

Dr. iur. Lorenz Franck

## Datenhehlerei nach dem künftigen § 202d StGB

Am 27. Mai 2015 beschloss das Bundeskabinett den Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten. Neben den Vorschriften

zur Vorratsdatenspeicherung wird hierin ein neuer Straftatbestand der Datenhehlerei geschaffen.

### I. Tatbestand

Der neue Straftatbestand der Datenhehlerei schützt das sog. „formelle Datengeheimnis“, welches durch eine rechtswidrige Vortat bereits verletzt worden ist, vor einer Aufrechterhaltung und Vertiefung (sog. „Perpetuierung“) dieser Verletzung<sup>1</sup>. Der Entwurfstext<sup>2</sup> der Bundesregierung lautet konkret:

(1) Wer Daten (§ 202a Abs. 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Abs. 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
2. solche beruflichen Handlungen der in § 53 Abs. 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

Ursprünglich handelte es sich bei der Datenhehlerei um einen eigenständigen Gesetzentwurf. Das Land Hessen brachte einen entsprechenden Antrag bereits 2013 in den Bundesrat ein<sup>3</sup>. Die Frage, warum die Datenhehlerei nunmehr mit der Vorratsdatenspeicherung verknüpft wird, beantwortet das Bundesministerium für Justiz und Verbraucherschutz nur vage: Dem Anliegen, in einer immer stärker von Informations- und Kommunikationstechnologie geprägten Gesellschaft effektive Strafverfolgung zu ermöglichen, stehe die Notwendigkeit gegenüber, den strafrechtlichen Schutz von Informationssystemen und der in ihnen gespeicherten Daten vor Angriffen und Auspähungen ausreichend zu gewährleisten<sup>4</sup>. Es fällt jedoch zugegebenermaßen schwer, sich das Gegenüberstehen von Anliegen und Notwendigkeit bildlich vorzustellen<sup>5</sup>.

Seit dem 12. Juni 2015 befindet sich der Gesetzentwurf in der Beratungsphase. Während der ersten Lesung im Bundestag wurde die Datenhehlerei neben dem Großprojekt Vorratsdatenspeicherung nur stiefmütterlich behandelt<sup>6</sup>. Im September folgen voraussichtlich die zweite und dritte Lesung.

### II. Einzelerläuterungen

#### 1. Tatobjekt

Der Tatbestand der Datenhehlerei erfasst ausschließlich Daten im Sinne von § 202a StGB. Geschützt werden nicht sämtliche erdenklichen Informationen, sondern lediglich solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (§ 202a Abs. 2 StGB).

Einschränkend verlangt § 202d Abs. 1 StGB-E zudem, dass die Daten nicht allgemein zugänglich sind. Sofern die Daten aus allgemein zugänglichen Quellen entnommen werden können (nicht: entnommen wurden!), sei die formelle Verfügungsbefugnis nicht in strafwürdiger Weise beeinträchtigt<sup>7</sup>. Die Entscheidungsgewalt über die Preisgabe der Daten liegt insoweit nicht ausschließlich beim Berechtigten. Allgemein zugänglich sind Daten (entsprechend § 10 Abs. 5 S. 2 BDSG<sup>8</sup>), die jedermann mit oder ohne vorherige Anmeldung, Zulassung oder Entrichtung eines Entgelts nutzen kann.

#### 2. Vortat

Ausweislich des Wortlauts von § 202d Abs. 1 StGB-E kann jede rechtswidrige Tat taugliche Vortat einer Datenhehlerei sein. Hiermit sind ausschließlich Straftaten gemeint. Dies ergibt sich bereits aus der Verwendung des Begriffes „Tat“ als strafrechtlicher Grundfeste (vgl. § 11 Abs. 1 Nr. 5 StGB). Zudem ist das Strafmaß in § 202d Abs. 2 StGB-E durch dasjenige der Vortat gedeckelt. Anderweitig rechtswidriges Handeln, wie etwa eine datenschutzrechtliche Ordnungswidrigkeit, genügt hingegen nicht<sup>9</sup>.

Dies deckt sich mit der Intention der Bundesregierung: Die Sachhehlerei nach § 259 StGB betreffe nicht nur das verletzte Eigentum, indem sie den herbeigeführten rechtswidrigen Ver-

1 Regierungsentwurf (RegE) vom 27.05.2015, S. 28, online unter [http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE\\_Hoehchstspeicherfrist.pdf](http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE_Hoehchstspeicherfrist.pdf); zweifelnd hingegen Golla/von zur Mühlen, JZ 2014, 668, 670 f.

2 RegE (Fn. 1), S. 20.

3 BR-Drs. 284/13.

4 BMJV, Frage- und Antwortenpapier, S. 8, online unter [http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/20150527\\_FAQ\\_Hoehchstspeicherfrist.pdf](http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/20150527_FAQ_Hoehchstspeicherfrist.pdf).

5 Ähnlich ratlos EAID, Stellungnahme vom 25.5.2015, S. 7, online unter [http://www.eaid-berlin.de/wp-content/uploads/2015/05/EAID\\_Stellungnahme\\_GE\\_VDS\\_25\\_.pdf](http://www.eaid-berlin.de/wp-content/uploads/2015/05/EAID_Stellungnahme_GE_VDS_25_.pdf).

6 Gedächtnisprotokoll unter <https://netzpolitik.org/2015/live-blog-ersterlesung-zur-vorratsdatenspeicherung-im-bundestag/>.

7 RegE (Fn. 1), S. 29/54.

8 RegE (Fn. 1), S. 54.

mögenszustand perpetuiert, sondern auch das allgemeine Sicherheitsinteresse, welches durch den von der Hehlerei geschaffenen Anreiz zur Verübung von Vortaten beeinträchtigt werde<sup>10</sup>. Entsprechendes gelte für die Datenhehlerei.

Nicht aus dem Normtext, sondern lediglich aus dem Schutzzweck der Norm ergibt sich die Einschränkung, dass die Vortat zumindest auch die formelle Verfügungsbefugnis an den Daten schützen muss. Sind rein öffentliche Interessen durch die Vortat betroffen (wie etwa bei § 184d StGB<sup>11</sup>), bleibt für die Datenhehlerei kein Raum.

### 3. Tathandlungen

Datenhehler ist, wer die Daten sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. Die Begehungshandlungen unterscheiden sich von denjenigen der Sachhehlerei nach § 259 Abs. 1 StGB („... ankauft oder sonst sich oder einem Dritten verschafft, sie absetzt oder absetzen hilft“) und sind stattdessen an § 202c StGB angelehnt. Die Daten sind erst dann verschafft, wenn die tatsächliche Verfügungsmacht über sie erlangt wurde<sup>12</sup>. Für die Zugänglichmachung genügt bereits die Möglichkeit des Zugriffs auf die Daten<sup>13</sup>.

### 4. Ausnahmen

§ 202d Abs. 1 StGB-E gilt nicht für Handlungen, „die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen“. Exemplarisch führt Abs. 3 S. 2 Nr. 1 Handlungen von Amtsträgern oder deren Beauftragten auf, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen. Gemeint ist hierbei insbesondere der Ankauf illegal beschaffter Steuer-CDs<sup>14</sup>. Zu beachten ist allerdings, dass diese Ausnahme keinen datenschutzrechtlichen Erlaubnistatbestand im Sinne von § 4 Abs. 1 BDSG darstellt und auch nicht als Ausschließungsgrund für eine etwaige Strafbarkeit nach § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nrn. 1-5 BDSG bzw. entsprechenden landesdatenschutzrechtlichen Strafvorschriften herangezogen werden kann<sup>15</sup>.

§ 202d Abs. 3 S. 2 Nr. 1 StGB-E stellt berufliches Handeln der in § 53 Abs. 1 S. 1 Nr. 5 StPO genannten Personen frei, wenn durch sie Daten entgegengenommen, ausgewertet oder veröffentlicht werden. Die Vorschrift meint all diejenigen Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken. Der Passus ist nachträglich eingefügt worden und eine Reaktion auf befürchtete Einschränkungen der Pressefreiheit sowie den damit einhergehenden Verstoß gegen Art. 5 Abs. 1 S. 2 GG.

### 5. Vorsatz

Die Datenhehlerei kann nur vorsätzlich begangen werden (§ 15 StGB). Der Täter muss daher mindestens billigend in Kauf nehmen, dass die Daten nicht öffentlich zugänglich sind und aus einer rechtswidrigen Vortat stammen (sog. „dolus eventualis“). Er muss zudem die Absicht verfolgen, sich oder einen Dritten zu bereichern oder einen anderen zu schädigen (be-

sondere Form des Vorsatzes, sog. „dolus directus“). Die Schädigungsabsicht umfasst nicht nur materielle, sondern auch immaterielle Schäden.

### 6. Strafmaß

Die Tat soll mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft werden. Die Strafdrohung orientiert sich damit am Ausspähen von Daten nach § 202a StGB und liegt im oberen Bereich der im 15. Abschnitt („Verletzung des persönlichen Lebens- und Geheimbereichs“, §§ 201-206 StGB) ausgeworfenen Sanktionen. Die Strafe darf allerdings gem. § 202d Abs. 2 StGB-E nicht schwerer sein als die für die Vortat angedrohte Strafe. Bei der Strafzumessung wägt das Gericht die Umstände ab, die für und gegen den Täter sprechen (§ 46 Abs. 2 StGB).

### 7. Versuchsstrafbarkeit

Gemäß § 23 Abs. 1 StGB ist der Versuch eines Vergehens im Sinne von § 12 Abs. 2 StGB nur dann strafbar, wenn das Gesetz dies ausdrücklich vorgibt. Eine Versuchsstrafbarkeit der Datenhehlerei ist im aktuellen Entwurf nicht mehr enthalten<sup>16</sup>.

### 8. Strafantrag

Nach § 205 Abs. 1 S. 2 StGB-E wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält<sup>17</sup>. Antragsberechtigt ist gem. § 77 Abs. 1 StGB nur der Verletzte selbst<sup>18</sup>. Sind mehrere Personen antragsberechtigt, so kann jeder den Antrag selbständig stellen (§ 77 Abs. 4 StGB).

### 9. Konkurrenzen

Eine Beteiligung (Anstiftung, § 26 StGB; Beihilfe, § 27 StGB) an der Vortat oder gar Mittäterschaft (§ 25 Abs. 2 StGB) dürfte ausscheiden, da die Vortat zum Zeitpunkt der Hehlerei bereits beendet sein wird. Mittäterschaft und Teilnahme sind hingegen bei Folgetaten denkbar.

Die Weitervermittlung gestohlener Daten steht an sich bereits gem. § 202c Abs. 1 Nr. 1 StGB unter Strafe, sofern es sich um Passwörter oder sonstige Sicherungscodes handelt und dadurch eine weitere Straftat nach den §§ 202a, 202b StGB vorbereitet wird.

Der Handel mit Geschäfts- und Betriebsgeheimnissen ist gem. § 17 Abs. 2 UWG umfassend mit Strafe bedroht. Der Regierungsentwurf übersieht insoweit, dass es dem Täter

9 RegE (Fn. 1), S. 55.

10 RegE (Fn. 1), S. 29.

11 RegE (Fn. 1), S. 54.

12 RegE (Fn. 1), S. 55.

13 Graf, in: Münchener Kommentar StGB, Bd. 4., 2. Aufl. 2012, § 202c Rn. 23.

14 Vgl. BVerfG, Beschl. v. 9.11.2010, Az. 2 BvR 2101/09, online unter <http://dejure.org/2010,53>; mit guten Gründen gegen einen entsprechenden Ausnahmetatbestand Klengel/Gans, ZRP 2013, 16, 17 ff.

15 A.A. wohl EAID, Stellungnahme (Fn. 5), S. 12.

16 Anders zuvor Abs. 4 des Entwurfs, BR-Drs. 284/13, S. 2 bzw. BT-Drs. 18/1288, S. 8.

17 RegE (Fn. 1), S. 21.

18 Vgl. anders im BDSG, § 44 Abs. 2 S. 2 („der Betroffene, die verantwortliche Stelle, der BfDI und die Aufsichtsbehörde“).

nach § 17 Abs. 2 Nr. 2 UWG durchaus möglich ist, auf rechtswidrige Vortaten Dritter aufzubauen.

Die unerlaubte Vervielfältigung und die gewerbsmäßige Verwertung urheberrechtlich geschützter Werke werden von den §§ 106 ff. UrhG erfasst. Dies gilt unabhängig davon, ob die Werke öffentlich zugänglich sind oder nicht.

Der illegale Handel mit personenbezogenen Daten unterfällt § 44 Abs. 1 iVm § 43 Abs. 2 Nrn. 1-5 BDSG bzw. landesrechtlichen Datenschutzvorschriften<sup>19</sup>.

An Begünstigung nach § 257 StGB und ggf. Strafvereitelung nach § 258 StGB ist ebenfalls zu denken.

Beschafft sich der Täter die Daten, um selbst eine weitere Straftat (z.B. Betrug, § 263 StGB; Computerbetrug, § 263a StGB) zu begehen, dürfte es sich bei der Datenhehlerei um eine mitbestrafte Vortat handeln. Sieht der Täter unterdessen reuig von der Verwirklichung der Nachtat ab, stellt § 202d StGB-E eine Ausweitung der Vorfeldstrafbarkeit dar.

### III. Kritik

#### 1. Strafbarkeitslücken

In der Entwurfsbegründung werden Strafbarkeitslücken angeführt, die die Schaffung einer neuen Strafnorm erforderlich machten<sup>20</sup>. Eine Strafbarkeitslücke ist jedoch nicht bereits deswegen gegeben, weil ein bestimmtes missbilligtes Verhalten nicht unter Strafe steht. Insoweit ist das gesamte Strafrecht auf Lückenhaftigkeit angelegt (vgl. Art. 103 Abs. 2 GG, § 1 StGB, „nulla poena sine lege“). Inwieweit die oben in Pkt. II. 3. genannten bestehenden einschlägigen Deliktsarten nicht geeignet sein sollen, die Weitergabe illegal beschaffter Daten wirksam zu unterbinden, wurde durch die Bundesregierung zu keinem Zeitpunkt belegt<sup>21</sup>. Es bedarf einiger Geistesanstrengung, einen Fall zu konstruieren, der nicht bereits von § 44 BDSG bzw. § 17 UWG erfasst ist, aber dennoch uneingeschränkt strafwürdig erscheint. So bleibt es vorerst bei der Note Montesquieues: „Wenn es nicht notwendig ist, ein Gesetz zu machen, dann ist es notwendig, kein Gesetz zu machen.“

#### 2. Presse- und Wissenschaftsfreiheit

Die Pressefreiheit stellt eines der wertvollsten Güter in einem demokratischen Rechtsstaat dar. Der Entwurfstext der Bundesregierung enthält mittlerweile immerhin eine Tatbestandsausnahme für „ausschließlich berufliche Pflichten“ von Journalisten und Reportern<sup>22</sup>. Dieser Passus erfordert jedoch Nachbesserung.

Unklar ist einerseits, was Journalismus zum Beruf im Sinne der Vorschrift qualifiziert. Immerhin ist gerichtlich festgestellt, dass der Besitz eines Presseausweises nicht Voraussetzung ist, um die Segnungen des Art. 5 Abs. 1 S. 2 GG zu empfangen<sup>23</sup>. Fraglich ist aber, ob sich auch Blogger, Podcaster und Whistleblower-Plattformen mit redaktionellem Unterbau auf die Ausnahme in § 202d Abs. 3 Nr. 2 StGB-E berufen dürfen.

Unklar ist ferner, was genau eine berufliche Pflicht insbesondere bei Freiberuflern ausmacht. Zwar stellt der Regierungsentwurf fest, dass auch selbstaufgelegte Pflichten genügen sollen<sup>24</sup>, handhabbarer wird die Vorschrift dadurch jedoch nicht. Die Dogmatik zum ähnlich lautenden § 184b Abs. 5 Nr. 3

StGB fordert außerdem eine journalistische Tätigkeit im Zusammenhang mit einer konkreten Veröffentlichung<sup>25</sup>. Ein Journalist, der Daten zugspielt bekommt, kann jedoch erst nach der Sichtung wirklich beurteilen, ob daraus eine Veröffentlichung werden soll. Aus ebenjenem Grund trifft der Entwurf vielfach auf Ablehnung<sup>26</sup>.

Die wissenschaftliche Forschung nach Art. 5 Abs. 3 S. 1 GG findet überhaupt keine Berücksichtigung in § 202d Abs. 3 StGB-E<sup>27</sup>. Sicherheitsforscher werden sich insoweit in der Beweisnot wiederfinden, dass sie die tatbestandliche Handlung nicht mit Bereicherungs- oder Schädigungsabsicht vorgenommen haben<sup>28</sup>. Eine ähnlich beschämende Situation trat zuvor schon bei Einführung des § 202c StGB auf.

#### 3. Rechtsunsicherheit

Die stillschweigende Beschränkung möglicher Vortaten auf solche, die zumindest auch die formelle Verfügungsgewalt schützen<sup>29</sup>, schafft Rechtsunsicherheit und ist dem juristischen Laien kaum zuzumuten. Hier findet sich ein unnötiges Einfallsort für Tatbestands- und Verbotsirrtümer nach den §§ 16 f. StGB<sup>30</sup>.

Völlig irreführend ist schließlich die Vorstellung der Bundesregierung, der datenschutzrechtlich Betroffene könne sich gemäß § 202d Abs. 1 StGB-E strafbar machen, wenn er Daten vom Vortäter erhält<sup>31</sup>. Der Betroffene dürfte kaum Schädigungs- oder Bereicherungsabsicht aufweisen. Abgesehen davon besitzt er ein Arsenal an Auskunfts- und Einsichtsrechten<sup>32</sup>, das er gegen die verantwortliche Stelle und damit den formell Verfügungsberechtigten ins Feld führen kann. Die Situation gleicht ihm gegenüber eher derjenigen bei öffentlich zugänglichen Daten<sup>33</sup>. Der Verletzte hat gegenüber dem datenschutzrechtlich Betroffenen kein ausschließliches Verfügungsrecht über die Daten. Der Verweis der Bundesregierung auf § 202a StGB<sup>34</sup> verkennt insoweit den strukturellen Unterschied zwischen Vortat und Perpetuierungsdelikt.

19 Diese sind z.T. subsidiär ausgestaltet, vgl. § 33 Abs. 2 DSG NRW.

20 RegE (Fn. 1), S. 27 f.; ebenso zuvor der 69. Deutsche Juristentag, Beschlüsse vom 18. bis 21.09.2012, S. 9.

21 Ebenso Golla/von zur Mühlen, JZ 2014, 668, 671 ff.

22 Anders zuvor Abs. 5 in BR-Drs. 284/13, S. 2 bzw. BT-Drs. 18/1288, S. 8.

23 VG Lüneburg, Urt. v. 22.05.2014, Az. 5 A 120/13.

24 RegE (Fn. 1), S. 57.

25 Hörnle, in: Münchener Kommentar StGB, Bd. 3, 2. Aufl. 2012, § 184b Rn. 41.

26 DAV, Pressemitteilung vom 21.5.2015, online unter <http://anwaltverein.de/de/newsroom/pm-17-15-dav-lehnt-vorratsdatenspeicherung-ab>; EAID, Stellungnahme (Fn. 5), S. 13; Härting, <http://www.cr-online.de/blog/2015/05/18/indiskretionen-werden-zur-strafbaren-datenhehlerei/>.

27 In § 184b Abs. 5 StGB ist sie hingegen enthalten, vgl. Hörnle in: Münchener Kommentar StGB, Bd. 3, 2. Aufl. 2012, § 184b Rn. 41.

28 Zur Tatbestandskorrektur auf subjektiver Ebene zugunsten von Journalisten bereits Golla/von zur Mühlen, JZ 2014, 668, 669.

29 Siehe oben Pkt. II. 2.

30 Die fehlende Bestimmtheit rügen auch Golla/von zur Mühlen, JZ 2014, 668, 670.

31 So ausdrücklich RegE (Fn. 1), S. 55.

32 Überblick bei Franck, RDV 2015, 137, 139 ff.

33 Siehe oben Pkt. II. 1.

34 RegE (Fn. 1), S. 55.

#### IV. Zusammenfassung

Der Gesetzentwurf zur Datenhehlerei ist unsauber gearbeitet und unzureichend begründet. Behauptete Strafbarkeitslücken sind keineswegs nachgewiesen, die Erforderlichkeit der Vorschrift steht damit insgesamt in Frage. Die verfassungsrechtlich verbriefte Pressefreiheit von nebenberuflichen und Amateurjournalisten wird in unzulässiger Weise eingeschränkt, hauptberufliche Journalisten werden mit rechtlichen Unwägbarkeiten konfrontiert. Insgesamt kann der Regierungsentwurf nur als fehlgeschlagener Versuch bewertet werden.



#### Dr. Lorenz Franck

Mitarbeiter der GDD-Geschäftsstelle sowie Lehrbeauftragter für Datenschutzrecht an der Fachhochschule Köln.