v. 30.5.2007, 2 BvR 2094/05, NJW 2007, 2749, 2761) und durch die Durchsuchung von Redaktionsräumen auf die zukünftige journalistische Tätigkeit (BVerfGE 117, 244, 259).

51 Ob die Beschaffung und Auswertung im Vorfeld strafbar erlangter Daten zur beruflichen Pflichterfüllung erforderlich ist, kann schließlich erst nach Sichtung des Materials durch die Staatsanwaltschaft bewertet werden.

52 BVerfGE 117, 244, 259.

sonen und der Presse schützen, um einen stetigen Informationsfluss als Grundvoraussetzung für investigativen Journalismus zu ermöglichen.[53]

3. Verfassungsrechtliche Rechtfertigung

Die Strafbarkeit der nicht von dem Tatbestandsausschluss privilegierten Hilfspersonen sowie die Einschüchterungseffekte, die § 202d StGB erzeugt, stellen unverhältnismäßige Eingriffe in die Pressefreiheit dar. § 202d StGB soll die formelle Verfügungsbefugnis an Daten schützen.[54] Hierfür ist die Vorschrift allerdings – wie oben ausgeführt[55] – schon nicht geeignet. Es besteht nicht einmal die Möglichkeit der Zweckerreichung.[56]

§ 202d StGB ist jedenfalls zu deren Schutz auch nicht erforderlich, denn: Der Gesetzgeber hätte sein Ziel durch mildere Mittel erreichen können. Zunächst hätte er entsprechend des ursprünglichen Gesetzeszwecks[57] das Tatobjekt auf besonders schützenswerte Daten beschränken können (etwa „Zahlungsinformationen" oder „Zugangsdaten"). Auch eine Verlagerung von §§ 44 Abs. 1 i. V. m. 43 BDSG in das StGB unter Anpassung des Tatobjektes und ggf. der Tathandlungen wäre milder gewesen.[58] Jedenfalls hätte er den Tatbestandsausschluss weiter formulieren müssen, um die gegenwärtig nicht erfassten aber von der Pressefreiheit geschützten Personen einzugliedern und den Einschüchterungseffekten vorzubeugen.

In Anbetracht der herausragenden Bedeutung der Pressefreiheit, die „konstituierend für die freiheitliche demokratische Grundordnung"[59] und unbedingt zu schützen ist, und den von § 202d StGB ausgehenden massiven Beeinträchtigungen ohne wirksamen Rechtsgüterschutz, ist die Regelung auch unverhältnismäßig.

---

53 BVerfGE 117, 244, 259; vgl. bereits BVerfGE 20, 162, 176, 187; BVerfGE 36, 193, 204.

54 Siehe BT-Drs. 18/5088, S. 3, S. 26 f. und S. 46.

55 Vgl. oben B.II.

56 BVerfGE 120, 224, 240.

57 Nämlich den auf Webportalen und Foren stattfindenden Handel mit rechtswidrig erlangten digitalen Identitäten wie z. B. Kreditkartendaten oder Zugangsdaten zu Onlinebanking, E-Mail-Diensten oder sozialen Netzwerken zu unterbinden; BT-Drs. 17/14362, S. 1 f.

58 Vgl. hierzu *Golla*, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, 2015, S. 235 ff.

59 Vgl. BVerfGE 7, 198, 208; BVerfGE 77, 65, 74; BVerfGE 117, 244, 258.

II. Verletzung der Berufsfreiheit (Art. 12 Abs. 1 GG)

§ 202d StGB ist auch mit der verfassungsrechtlich geschützten Berufsfreiheit unvereinbar. Besonders Rechtsanwälte, die im Rahmen einer entgeltlichen Beratung in Kontakt mit tatbestandlich relevantem Datenmaterial kommen, sind Strafbarkeitsrisiken ausgesetzt. Nicht in Presseunternehmen eingegliederte Rechtsanwälte unterfallen nicht § 53 Abs. 1 Satz 1 Nr. 5 StPO und damit nicht dem Tatbestandsausschluss in § 202d Abs. 3 Satz 2 StGB. Aufgrund der restriktiven Formulierung und Auslegung des allgemeinen Ausschlusstatbestandes § 202d Abs. 3 Satz 1 StGB hilft auch dieser nicht ab.[60] Neben der eigenen möglichen Strafbarkeit wirkt sich zudem der von § 202d StGB ausgehende Einschüchterungseffekt in verfassungsrechtlich unvereinbarer Weise auf die Berufsfreiheit aus.

III. Verletzung des Bestimmtheitsgebots (Art. 103 Abs. 2 GG)

Der Gesetzgeber hat mangels hinreichend klarer Konturierung des § 202d StGB auch den strafrechtlichen Bestimmtheitsgrundsatz nach Art. 103 Abs. 2 GG missachtet. Demnach ist der Gesetzgeber gehalten, „die Voraussetzungen der Strafbarkeit so konkret zu umschreiben, dass Tragweite und Anwendungsbereich der Straftatbestände zu erkennen sind und sich durch Auslegung ermitteln lassen“.[61] Wann ein Verhalten mit Strafe bedroht ist, muss für den Normadressaten vorhersehbar sein.[62] § 202d Abs. 1 StGB ist ein weiter, nicht durch einen verfolgbaren Zweck weiter konkretisierbarer Tatbestand. Der Tatbestandsausschlusses in § 202d Abs. 3 ist unklar und eng formuliert sowie aufgrund seiner Verweisungstechnik[63] schwerlich fassbar.

---

60 Vgl. oben I.1.b.bb.

61 BVerfGE 47, 109, 120; BVerfGE 126, 170, 195; BVerfG v. 21.9.2016, 2 BvL 1/15, „Rindfleischetikettierung“, Rn. 38.

62 BVerfGE 92, 1, 12.

63 So beispielsweise die verwirrende Dopplung der Berufsmäßigkeit mit divergierenden Formulierungen („berufliche Tätigkeit“ in § 202d Abs. 3 Satz 2 Nr. 2 StGB, hingegen nur „berufliche Mitwirkung“ in § 53 Abs. 1 Satz 1 Nr. 5 StPO).

D. Fazit: Es bleibt spannend

Die Erfolgsaussichten der Verfassungsbeschwerde sind offen. Bisher zeigte sich das BVerfG bei der Verwerfung von Straftatbeständen zurückhaltend.[64] Die Verfassungsbeschwerde zur „Datenhehlerei" steht allerdings unter ihren eigenen besonderen Vorzeichen. Weil die Verletzung der Presse- und Rundfunkfreiheit zentrale Angriffspunkte sind, liegt die Beschwerde richtigerweise beim Ersten Senat und nicht bei dem für strafrechtliche Verfassungsbeschwerden üblicherweise zuständigen Zweiten Senat. Trotz der genannten erheblichen Mängel ist eine Aufhebung der Norm durch das BVerfG nicht unbedingt zu erwarten. Es wäre aber erfreulich, wenn Strafverfolgungsbehörden und Strafgerichten durch die Entscheidung eine einschränkende Auslegung und Anwendung der Norm vorgegeben werden würde.

Hierbei bestünde für den Ersten Senat auch Gelegenheit, sich im Lichte der aktuellen Diskussionen um ein „Dateneigentum" zu dem (straf-)rechtlichen Schutz der formellen Verfügungsbefugnis an Daten zu äußern. *Johannes Masing*, Richter des Ersten Senats, ließ in seinen Schriften im Zusammenhang mit dem Schutz freier Kommunikation bereits eine kritische Haltung zu der Anerkennung absoluter Verfügungsrechte an Daten erkennen.[65] Kommunikation sei gerade der „Austausch von Daten" nach den Prinzipien der „Unvorhersehbarkeit und Unbeherrschbarkeit, welches Handeln und welche Informationen von wem wie aufgegriffen, verarbei-

---

64 Eine jüngere Entscheidung (BVerfG v. 21.9.2016, 2 BvL 1/15, „Rindfleischetikettierung"), mit der der Zweite Senat eine Strafvorschrift wegen Unbestimmtheit für verfassungswidrig erklärte, könnte zwar auf eine künftig gegenüber dem Gesetzgeber etwas strengere Linie hindeuten. Allerdings ist die der Entscheidung zugrunde liegende Blankettproblematik im Zusammenhang mit unionsrechtlichen Verhaltensnormen mit den Problemen der „Datenhehlerei" nicht vergleichbar.

65 Vgl. im Zusammenhang mit personenbezogenen Daten *Masing*, NJW 2012, 2305, 2307 sowie jüngst *Masing*, Informationelle Selbstbestimmung – ein erstrebenswertes Ziel, Spektrum SPEZIAL, 1/2017, S. 69, 70 f.: Der verfassungsrechtliche Schutz der informationellen Selbstbestimmung bedeute nicht „frei über den Fluss der eigenen Daten verfügen zu können." „Der Gedanke eines Rechts, jederzeit autonom und widerruflich entscheiden zu können, welche Informationen unter welchen Bedingungen an welche Personen gelangen," sei „schon der Grundvorstellung nach irreführend."

tet, kombiniert und an andere verbreitet werden".[66] Auch vor diesem Hintergrund ist die Entscheidung mit Spannung abzuwarten.

Ganz unabhängig von der Beschwerde wird die Diskussion um die Schaffung eines „Dateneigentums" weitergehen und sich voraussichtlich auch erhitzen. Es ist zu hoffen und darauf hinzuwirken, dass die Politik besonnen vorgeht, wissenschaftliche Expertise hinzuzieht und den Dialog mit Vertretern der betroffenen Interessengruppen sucht. Letztlich handelt es sich um ein zukunftsweisendes Thema von globaler Tragweite. Die Regelung des Tatbestandes der „Datenhehlerei" kann hier nur als mahnendes Beispiel gelten für eine konzeptionell verunglückte und mit Blick auf die verfassungsrechtlich gewährleisteten Kommunikationsfreiheiten gefährliche Regelung des „Datenrechts".

66 *Masing*, Informationelle Selbstbestimmung – ein erstrebenswertes Ziel, Spektrum SPEZIAL, 1/2017, S. 69, 71.

Das dingliche Genussrecht des Erwerbers digitaler Werkexemplare

Linda Kuschel[*]

Bücher, Musik, Filme und Bilder werden seit geraumer Zeit nicht mehr nur analog erworben, sondern auch in digitaler Form. Solche digitalen Werkexemplare können sowohl auf einem körperlichen Träger, etwa einer CD oder DVD, als auch körperlos, z.B. per Download, erworben werden. Keineswegs handelt es sich hierbei um eine brandneue Technologie. Längst haben sich neue Geschäftsmodelle entwickelt, die digitalen Werkgenuss ermöglichen, ohne dass ein Erwerb des Werkexemplars stattfindet. Solche Geschäftsmodelle erlauben häufig den Zugang zu großen Datenbanken und verschiedensten Werken. Und dennoch ist bereits der vermeintlich simple Fall eines endgültigen Erwerbs digitaler Werkexemplare zum privaten Gebrauch dogmatisch kaum durchdrungen. Die rechtlichen Grundlagen, etwa die Frage nach dem Vertragstyp oder dem dinglichen Gegenstand des Vertrags, sind nach wie vor weitestgehend ungeklärt.[1] Im Rahmen dieses Beitrags wird der Frage nach der urheberrechtlichen Berechtigung nachgegangen, die der Erwerber eines digitalen Werkexemplars erlangt.

A. Vorüberlegungen

Um die dingliche Ebene eines Erwerbs digitaler Werkexemplare rechtlich einordnen zu können, ist zunächst die urheberrechtliche Relevanz des digitalen Werkgenusses zu betrachten.

Während bei analogen Werkexemplaren weder der Erwerb noch die private Nutzung urheberrechtliche Ausschließlichkeitsrechte berühren, ist

---

* LL.M. (Harvard). Die Autorin ist wissenschaftliche Mitarbeiterin von Prof. Dr. Katharina de la Durantaye, LL.M. (Yale), Humboldt-Universität zu Berlin.

1 Zu diesen Fragen ausführlich *Kuschel*, Der Erwerb digitaler Werkexemplare, erscheint voraussichtlich 2018.

dies im digitalen Bereich anders.[2] Bereits der Erwerb geht, wenn sich das Werkexemplar nicht schon auf einem Datenträger befindet, mit einer urheberrechtlich relevanten Vervielfältigung einher.[3] Und auch die Werkwiedergabe erfordert (zumindest kurzzeitige) Speicherungen, so dass ebenfalls das Vervielfältigungsrecht betroffen ist.[4]

Die urheberrechtlichen Schrankenbestimmungen decken diese Handlungen nicht vollständig ab. Die Privatkopieschranke nach § 53 Abs. 1 S. 1 UrhG etwa erlaubt ohne Einwilligung des Berechtigten nicht die vollständige Vervielfältigung von Büchern (§ 53 Abs. 4 lit. b UrhG). Zwar wird teilweise vorgeschlagen, diese Einschränkung nicht auf digitale Bücher anzuwenden, weil nur die vollständige Vervielfältigung von Druckwerken ausgeschlossen sein sollte.[5] Allerdings finden sich weder im Wortlaut noch in der Gesetzesbegründung Anhaltspunkte für eine entsprechende Reduktion. Die Gefahr, dass vollständig (privat) vervielfältigte Bücher den Primärmarkt gefährden, besteht bei E-Books ebenso wie im analogen Bereich.[6] Letztlich ist diese Gefährdung bei E-Books sogar präsenter, denn eine digitale Kopie kann zum einen schneller und zum anderen qualitativ hochwertiger angefertigt werden. Eine weitere Schrankenbestimmung, die im Zusammenhang mit Erwerb und Nutzung digitaler Werkexemplare eine wichtige Rolle spielt, ist § 69d Abs. 1 UrhG. Hiernach ist (u.a.) die Vervielfältigung von Computerprogrammen im Rahmen der „bestimmungsgemäßen Benutzung" durch den „zur Verwendung eines Vervielfältigungsstücks des Programms Berechtigten" zulässig. Durch die Begrenzung auf die Person des „Berechtigten" wird allerdings deutlich, dass die Vorschrift

2 Der Frage nach der „Freiheit des digitalen Werkgenusses" ist insbesondere *Sucker*, Der digitale Werkgenuss im Urheberrecht, 2014, eingehend nachgegangen. Vgl. auch *Lauber-Rönsberg*, Urheberrecht und Privatgebrauch, 2011.

3 Vgl. *Nieland*, Die Online-Lieferung im Urheberrecht, 2006, S. 199; *Poeppel*, Die Neuordnung der urheberrechtlichen Schranken im digitalen Umfeld, 2005, S. 77; *Wegner*, in: Berger/Wündisch, Urhebervertragsrecht, 2. Aufl. 2015, § 17 Rn. 12.

4 Vgl. Wandtke/Bullinger/*Heerma*, Praxiskommentar zum Urheberrecht, 4. Aufl. 2014, § 16 Rn. 16; *Imhof*, in: Bisges, Handbuch Urheberrecht, 2016, Kapitel 4 Rn. 128; *Redeker*, CR 2011, 634, 637; *Zech*, ZGE 2013, 368, 379.

5 *Kitz*, MMR 2001, 727, 729 f.; *Lauber-Rönsberg* (Fn. 2), S. 204; *Stieper*, AfP 2010, 217, 218 f.

6 So auch *Ganzhorn*, Rechtliche Betrachtung des Vertriebs und der Weitergabe digitaler Güter, 2015, S. 259.

keinen „urheberrechtsfreien Raum“ schafft, sondern stets an eine initiale Zustimmung des Rechtsinhabers anknüpft.[7]

Im Übrigen erscheint es inadäquat, den Erwerber auf die urheberrechtlichen Schranken zu verweisen. Denn zum einen können Schranken (zumindest mit schuldrechtlicher Wirkung)[8] durch vertragliche Bestimmungen oder technische Schutzmaßnahmen eingeengt werden. Zum anderen besteht – aus ökonomischer Perspektive – die Rechtfertigung der Schranken insbesondere darin, Freiräume für die Nutzung zu schaffen, wenn die Einholung einer individuellen Erlaubnis mit prohibitiv hohen Transaktionskosten verbunden wäre und dies zu einer Unternutzung des Werkes führt.[9] Im Falle des Erwerbs digitaler Werkexemplare treffen diese Erwägungen nicht zu. Der Erwerber schließt einen Vertrag und entrichtet (in der Regel) ein Entgelt, um das Werkexemplar nutzen zu dürfen. Es erscheint daher geboten, über ein dingliches Recht des Erwerbers zur Nutzung nachzudenken.

Es verwundert, dass die dingliche Ebene des Erwerbs digitaler Werkexemplare meist ausgeblendet wird. Der Erwerb wird stattdessen rein schuldrechtlich erklärt. Vertragsinhalt und Rechte des Erwerbers sollen vor allem über die AGB der Diensteanbieter bzw. über Endnutzer-Lizenzvereinbarungen festgelegt werden.[10] Dies führt allerdings zu einem Zirkelschluss, wenn eben diese Vertragsbedingungen auf ihre inhaltliche Zulässigkeit überprüft werden sollen. Wenn Gegenstand und Rechtsnatur des Vertrages nicht bereits unabhängig vom konkreten Einzelfall feststehen, fehlt es an einem Maßstab für die AGB-Kontrolle.[11]

Durch die Nichtbeachtung der dinglichen Ebene des Erwerbs digitaler Werkexemplare entsteht daneben ein urheberrechtliches Problem. Viele rechtswissenschaftliche Untersuchungen und gerichtliche Entscheidungen widmen sich der Frage nach der Verkehrsfähigkeit digitaler Inhalte, also

---

7 Zur dogmatischen Einordnung des § 69d Abs. 1 UrhG siehe *Lutz*, Softwarelizenzen und die Natur der Sache, 2009, S. 122 ff.

8 Vgl. hierzu *Stieper*, Rechtfertigung, Rechtsnatur und Disponibilität der Schranken des Urheberrechts, 2009, S. 213 ff.

9 Zu der ökonomischen Funktion von Schranken, Marktversagen zu beheben, siehe *Stieper* (Fn. 8), S. 84 ff.

10 OLG Hamm, NJW 2014, 3659, 3666.

11 Vgl. *Grübler*, Digitale Güter und Verbraucherschutz, 2010, S. 90; *Koch*, Computer-Vertragsrecht, 7. Aufl. 2009, S. 398 f.