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.

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

„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 Strafgesetzbuch[2] 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. Datenstrafrechts[4], das „Schutzlücken" 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 pönalisieren.[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. Perpetuierungstheorie[8] 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 Strafrahmen 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. 441 ff.; *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. 95 ff.; *Bartsch*, in: FS Schneider, S. 297 ff.; *Berberich/Golla*, PinG 2016, S. 165 ff.; *Determann*, ZD 2018, S. 503 ff.; *Ensthaler*, NJW 2016, S. 3473 ff.; *Fetzer*, MMR 2015, S. 777 ff.; *Fezer*, MMR 2017, S. 3 ff.; *Golla/Thess*, Das Strafrecht als schlechtes Vorbild – Betrachtung zum „Dateneigentum“ und § 202d StGB, in: Immaterialgüter und Digitalisierung, S. 9 ff.; *Grützmacher*, CR 2016, S. 485 ff.; *Härting*, Acht Thesen zum „Dateneigentum“: CR-online.de Blog; *Heymann*, CR 2016, S. 650 ff.; *Hoeren*, MMR 2013, S. 486 ff.; *ders.*, in: FS Schneider, S. 303 ff.; *Kornmeier/Baranowski*, BB 2019, S. 1219 ff.; *Kühling/Sackmann*, ZD 2020, S. 24 ff.; *Markendorf*, ZD 2018, S. 409 ff.; *Röttgen*, Rechtspositionen an Daten, in: Datenrecht in der Digitalisierung, § 4.2 Rn. 55 ff.; *Specht*, CR 2016, S. 288 ff.; *dies.*, GRUR-Int 2017, S. 1040 ff.; *Thalhofer*, GRUR-Prax 2017, S. 225 ff.; *Wagner*, in: MüKo-BGB, 9. Aufl., § 823 Rn. 285 ff.; *Zech*, CR 2015, S. 137 ff.; *Zurth/Lersch*, ZfDR 2021, S. 175 ff.

[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. 5 ff.

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 1986[20] und das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) im Jahre 2007[21] 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 *Heghmanns*, 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 *Gröseling/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.