

Schriften zum Strafrecht

Band 438

Das Rechtsgut der Datenhehlerei

Untersuchungen zu § 202d StGB

Von

Niklas Kindhäuser



Duncker & Humblot · Berlin

NIKLAS KINDHÄUSER

Das Rechtsgut der Datenhehlerei

Schriften zum Strafrecht

Band 438

Das Rechtsgut der Datenhehlerei

Untersuchungen zu § 202d StGB

Von

Niklas Kindhäuser



Duncker & Humblot · Berlin

Die Juristische Fakultät der Eberhard Karls Universität Tübingen
hat diese Arbeit im Jahre 2024 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

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

D21

Alle Rechte vorbehalten

© 2025 Duncker & Humblot GmbH, Berlin
Satz: Klaus-Dieter Voigt

Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 0558-9126

ISBN 978-3-428-19339-4 (Print)
ISBN 978-3-428-59339-2 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Verlagsanschrift: Duncker & Humblot GmbH, Carl-Heinrich-Becker-Weg 9,
12165 Berlin, Germany | E-Mail: info@duncker-humblot.de

Internet: <http://www.duncker-humblot.de>

Für Pia und Leander

Vorwort

Die vorliegende Arbeit wurde von der Juristischen Fakultät der Eberhard Karls Universität Tübingen im Sommersemester 2024 als Dissertation angenommen.

Mein besonderer Dank gilt meinem Doktorvater Herrn Prof. Dr. Dr. h.c. Bernd Heinrich für seine Unterstützung und viele wertvolle Anregungen und Diskussionen.

Herrn Prof. Dr. Jörg Eisele danke ich für die schnelle und wohlwollende Erstattung des Zweitgutachtens.

Zu Dank verpflichtet bin ich außerdem Herrn Prof. Dr. Dr. h.c. mult. Ulrich Sieber für die Ermöglichung der Nutzung der herausragenden Bibliothek des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg während der „Findungsphase“ meiner Arbeit.

Den Großteil der vorliegenden Arbeit habe ich neben meiner Tätigkeit als Strafverteidiger für die Kanzlei Feigen Graf verfasst. Meiner Kanzlei, insbesondere Herrn Dr. Walther Graf und Herrn Dr. Matthias Sartorius, danke ich für die Unterstützung und Geduld.

Meike van de Loo und Dr. Lukas Schefer danke ich für das sorgfältige Korrekturlesen des Manuskripts.

Meinen Eltern gilt in vielfältiger Hinsicht mein besonderer Dank für die Unterstützung und Förderung meines Studiums im Allgemeinen und dieser Arbeit im Besonderen.

Ganz besonders danke ich meiner Ehefrau Dr. Pia-Marie Hilsberg, nicht nur für ihre jahrelange Geduld und die inhaltliche und moralische Unterstützung, sondern auch den steten Zuspruch und die Beharrlichkeit, mit der sie an einen erfolgreichen Abschluss meiner Arbeit geglaubt hat. Ihr und unserem Sohn Leander ist dieses Buch gewidmet.

Bonn, im Juli 2024

Niklas Kindhäuser

Inhaltsverzeichnis

Einleitung	15
-------------------------	----

Teil 1

Grundlagen und Begriffsbestimmungen	19
§ 1 Überblick zur Normgenese	19
A. Vorgeschichte	19
B. Normtext	21
C. Zu den Motiven der Gesetzgebung	21
D. Verfassungsbeschwerde	23
§ 2 Rechtsgut	24
A. Der Begriff des Rechtsguts	25
I. Die Ansätze in der Literatur	26
1. Systemimmanenter Rechtsgutsbegriff	26
2. Systemkritischer Rechtsgutsbegriff	27
3. Ablehnung des Rechtsgutsbegriffs	28
II. Rechtsgutsbegriff und Verfassung	28
III. Konsequenzen: Bedeutung des Rechtsgutsbegriffs für die vorliegende Arbeit	29
B. Methodik zur Bestimmung des Rechtsguts	31
I. Die „Achillesferse“ der rechtsgutsbezogenen Auslegung	32
II. Subjektive und objektive Auslegung	35
C. Zusammenfassung: Hermeneutisch-methodischer (systemimmanenter) Rechtsgutsbegriff	37
§ 3 Anschlussdelikt	39
§ 4 Daten, Informationen und Geheimnisse	41
A. Computer- und Datenstrafrecht	41
B. Der Begriff der Daten im StGB	43
C. Informationsbegriffe	44
D. Daten und Informationen in der Informatik	46
E. Schlussfolgerungen	47
I. Semantische, syntaktische und strukturelle Informationen	47
II. Daten i. S. d. Datenschutzrechts	49

III.	Daten und Datenträger	51
1.	Datenträger als „notwendige Lebensbedingung“	51
2.	Verkörperung und digitale Daten	52
F.	Zur Zuordnung von Daten und Geheimnissen	54
I.	Einführung	54
II.	Mögliche Anknüpfungspunkte für die Zuordnung von Daten	56
III.	Die strafrechtliche Diskussion über die Zuordnung von Daten bei § 303a StGB	57
1.	Zum Tatbestand der Datenveränderung	57
2.	Zuordnungskriterien	58
3.	Unbeachtlichkeit semantischer Aspekte	60
4.	Rechte am Datenträger	61
5.	Skripturaktstheorie	62
a)	Strenge Skripturaktstheorie	63
b)	Modifizierte Skripturaktstheorie	64
6.	Wertungen des UrhG	64
7.	Stellungnahme	65
IV.	Zuordnung über den Zugang: Geheimnisse	66
1.	Geheimnisschutz	66
a)	Zum Begriff des Geheimnisses	67
b)	Die von Geheimnisschutznormen geschützten Rechtsgüter und die Zuordnung von Geheimnissen	68
2.	Formeller Geheimnisschutz (§ 202 StGB)	69

Teil 2

	Der Rechtsgüterschutz der Datenhehlerei	71
§ 5	Rechtsgutsbezeichnungen in der Begründung des Gesetzentwurfs	71
§ 6	Formelles Datengeheimnis	72
A.	Das „formelle Datengeheimnis“ bei §§ 202a, 202b, 202c StGB	72
I.	Rechtsgüterschutz bei § 202a StGB (Ausspähen von Daten)	72
1.	Überblick	72
2.	Merkmale des „formellen Datengeheimnisses“	76
a)	Besondere Sicherung und Überwindung der Sicherung	76
b)	§ 202a StGB als „elektronischer Hausfriedensbruch“	77
c)	Europa- und völkerrechtliche Vorgaben und Rahmenbedingungen	79
3.	Missverständliche Begrifflichkeiten im Schrifttum	81
a)	„Recht am gedanklichen Inhalt“	81
b)	„Besitz“	83

c) Zugänglichkeit der Information	83
4. Rechtsgutsträger und „Verfügungsbefugnis“: Zuordnung der Daten bei § 202a StGB	84
a) Ansichten im Schrifttum	84
b) Stellungnahme: Zuordnung des Geheimbereichs	85
aa) Unterschied zur Situation bei § 303a StGB	85
bb) Situation bei § 202 StGB	87
cc) Übertragung auf § 202a StGB	90
(1) Keine notwendige Reihenfolge von Datenspeicherung und Sicherung	90
(2) Kriterien für die Zuordnung des Geheimbereichs	94
(3) Übermittlung	95
5. Fazit	95
II. Rechtsgüterschutz bei § 202b StGB (Abfangen von Daten)	97
III. Rechtsgüterschutz bei § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten)	99
IV. Fazit und Schlussfolgerungen	100
B. Schutz „vor einer Aufrechterhaltung und Vertiefung“ der Verletzung: Perpetuierungstheorie	101
C. Formelles Datengeheimnis als Rechtsgut der Datenhehlerei?	102
I. Zum Tatbestand des § 202d Abs. 1 StGB	102
1. Anhaltspunkte für formellen Geheimnisschutz?	103
a) Merkmale formellen Geheimnisschutzes in anderen Normen ..	103
b) Daten, „die nicht allgemein zugänglich sind“	103
aa) Wortlaut	103
bb) Hinweise in den Gesetzesmaterialien	104
(1) Begründung in früheren Entwürfen	104
(2) Begründung des späteren Gesetzentwurfs	106
cc) Datenschutzrechtliches Begriffsverständnis	107
dd) Fazit	108
c) Tathandlungen	109
aa) Verschaffen, Überlassen, Zugänglichmachen	109
bb) Verbreiten	109
cc) Vergleich mit § 202c StGB	111
d) Bereicherungs- oder Schädigungsabsicht	112
e) Fazit	112
2. Anhaltspunkte für einen Perpetuierungstatbestand?	113
a) Vergleich mit § 259 StGB	113
aa) Vortat	113
bb) Tathandlungen	114
b) Loslösung von der Vortat	114

3. Fazit	115
II. Zur Stellung im Gesetz	115
III. Zum Konzept formellen Geheimnisschutzes durch das Anschlussdelikt	115
1. Zur Verletzung des formellen Datengeheimnisses durch die Vortat ..	116
a) Ausführungen und Beispiele in der Begründung	116
b) Überprüfung der Annahmen	117
2. Zur Perpetuierbarkeit einer Verletzung des formellen Datengeheimnisses durch die Vortat	120
a) Ausführungen in der Begründung des Gesetzentwurfs	120
b) Überprüfung der Annahmen	121
aa) Geheimbereich der Vortat	122
bb) Zuordnung der durch die Vortat erlangten Daten	125
(1) Verfügungsbefugter der Vortat?	125
(2) Zur Phänomenologie von Datenschwarzmärkten	127
(3) Schlussfolgerungen	129
(4) Vergleich mit § 202 StGB	130
(5) Verfügungsbeifugnis des von der semantischen Information Betroffenen	131
3. Konsequenzen	132
a) Gesetzesmaterialien und „Wille des Gesetzgebers“	132
b) Kontextualisierung des Fehlers der Begründung des Gesetzentwurfs	135
aa) Anderweitige Ausführungen in der Begründung des Gesetzentwurfs	135
(1) Siebers Gutachten zum 69. DJT	135
(2) „Schutzlücken“ bei § 17 Abs. 2 UWG a.F. und § 44 i.V.m. § 43 Abs. 2 Nr. 1, 3 BDSG a.F.	136
bb) Anhaltspunkte in der Genese des Gesetzes	138
IV. Ergebnis	140
§ 7 Allgemeine Sicherheitsinteressen	140
A. Argumente für und gegen die Gefährlichkeitstheorie bei § 259 StGB	141
B. Situation bei § 202d StGB	142
I. Strafmaß	142
II. Bereicherungsabsicht	143
III. Antragsdelikt	143
IV. Argumente in der Begründung des Gesetzentwurfs	143
C. Konsequenzen	144
§ 8 Materielles Datengeheimnis	145
A. Zum Tatbestand des § 202d Abs. 1 StGB	146
I. Daten	147

II.	Nicht allgemein zugänglich	147
III.	Vortäter	150
IV.	Tathandlung des „Verbreitens“	150
V.	Bereicherungs- oder Schädigungsabsicht	151
B.	Weitergabe und Verbreitung semantischer Informationen als Unrecht	151
C.	Zum Konzept materiellen Informationsschutzes durch das Anschlussdelikt	152
I.	Verletzter und Geheimhaltungsinteresse	152
II.	Bezug zur Vortat	154
1.	Vortaten	154
2.	Unmittelbarkeit, Datenkreationen, Ersatzhehlerei und „Sachidentität“	155
a)	Datenkreationen	156
b)	„Sachidentität“	159
aa)	Zu Wortlaut und Systematik	159
bb)	Zum „Schokoriegel“-Vergleich	161
D.	Ergebnis: Die Datenhehlerei als materielles Geheimnisschutzdelikt	164
§ 9	Schluss	165
Literaturverzeichnis		167
Stichwortverzeichnis		190

Einleitung

„Ich bin der Auffassung, dass, wenn mit Daten gehehlt wird, das nichts anderes ist, als wenn mit Sachen gehehlt wird. Deshalb haben wir einen entsprechenden Tatbestand geschaffen.“

So äußerte sich der damalige Bundesminister der Justiz und für Verbraucherschutz Heiko Maas im Deutschen Bundestag anlässlich der ersten Beratung des von den Fraktionen der CDU/CSU und SPD eingebrachten Entwurfs eines „Gesetzes zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“ am 12.06.2015 über einen Tatbestand der Datenhehlerei.¹

Mit Artikel 5 dieses Gesetzes wurde der Tatbestand der Datenhehlerei als § 202d in das Strafgesetzbuch² eingefügt.³ Die Datenhehlerei ist systematisch im Fünfzehnten Abschnitt des StGB verortet („Verletzung des persönlichen Lebens- und Geheimbereichs“) und folgt auf das Ausspähen (§ 202a StGB) und Abfangen von Daten (§ 202b StGB) sowie das Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB). Bei der Datenhehlerei handelt sich um ein Anschlussdelikt im Bereich des Computer- bzw. Datenstrafrechts⁴, das „Schlitzlücken“ der geltenden strafrechtlichen Regelungen schließen soll.⁵ Nach der Begründung des Gesetzentwurfs soll die Norm insbesondere den Online-Schwarzmarkthandel von Kreditkarten- und anderen ähnlich sensiblen Daten pönalisiieren.⁶

Der Tatbestand der Datenhehlerei ist der Hehlerei gem. § 259 StGB nachgebildet.⁷ Tatobjekt von § 202d StGB sind keine Sachen, sondern durch eine rechtswidrige Tat erlangte Daten, die der Datenhehler sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. Analog zur sog. Perpetuierungstheorie⁸ bei § 259 StGB soll die Datenhehlerei nach der Begründung des Gesetzentwurfs in erster Linie das durch die Vortat verletzte

¹ Maas, Plenarprotokoll 18/110, S. 10585 A.

² Im Folgenden: StGB.

³ BGBl. 2015 Teil I Nr. 51, S. 2218, 2227.

⁴ Vgl. zu diesen Begriffen unten § 4 A.

⁵ BT-Drs. 18/5088, S. 3, 25.

⁶ BT-Drs. 18/5088, S. 26.

⁷ Für eine vergleichende Gegenüberstellung der Tatbestände vgl. Berghäuser, JA 2017, S. 244; Tassi, DuD 2018, S. 165.

⁸ Vgl. unten § 6 B.

Rechtsgut des „formellen Datengeheimnisses“ vor einer „Aufrechterhaltung und Vertiefung dieser Verletzung“ schützen.⁹

Der Datenhehlerei wurde eine „bemerkenswerte Inkongruenz“ zwischen diesem erklärten gesetzgeberischen Ziel und der konkreten Ausgestaltung des Straftatbestands attestiert.¹⁰ § 202d StGB würde „in Analogie zur Sachhehlerei zu Unrecht als Perpetuierungsdelikt verstanden, das an den Strafraahmen der Vortat angebunden wird, obwohl dem Opfer hier nichts vorenthalten wird, was es wiedererlangen könnte“.¹¹

Die gesetzgeberische Idee einer Übertragung der Sachhehlerei in das Datenstrafrecht steht in einem besonderen Spannungsfeld. Die Übertragung von Konzepten aus „klassischen“ Delikten in Tatbestände des Datenstrafrechts wird vom Gesetzgeber regelmäßig praktiziert, ist aber – aufgrund der Besonderheiten immaterieller Güter – bereits im Ansatz problematisch.¹²

Die Zuordnung von Daten und Informationen ist ein in der Rechtswissenschaft intensiv diskutiertes Thema.¹³ Um ihre Bedeutung zu veranschaulichen, werden Daten metaphorisch etwa als das „neue Öl“¹⁴ oder „digitales Gold“¹⁵ bezeichnet.

Die Diskussion ist notwendig, da aufgrund der fortschreitenden Digitalisierung immer größerer Bereiche des menschlichen Lebens Daten in enormem – und stetig wachsendem – Umfang anfallen.¹⁶ Fragen der Zuordnung stellen sich somit fortwährend und eindringlich an das Recht als Mittel zur Konfliktlösung und zum Schutz von Interessen und Rechtsgütern.

⁹ BT-Drs. 18/5088, S. 26.

¹⁰ Verfassungsbeschwerde gegen die „Datenhehlerei“ vom 16.12.2016, S. 5.

¹¹ Stuckenberg, ZIS 2016, S. 526, 533.

¹² Vgl. Schuhr, ZIS 2012, S. 441ff.; Sieber, ZStW 103 (1991), S. 779, 787.

¹³ Vgl. nur Arkenau/Wübbelmann, Eigentum und Rechte an Daten: Wem gehören die Daten?, in: Internet der Dinge, S. 95ff.; Bartsch, in: FS Schneider, S. 297ff.; Berberich/Golla, PinG 2016, S. 165ff.; Determann, ZD 2018, S. 503ff.; Ensthaler, NJW 2016, S. 3473ff.; Fetzer, MMR 2015, S. 777ff.; Fezer, MMR 2017, S. 3ff.; Golla/Thess, Das Strafrecht als schlechtes Vorbild – Betrachtung zum „Dateneigentum“ und § 202d StGB, in: Immateriagüter und Digitalisierung, S. 9ff.; Grützmacher, CR 2016, S. 485ff.; Härtling, Acht Thesen zum „Dateneigentum“: CR-online.de Blog; Heymann, CR 2016, S. 650ff.; Hoeren, MMR 2013, S. 486ff.; ders., in: FS Schneider, S. 303ff.; Kornmeier/Baranowski, BB 2019, S. 1219ff.; Kühling/Sackmann, ZD 2020, S. 24ff.; Markendorf, ZD 2018, S. 409ff.; Röttgen, Rechtspositionen an Daten, in: Datenrecht in der Digitalisierung, § 4.2 Rn. 55ff.; Specht, CR 2016, S. 288ff.; dies., GRUR-Int 2017, S. 1040ff.; Thalhofer, GRUR-Prax 2017, S. 225ff.; Wagner, in: MüKo-BGB, 9. Aufl., § 823 Rn. 285ff.; Zech, CR 2015, S. 137ff.; Zurth/Lersch, ZfDR 2021, S. 175ff.

¹⁴ Berberich/Golla, PinG 2016, S. 165 Fn. 1 mit Verweis auf die Süddeutsche Zeitung vom 11.02.2014; Bußmann-Welsch/Tholey, InTeR 2020, S. 225; Dorner, CR 2014, S. 617, 618 zitiert entsprechend die ehemalige EU-Kommissarin für Verbraucherpolitik, Kuneva.

¹⁵ Lehmann, in: FS Schneider, S. 133.

¹⁶ Vgl. von Lewinski, Datenflut und Recht, S. 5ff.

Mit der Datenhehlerei hat der Gesetzgeber einen (weiteren) Straftatbestand geschaffen, der Kriterien für die Zuordnung von Daten voraussetzt, aber nicht definiert oder festlegt. Dem deutschen Recht im Allgemeinen und dem Strafrecht im Besonderen fehlt ein einheitliches gesetzliches System zur Zuordnung von Daten.¹⁷ Es existiert keine „primäre Normenordnung des allgemein erlaubten und verbotenen Umgangs mit Daten“.¹⁸ Rechte und Regelungen entsprechend Eigentum und Besitz bei Sachen i. S. v. § 90 BGB gibt es für Daten nicht. Die Zuordnung von Daten im deutschen Recht ist „zurzeit vollkommen unklar“.¹⁹ Seit Einführung der §§ 202a ff., 303a f. StGB durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) im Jahre 1986²⁰ und das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) im Jahre 2007²¹ hat sich die Strafrechtswissenschaft bemüht, die (straf-)rechtliche Zuordnung von Daten zu systematisieren.²²

Der Tatbestand der Datenhehlerei fügt der komplexen und andauernden Diskussion weitere Facetten hinzu.

Die vorliegende Arbeit widmet sich einer Untersuchung dieser teils neuen und teils altbekannten Problemkreise und adressiert sie im Kontext der Bestimmung des Rechtsgüterschutzes der Datenhehlerei.

Die Frage der Zuordnung von Daten stellt sich bei einem Anschlussdelikt in besonderer Weise, da sie an gleich zwei Stellen virulent werden kann: Die Zuordnung kann sowohl mit Blick auf die Vortat (der Tatbestand der Datenhehlerei setzt Daten voraus, die durch eine rechtswidrige Tat erlangt worden sind) als auch das Anschlussdelikt betrachtet werden. Ob die Zuordnung bei § 202d StGB der Vortat entspricht und wer als Rechtsgutsträger in Frage kommt, sind wichtige Aspekte der folgenden Untersuchung. Es sind Kriterien zu ermitteln, anhand derer der Verletzte der Datenhehlerei bestimmt werden kann.²³

¹⁷ Zum Begriff der Zuordnung von Daten vgl. unten § 4 F.

¹⁸ Stuckenberg, ZIS 2016, S. 526, 533; vgl. auch Hegmanns, in: FS Tolksdorf, S. 271, 275 („Einen eigenständigen und vor allem flächendeckenden Schutz genießen Daten als solche innerhalb der Rechtsordnung nicht“).

¹⁹ Hoeren, in: FS Schneider, S. 303.

²⁰ BGBl. 1986 Teil I Nr. 21, S. 721 ff.; vgl. die Überblicke bei Haft, NStZ 1987, S. 6 ff.; Lenckner/Winkelbauer, CR 1986, S. 483 ff.; Möhrenschlager, wistra 1986, S. 123 ff.; ders., wistra 1986, S. 128 ff.; Schlüchter, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, S. 56 ff.; Tiedemann, JZ 1986, S. 865, 868 ff.

²¹ BGBl. 2007 Teil I Nr. 38, S. 1786 ff.; vgl. die Überblicke bei Grösling/Höfinger, MMR 2007, S. 549 ff.; Schultz, DuD 2006, S. 778 ff.; Schumann, NStZ 2007, S. 675 ff.

²² Weshalb dem Computerstrafrecht Modellcharakter – insbesondere auch für das Zivilrecht – attestiert wird. Vgl. Zech, Information als Schutzgegenstand, S. 388.

²³ Die Bestimmung des Verletzten ist auch deshalb von praktischer Bedeutung, weil die Datenhehlerei ein relatives Antragsdelikt ist, § 205 Abs. 1 S. 2 StGB.