

# Steueranwalt 2010/2011

von

Michael Schwarz, Martin Wulf, Martin Strahl, Jürgen Wessing, Jürgen Wagner, Johanna Hey, Helga Opitz, Gerhard Michel, Christoph Schlieff, Burkhard Binnewies, Arbeitsgemeinschaft Steuerrecht im DAV

1. Auflage

[Steueranwalt 2010/2011 – Schwarz / Wulf / Strahl / et al.](#)

schnell und portofrei erhältlich bei [beck-shop.de](#) DIE FACHBUCHHANDLUNG

Thematische Gliederung:

[Steuerrecht](#)

Boorberg Stuttgart/München 2011

Verlag C.H. Beck im Internet:

[www.beck.de](http://www.beck.de)

ISBN 978 3 415 04661 0

# Ankauf und Verwertung gespeicherter und geklauter Bankdaten durch Bund und Länder – „Contra“

Rechtsanwalt Prof. Dr. Jürgen Wessing, Düsseldorf

## I. Einleitung

Der Ankauf von den Kreditinstituten gestohlenen Daten deutscher Kunden, erst liechtensteinischer und jetzt Schweizer Banken, bewegt die Gemüter der gesamten Öffentlichkeit und darüber hinaus der Fachwelt. Beleg dafür sind eine ausführliche Berichterstattung in den Medien sowie eine intensive fachliche Debatte, die in einer stetig steigenden Zahl von Publikationen in juristischen Zeitschriften und – wie hier beim Steueranwaltstag 2010 – auf Tagungen geführt wird. Bei der Bewertung der Vorgänge stehen sich zwei Fundamentalpositionen gegenüber. Die Einen melden rechtsstaatliche Bedenken an, beklagen Rechtsbrüche der Behörden und stehen auf dem Standpunkt, dass der Zweck nicht alle Mittel heiligen darf. Die Anderen betonen die Pflicht des Staates zur Aufklärung von Straftaten und der Verfolgung von Straftätern. In Zeiten wirtschaftlicher Krisen und unsicherer Steuereinnahmen spielen zudem fiskalische Interessen eine große Rolle. Nicht zu unterschätzen sind die Sanktionsbedürfnisse in der Öffentlichkeit und die Rufe nach einer konsequenteren Bestrafung von prominenten beziehungsweise wohlhabenden Straftätern. Wie bei wenigen anderen Themen wird die Diskussion über die staatlichen Datenaufkäufe durch das Zusammentreffen von rechtlichen, politischen und moralischen Fragen geprägt.

## II. Chronologie des staatlichen Datenankaufs

Als Überblick und Grundlage der rechtlichen Bewertung wird hier eine komprimierte Chronologie der staatlichen Datenankäufe präsentiert:

Den Auftakt in der jüngeren Vergangenheit bildete das Batliner-Verfahren.<sup>1</sup> Im Jahre 2000 ging bei der Bochumer Staatsanwaltschaft anonym eine CD-ROM mit Internetaufzeichnungen über Stiftungen von Kunden des Liechtensteiner Treuhänders Herbert Batliner ein. Ehemalige Mitarbeiter von Batliner hatten die Kundendaten gestohlen. Die auf der CD enthaltenen Daten waren Auslöser für Steuerstrafverfahren in großem Umfang gegen teils prominente Beschul-

---

<sup>1</sup> Siehe dazu auch den Überblick bei *Spatscheck*, Wird Gauner, wer mit Gaunern dealt?, in: Festschrift für Klaus Volk, München 2009, S. 771 f.

digte. Die Staatsanwaltschaft Bochum stieß auf 200 Millionen Euro Schwarzgeld. Weit über 100 Verfahren wegen Steuerhinterziehung wurden rechtskräftig abgeschlossen.

Es folgte das Rostocker LLB-Verfahren. Vier Männer gelangten im Jahre 2005 auf ungeklärte Weise in den Besitz von Kontenbelegen deutscher Kunden der Liechtensteinischen Landesbank (LLB). Die Kontenbelege hatte zuvor ein Mitarbeiter der LLB kopiert. Die Männer boten die Kontenbelege der LLB gegen Millionensummen zum Rückkauf an. Nachdem die LLB einen Teil ihrer Belege zurückgekauft hatte, wurden die Männer vor der bevorstehenden Übergabe weiterer Belege verhaftet und vor dem LG Rostock wegen Erpressung angeklagt. Während des Verfahrens übergab die Verteidigung eines der Angeklagten Gericht und Staatsanwaltschaft Datensätze der LLB, die zu mehr als 1.800 deutschen Kunden gehörten. Zu Geldzahlungen als Gegenleistung kam es nicht. Die Staatsanwaltschaft Rostock gab die Unterlagen an die Steuerfahndungen weiter.<sup>2</sup>

Der nächste Schritt waren die 2008 eingeleiteten LGT-Verfahren, die sich aufgrund der Bilder von der Festnahme des prominentesten Beschuldigten, des ehemaligen Post-Chefs Klaus Zumwinkel, in das kollektive Gedächtnis eingepreßt haben. Heinrich Kieber, ein früherer Mitarbeiter der LGT, hatte Kundendaten heimlich kopiert. Nachdem er zunächst vergeblich versucht hatte, das liechtensteinische Fürstenhaus als Eigner der LGT zu erpressen, bot er die kopierten Daten im Jahre 2006 dem Bundesnachrichtendienst (BND) an. Nach ersten „Probefieferungen“ an den BND und die Wuppertaler Steuerfahndung hat Kieber im Jahre 2007 mehrere DVDs mit Angaben zu 4.000 Steuerpflichtigen übergeben. Hierfür soll Kieber auf Rechnung der Steuerbehörden einen vom BND vorfinanzierten Betrag von 4,2 Millionen Euro erhalten haben.<sup>3</sup>

Betroffen von der Weitergabe von Kundendaten war in den letzten Jahren auch das Bankhaus Julius Bär. Ein ehemaliger Mitarbeiter, von dem sich das Institut im Streit getrennt hatte, gab Informationen über Schwarzgeld an die Behörden der USA, der Schweiz und Deutschlands weiter. Eine Bezahlung erhielt er hierfür nicht.<sup>4</sup>

In dem aktuellen Schweizer Fall bot ein unbekannter Informant der Wuppertaler Steuerfahndung eine CD mit circa 1.500 Namen deutscher Kunden

---

2 Sachverhaltschilderung bei *Spatscheck* (o. Fn. 1), S. 773.

3 Vgl. *Kölbel*, NStZ 2008, 241; *Spatscheck* (o. Fn. 1), S. 773ff.; *Trüg/Habetha*, NJW 2008, 887.

4 Siehe wiederum die Sachverhaltsschilderung bei *Spatscheck* (o. Fn. 1), S. 775.

der Credit Suisse zum Kauf an.<sup>5</sup> Die ersten von der Steuerfahndung durchgeführten Stichproben ergaben Volltreffer. Die Bundesregierung sprach sich frühzeitig – und wohl einer verbreiteten Erwartungshaltung entsprechend – für einen Ankauf der CD aus. Der Informant soll ein Entgelt von 2,5 Millionen Euro erhalten haben. Die Medienberichte über den Datenaufkauf führten zu einer Flut von Selbstanzeigen. Dadurch sollen Steuermehreinnahmen von circa 400 Millionen Euro in die Kassen gespült worden sein. Seitdem kursieren Berichte über weitere Datenaufkäufe.<sup>6</sup>

Der Schweizer Fall wird als Grundlage für die folgende rechtliche Bewertung genommen. Es wird davon ausgegangen, dass es sich bei dem Informanten um einen Mitarbeiter der betroffenen Schweizer Bank handelt.

### III. Materiell-rechtliche Strafbarkeit

Vom Kopieren der Daten bis zum Verwerten durch die Steuerfahndung ist es ein langer, auch juristisch langer Weg, der im Einzelnen aufzuzeigen ist.<sup>7</sup>

#### 1. Kopieren und Anbieten der Kundendaten durch den Informanten

##### a) Strafbarkeit nach deutschem Strafrecht

###### aa) Diebstahl (§ 242 StGB) und Ausspähen von Daten (§ 202 a StGB)

Es wird davon ausgegangen, dass der Informant die Daten auf einen ihm gehörenden Datenträger kopiert hat. Damit scheidet eine Sache – d. h. ein körperlicher Gegenstand – als Tatobjekt voraussetzender Tatbestand des Diebstahls (§ 242 StGB) aus; die Daten selbst sind keine Sachen.

Der Tatbestand des Ausspähens von Daten (§ 202 a StGB) erfordert zum einen, dass die Daten nicht für den Täter bestimmt sind. Zum anderen muss sich der Täter Zugang zu den Daten unter Überwindung einer besonderen Zugangssicherung verschafft haben. An beiden Voraussetzungen fehlt es, wenn es sich bei dem Informanten um einen Mitarbeiter der betroffenen Bank handelte und die Betreuung der Konten deutscher Kunden zu seinem Aufgabenkreis gehörte. Die pflichtwidrige Verwendung dienstlich zur Verfügung stehender Daten erfüllt den Tatbestand des § 202 a StGB nicht.<sup>8</sup> Gleich-

---

5 Es wird davon ausgegangen, dass dem kundigen Leser die Vorfälle aus der Berichterstattung in den Medien vertraut sind. Daher wird auf Nachweise verzichtet; siehe nur die kurze Sachverhaltsmitteilung bei *Ostendorf*, ZIS 2010, 301.

6 Siehe zuletzt beispielsweise die Meldung im FOCUS, Heft 40/2010, S. 204.

7 So auch übersichtlich *Ostendorf*, ZIS 2010, 301, 302 ff.

8 *Fischer*, Strafgesetzbuch, 57. Aufl. 2010, § 202 a Rn. 7.

ches gilt für Verstöße gegen Verbote und Anweisungen des Verfügungsberechtigten (hier der Bank).<sup>9</sup> Damit scheidet eine Strafbarkeit § 202a StGB ebenfalls aus.<sup>10</sup>

**bb) Unbefugte Verwertung von Geschäfts- oder Betriebsgeheimnissen (§ 17 Abs. 2 Nr. 2 UWG)**

Es bleibt die Strafvorschrift des § 17 UWG. Einschlägig ist § 17 Abs. 2 Nr. 2 UWG, die unbefugte Verwertung von Geschäfts- oder Betriebsgeheimnissen (sog. Geheimnishehlerei). Das Tatobjekt des Geschäftsgeheimnisses ist bei jeder im Zusammenhang mit einem Betrieb stehende Tatsache gegeben, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem Willen des Betriebsinhabers aufgrund eines berechtigten wirtschaftlichen Interesses geheim gehalten werden soll.<sup>11</sup> Es besteht kein Zweifel, dass die Kontodaten der Bankkunden dem Geheimnisbegriff unterfallen. Ebenso ist ein berechtigtes Geheimhaltungsinteresse der Bank zu bejahen. Dieses ist schon dann gegeben, wenn die Geheimhaltung für die Wettbewerbsfähigkeit des Unternehmens von Bedeutung ist, beziehungsweise wenn das Bekanntwerden der Tatsache geeignet ist, die Stellung des eigenen Betriebs im Wettbewerb zu schmälern.<sup>12</sup> Die Position der Bank wird gegenüber ihren Wettbewerbern nachhaltig beeinträchtigt, wenn bekannt wird, dass vertrauliche Kundendaten ihren Weg zu den Strafverfolgungsbehörden finden. Andere Kunden – und zwar nicht nur solche, die Kapitaleinkünfte gegenüber dem Finanzamt verschweigen – könnten sich zur Auflösung ihrer Konten veranlasst sehen. Neue Kunden werden unter Umständen von der Eröffnung eines Kontos bei dieser Bank abgehalten.

Das berechtigte Geheimhaltungsinteresse der Bank entfällt auch nicht dadurch, dass die deutschen Bankkunden ihrerseits steuerrechtlich zur Offenbarung ihrer Konten beziehungsweise des darauf gelagerten Kapitals verpflichtet sind und sich durch Nichterklärung der Kapitaleinkünfte wegen Steuerhinterziehung strafbar machen. In der Literatur wird zum Teil ein berechtigtes Geheimhaltungsinteresse an gesetzwidrigen oder strafbaren Geschäftsgeheimnissen verneint.<sup>13</sup> Doch betrifft diese Einschränkung Fälle,

---

9 *Fischer* (Fn. 8), Rn. 8 a.

10 Vgl. *Ignor/Jahn*, *JUS* 2010, 390, 391.

11 *Harte-Bavendamm*, in: *ders./Henning-Bodewig*, *UWG*, 2. Aufl. 2009 § 17 Rn. 1; *Köhler/Bornkamm*, *UWG*, 28. Aufl. 2010, § 17 Rn. 4; *Janssen/Maluga*, in: *Münchener Kommentar*, 1. Aufl. 2010, § 17 UWG Rn. 14.

12 *Diemer*, in: *Erbs/Kohlhaas*, *Strafrechtliche Nebengesetze*, 177. Aufl. 2009, § 17 UWG Rn. 15; *Harte-Bavendamm* (o. Fn. 11) Rn. 6; *Köhler/Bornkamm* (o. Fn. 11), Rn. 9.

13 *Möhrenschlager*, in: *Wabnitz/Janovsky*, *Handbuch des Wirtschafts- und Steuerstrafrechts*, 3. Aufl. 2007, Kapitel 13 Rn. 10.

in denen der Geheimnisträger selbst nicht schutzwürdig ist, weil er etwa Patentverletzungen begeht oder unter gesundheitsgefährdenden Bedingungen produzieren lässt.<sup>14</sup> Das Geheimhaltungsinteresse der Bank wird nicht dadurch beseitigt, dass ein Teil ihrer Kunden steuerrechtlichen Pflichten gegenüber dem deutschen Staat nicht nachkommt. Man kann keinesfalls unterstellen, dass jeglicher deutscher Steuerbürger, der Konten im Ausland unterhält, die dort erwirtschafteten Erträge der deutschen Steuer vorenthält. Einen derartigen Generalverdacht gibt es nicht. Auch der Datendieb selbst weiß nicht, ob und welche Kunden Kapitalertragsteuer hinterzogen haben.<sup>15</sup>

Durch die elektronische Speicherung der Kundendaten auf einem Datenträger hat sich der Bankmitarbeiter das Geschäftsgeheimnis auf eine von § 17 Abs. 2 Nr. 2 UWG verlangte Weise verschafft. Der Tatbestand knüpft an die Verschaffungsmodalitäten des § 17 Abs. 2 Nr. 1 a) bis c) UWG an. Einschlägig ist Nr. 1 a), die Anwendung technischer Mittel. Darunter fällt die Übertragung von EDV-Daten auf Speichermedien.<sup>16</sup> Die Tathandlung des Abs. 2 Nr. 2 selbst liegt in der Verwertung oder Mitteilung des Geheimnisses. Verwerten ist jede Tätigkeit, die darauf gerichtet ist, das Geheimnis zu wirtschaftlichen Zwecken zu nutzen.<sup>17</sup> Eine Einschränkung der Tathandlung auf die Verwertung im Rahmen einer Wettbewerbssituation unter Konkurrenten ist abzulehnen. Auszugehen ist von den geschützten Interessen des Geheimnisinhabers. Das ist die betroffene Bank. Deren Interessen werden nicht minder beeinträchtigt, wenn die Kundendaten nicht an einen Mitkonkurrenten, sondern an den deutschen Staat verkauft werden.<sup>18</sup> Im subjektiven Tatbestand ist neben dem Vorsatz das Handeln aus einem der gesetzlich genannten Beweggründe erforderlich. Gegeben ist hier ein Handeln aus Eigennutz, weil der Bankmittäter sich – wie für diesen Beweggrund erforderlich<sup>19</sup> – einen materiellen Vorteil verschaffen wollte.

## b) Rechtfertigung?

Die Geheimnisverwertung nach § 17 Abs. 2 Nr. 2 UWG muss unbefugt sein. Das wäre nicht der Fall, wenn die Weitergabe der Bankkundendaten durch einen Rechtfertigungsgrund gedeckt wäre.<sup>20</sup> Zu denken ist an den rechtfert-

---

14 Siehe wiederum *Möhrenschlager* (o. Fn. 13), Rn. 10.

15 Vgl. hierzu *Ignor/Jahn*, JUS 2010, 390, 391.

16 *Diemer* (o. Fn. 12), Rn. 37; *Harte-Bavdendamm* (o. Fn. 11), Rn. 22.

17 *Janssen/Maluga* (o. Fn. 11), Rn. 104.

18 Vgl. *Ignor/Jahn*, JUS 2010, 390, 391.

19 *Harte-Bavdendamm* (o. Fn. 11), Rn. 15.

20 Zum Merkmal „unbefugt“ *Diemer* (o. Fn. 12), Rn. 23.

tigenden Notstand des § 34 StGB. Das gefährdete und zu schützende Interesse wäre das Rechtsgut des § 370 AO, also der staatliche Steueranspruch.<sup>21</sup> Dieses müsste im Rahmen der bei § 34 StGB vorzunehmenden Güterabwägung das beeinträchtigte Interesse – hier das Geheimhaltungsinteresse der Bank – wesentlich überwiegen. Ein genereller Vorrang des staatlichen Steueranspruchs lässt sich jedoch auch im Hinblick der Höhe der hinterzogenen Steuern und der erwartenden Einnahmen als Folge von Selbstanzeigen nicht begründen.<sup>22</sup> Umgekehrt bedeutet die Annahme einer Berechtigung zur Weitergabe von Kontendaten an die Steuerbehörden eine erhebliche Beeinträchtigung der Geheimhaltungsinteressen der betroffenen Bank und des Persönlichkeitsschutzes ihrer Kunden.<sup>23</sup>

Lässt man die Rechtfertigung nach § 34 StGB nicht schon an der Interessenabwägung scheitern, steht ihr jedenfalls das Fehlen des subjektiven Rechtfertigungselements entgegen. Der Täter muss mit Rettungswillen handeln. Zwar lässt die überwiegende Meinung ein Handeln in Kenntnis der rechtfertigenden Sachlage ausreichen und sieht es unschädlich an, wenn der Täter mit der Rettungshandlung noch andere Motive verfolgt.<sup>24</sup> Jedoch dürfen die anderen Motive den Rettungswillen nicht ganz nebensächlich werden lassen.<sup>25</sup> Genau dies ist bei der Weitergabe von Bankdaten an die deutschen Steuerbehörden gegen Belohnung der Fall. Dem Bankmitarbeiter geht es primär um seinen materiellen Vorteil. Dass er darüber hinaus zur Sicherung des Steueranspruchs des deutschen Staates beiträgt, ist für ihn belanglos. Damit tritt der Grund für die gesetzliche Rechtfertigung völlig in den Hintergrund, so dass ein solcher Täter die Straffreiheit nicht verdient.<sup>26</sup> Anlass für abweichende Beurteilung kann allenfalls ein neuerer Fall geben, in dem der Informant das Geld für die gelieferten Daten von Kunden – wiederum der Privatbank Julius Bär – nicht behalten, sondern zugunsten der Erdbebenopfer in Haiti an eine Hilfsorganisation gespendet hat.<sup>27</sup> Dieser

---

21 Vgl. BGH NJW 2009, 528 Rn. 21.

22 *Ignor/Jahn*, *JUS* 2010, 390, 392; anders – bei der Frage der Rechtfertigung des Ankaufs durch deutsche Beamte – *Ambos*, *FAZ* vom 11.02.2010, S. 6.

23 *Sieber*, *NJW* 2008, 881, 884; *Spernath*, *NJW* 2010, 307, 308.

24 *Fischer* (o. Fn. 8), § 34 Rn. 17; *Perron*, in: Schönke/Schröder, *Strafgesetzbuch*, 28. Aufl. 2010, § 34 Rn. 48.

25 *Fischer* (o. Fn. 8), § 32 Rn. 26 m. w. N. Diese Einschränkung bei der Notwehr ist auf den rechtfertigenden Notstand voll übertragbar.

26 Gegen eine Rechtfertigung nach § 34 StGB auch *Ignor/Jahn*, *JUS* 2010, 390, 392; *Sieber*, *NJW* 2008, 881, 884; *Spernath*; *NStZ* 2010, 307, 308; anders *Ambos*, *FAZ* vom 11.02.2010, S. 6.

27 Siehe die Meldung in der *Süddeutschen Zeitung* vom 22.10.2010; abrufbar im Internet unter <http://www.sueddeutsche.de/geld/2.220/steuer-cd-datenklau-robin-hood-mit-sonnenbrille-1.1014637>.

Person ging es offenbar nicht um ihren materiellen Vorteil. Im Gegensatz zu den vielen anderen Fällen liegt zumindest ein Indiz für das subjektive Rechtfertigungselement vor.

### c) Anwendbarkeit deutschen Strafrechts

Wird eine Rechtfertigung nach § 34 StGB abgelehnt, hängt die Strafbarkeit des Bankmitarbeiters nach § 17 Abs. 2 Nr. 2 UWG letztlich davon ab, ob deutsches Strafrecht anwendbar ist. Geht man davon aus, dass der Bankmitarbeiter die Daten den Steuerbeamten auf deutschem Boden zum Kauf angeboten hat, folgt die Anwendbarkeit aus dem Territorialitätsprinzip des § 3 StGB. Danach gilt das deutsche Strafrecht für Taten, die im Inland begangen werden. Diese Voraussetzung ist gegeben. Gemäß § 9 Abs. 1 StGB ist die Tat unter anderem an dem Ort begangen, an dem der Täter gehandelt hat. Tat handlung des § 17 Abs. 2 Nr. 2 UWG ist die Verwertung des unbefugt verschafften Geheimnisses – hier durch Verkauf und Übergabe der Daten in Deutschland.<sup>28</sup>

Geht man davon aus, dass die Übergabe des Datenträgers auf ausländischem Boden erfolgte, lässt sich die Anwendbarkeit deutschen Strafrechts ebenfalls begründen. In der Literatur wird überzeugend darauf hingewiesen, dass die Straftat nach § 17 Abs. 2 Nr. 2 UWG kein bloßes Tätigkeits-, sondern ein Erfolgsdelikt ist. Der tatbestandliche Erfolg ist die Verwertung, d. h. die wirtschaftliche Nutzung des Geheimnisses. Diese erfolgte durch die Nutzung der Bankkundendaten durch die Steuerfahndungen in Deutschland zum Zwecke steuerstrafrechtlicher Ermittlungen. Die Anwendbarkeit des deutschen Strafrechts ergibt sich hier aus § 3 StGB in Verbindung der 3. Variante des § 9 Abs. 1 StGB. Danach ist eine Tat auch dort begangen, an dem der zum Tatbestand gehörende Erfolg eingetreten ist.<sup>29</sup>

### d) Strafbarkeit nach schweizerischen Strafrecht

Da der Kopiervorgang der Kontodaten deutscher Kunden durch den Bankmitarbeiter in der Schweiz geschah, es sich bei den Banken um Schweizer Rechtssubjekte und bei dem Täter um einen schweizerischen Staatsbürger handelt, liegt unter mehreren Gesichtspunkten eine Strafbarkeit nach schweizerischem Strafrecht nahe.<sup>30</sup>

---

28 Für die Anwendbarkeit des deutschen Strafrechts auch *Ignor/Jahn*, JUS 2010, 390, 393.

29 Vgl. wiederum *Ignor/Jahn*, JUS 2010, 390, 393.

30 Vgl. hierzu und zum Folgenden *Ostendorf*, ZIS 2010, 301, 302 f.



Erfüllt ist der Straftatbestand der Verletzung eines Fabrikations- oder Geschäftsgeheimnisses (Art. 162 StGB-Schweiz). Strafbar nach dieser Vorschrift ist das Verraten oder Ausnutzen eines Geheimnisses, das der Täter infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte. Als Mitarbeiter der Bank mit Zugriff auf die Kundendaten – und einer zu unterstellenden vertraglichen Verschwiegenheitspflicht – hatte die betreffende Person Täterqualität. In dem Verkauf der kopierten Daten an die deutschen Behörden liegt das Ausnutzen des Geschäftsgeheimnisses.

Eine dem Ausspähen von Daten (§ 202 a StGB) vergleichbare Strafvorschrift enthält Art. 143 StGB-Schweiz (Unbefugte Datenbeschaffung). Verlangt wird dort ebenfalls eine besondere Sicherung der Daten gegen unbefugten Zugriff. Ob diese Voraussetzung erfüllt ist, bleibt letztlich Tatfrage. Sie ist aber aus den gleichen Gründen wie bei § 202 a StGB<sup>31</sup> zu verneinen, wenn dem Mitarbeiter die Daten dienstlich zur Verfügung standen.<sup>32</sup>

Eine § 17 Abs. 2 Nr. 2 UWG vergleichbare Bestimmung ist die Verletzung von Fabrikations- und Geschäftsgeheimnissen gemäß Art. 6 des schweizerischen Bundesgesetzes gegen den unlauteren Wettbewerb. Unlauter handelt nach dieser Vorschrift, wer Fabrikations- oder Geschäftsgeheimnisse, die er ausgekundschaftet oder sonst wie unrechtmäßig erfahren hat, verwertet oder anderen mitteilt. Nach Art. 23 Abs. 1 desselben Gesetzes ist die unlautere Handlung strafbar. Die Voraussetzungen des Art. 6 können aus denselben Gründen wie bei § 17 Abs. 2 Nr. 2 UWG<sup>33</sup> bejaht werden.

Schließlich ist nach Art. 47 des Schweizerischen Bankengesetzes strafbar, wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als – unter anderem – Angestellter einer Bank anvertraut worden ist oder das er in dieser Eigenschaft wahrgenommen hat. Dieser Straftatbestand ist erfüllt, wenn die betreffende Person als Mitarbeiter der Bank dienstlich Zugang zu den vertraulichen Bankkontodaten hatte.

Nicht zuletzt: Die Schweizer Staatsanwaltschaft verfolgt die Datenkopierer national und international. Es steht zu vermuten, dass dies auf solider rechtlicher Grundlage steht.

## e) Ergebnis

Das Kopieren der Bankdaten und ihr Verkauf an die deutschen Steuerbehörden begründet eine Strafbarkeit gemäß § 17 Abs. 2 Nr. 2 StGB sowie nach

---

31 Oben III.1.a) aa).

32 Insoweit anders *Ostendorf*, ZIS 2010, 301, 303.

33 Oben III.1.a) bb).

schweizerischem Strafrecht gemäß Art. 162 StGB-Schweiz, Art. 6 des Schweizerischen Bundesgesetzes gegen den unlauteren Wettbewerb und Art. 47 des Schweizerischen Bankengesetzes.

## 2. Ankauf der Daten durch Amtspersonen

### a) Hehlerei (§ 259 StGB)

Eine Strafbarkeit wegen Hehlerei durch Ankauf des Datenträgers mit den Bankkundendaten scheidet aus. Tatobjekt des § 259 StGB ist allein eine Sache, also ein körperlicher Gegenstand, der aus einer gegen fremdes Vermögen gerichteten Straftat eines anderen stammt. Daran fehlt es, wenn der Mitarbeiter die Bankdaten auf einem in seinem Eigentum befindlichen Datenträger gespeichert hat. Der Datenträger selbst ist aller Vermutung nach<sup>34</sup> nicht durch die Straftat eines anderen erlangt; auf die Daten selbst ist § 259 StGB mangels Körperlichkeit nicht anwendbar.<sup>35</sup>

### b) Begünstigung (§ 257 StGB)

Näher liegt eine Strafbarkeit wegen Begünstigung (§ 257 StGB). Die als Vortat erforderliche rechtswidrige Tat – eine mit Strafe bedrohte Handlung jeder Art<sup>36</sup> – ist mit der von dem Bankmitarbeiter begangenen unbefugten Verwertung eines Geschäftsgeheimnisses gemäß § 17 Abs. 2 Nr. 2 UWG gegeben. Tathandlung ist das „Hilfeleisten“. Darunter fällt jede Handlung, die geeignet ist, die durch die Vortat erlangten Vorteile gegen Entziehung zu sichern.<sup>37</sup> Im Falle des Ankaufs von Daten der LGT durch Mitarbeiter des BND ist das Hilfeleisten in manchen Literaturbeiträgen bejaht worden. Zur Begründung wurde angeführt, dass schon das Hilfeleisten beim Absetzen der Tatbeute im Rahmen des § 257 StGB ausreiche und dass der direkte Ankauf der durch die Straftat erlangten Daten erst recht eine Tathandlung darstelle.<sup>38</sup> Daneben wurde darauf hingewiesen, dass § 257 StGB jeder Erschwerung beziehungsweise Vereitelung der Restitution entgegen treten will. Der Ankauf der Daten vereitele die Restitution des gesetzmäßigen

---

34 Ein vorsichtiger deutscher Aufkäufer würde darauf achten, dass der Datenträger nicht mit dem Logo der geschädigten Bank versehen ist.

35 Siehe zur einhelligen Ablehnung des § 259 StGB *Ignor/Jahn*, JUS 2010, 390, 391; *Ostendorf*, ZIS 2010, 301, 303; *Spernath*, NStZ 2010, 307, 309; *Trüg/Habetha*, NJW 2008, 887 f.

36 Vgl. *Fischer* (o. Fn. 8), § 257 Rn. 2.

37 *Stree/Hecker*, in: *Schönke/Schröder* (o. Fn. 24), § 257 Rn. 11.

38 *Kelnhöfer/Krug*, StV 2008, 660, 662 f.

Zustandes gänzlich.<sup>39</sup> Dagegen wird eingewandt, dass der Datenkauf keine wirkliche Hilfestellung für den Vortäter darstellt. Dessen Verfügungsmacht über die Bankdaten werde nicht dadurch verbessert, dass die deutschen Beamten die Daten aufkauften und bestehe unabhängig davon fort.<sup>40</sup> Deutlich vorzugswürdig ist das Argument der Vereitelung des ursprünglichen Zustands, mit dem die Tathandlung zu bejahen ist.

Der subjektive Tatbestand verlangt neben vorsätzlichem Handeln die Absicht, dem Vortäter die Vorteile der Tat zu sichern. Es muss dem Täter der Begünstigung darauf ankommen, im Interesse des Vortäters die Wiederherstellung des gesetzmäßigen Zustandes zu verhindern oder zumindest zu erschweren.<sup>41</sup> Die Vorteilssicherung muss nicht einziger Beweggrund des Täters und kann auch bloßes Zwischenziel zur Erreichung eines weiteren Ziels sein.<sup>42</sup> Daraus ist in der Liechtenstein-Affäre das Vorliegen der Vorteilssicherungsabsicht in den Fällen des staatlichen Datenankaufs gefolgert worden. Der Ankauf der Daten und die damit eintretende Vereitelung der Wiederherstellung des gesetzmäßigen Zustandes (etwa durch Rückgabe des Datenträgers) ist aus Sicht der Beamten notwendiges Zwischenziel. Dieses – für § 257 StGB ausreichende – Zwischenziel hätten die Beamten anstreben müssen, um die beabsichtigte Verfolgung von Straftaten vornehmen zu können.<sup>43</sup> Die Gegenposition behauptet, dass es den Beamten allein um eine Beweismittelgewinnung und kaum um eine Besserstellung des Informanten geht. Der Begünstigungseffekt werde allenfalls als unvermeidliche Nebenfolge hingenommen, was für § 257 StGB nicht genüge.<sup>44</sup>

Es überzeugt jedoch nicht, die Besserstellung des Informanten zu einer bloßen Nebenfolge herabzustufen. Die Beamten mussten als Zwischenziel den Besitz an dem Datenträger erlangen, um die beabsichtigten Ermittlungen wegen Straftaten durchführen zu können. Das genügt für die Begünstigungsabsicht. Zudem: Das Ausblenden des notwendigen Begünstigungserfolges aus dem Tatbestand wäre eine verkappte Rechtfertigungsargumentation. Letztendlich liegt darin eine Verkürzung des Tatbestandes aufgrund des angeblich hehren Zieles, die Daten zwecks Besteuerung und Verfolgung von Steuersündern zu erhalten. Warum jemand begünstigt, kann aber nur eine Frage der Strafzumessung, nicht des Tatbestandes sein.

---

39 *Trüg/Habetha*, NJW 2008, 887, 889.

40 *Ostendorf*, ZIS 2010, 301, 303 f.

41 *Fischer* (o. Fn. 8), § 257 Rn. 10; *Stree/Hecker* (o. Fn. 37) Rn. 19.

42 *Stree/Hecker* (Fn. 37), Rn. 17.

43 *Trüg/Habetha*, NJW 2008, 887, 889; in diesem Sinne auch *Kelnhöfer/Krug*, StV 2008 660, 663.

44 *Ostendorf*, ZIS 2010, 301, 304; *Stree/Hecker* (Fn.), Rn. 19. Gegen die Vorteilssicherungsabsicht auch *Walter*, in: *Leipziger Kommentar zum StGB*, Band 8, 12. Aufl. 2010, § 257 Rn. 77.

Ansonsten wird tatbestandsmäßiges Handeln und Rechtfertigungsgrund unzulässig vermischt.

**c) Teilnahme an der unbefugten Verwertung von Geschäftsgeheimnissen (§§ 17 Abs. 2 Nr. 2 UWG, 26 oder 27 StGB)**

Einer Teilnahmestrafbarkeit der die Daten ankaufenden Beamten steht nicht von vornherein entgegen, dass es sich um eine notwendige Teilnahme an der unbefugten Geheimnisverwertung durch den Bankmitarbeiter handelt. Eine straflose notwendige Teilnahme liegt vor, wenn die Mitwirkung nicht über den zur Tatbestandserfüllung notwendigen Beitrag hinausgeht.<sup>45</sup> Im vorliegenden Fall wäre das die Entgegennahme des Datenträgers mit den Bankdaten. Die Mitwirkung der Beamten geht jedoch darüber hinaus. Sie sind nicht nur passive Nehmer, sondern greifen durch die Zusage einer Zahlung im Millionenbereich aktiv ein. Dies ist aus meiner Sicht der (entscheidungs-) erhebliche Unterschied zu denjenigen Fällen, in denen die Daten ohne jede Gegenleistung zur Verfügung gestellt werden, wie dies in den Batliner-Fällen geschehen ist. Insofern liegt zumindest eine psychische Beihilfe durch Bestärkung des Entschlusses des Informanten zur unbefugten Geheimnisverwertung vor.<sup>46</sup>

Zudem wird mit überzeugenden Gründen eine Strafbarkeit wegen Anstiftung bejaht. Ausgangspunkt ist die Überlegung, dass der Bankmitarbeiter vor Beginn der Verhandlungen mit deutschen Behörden noch nicht zur Begehung der konkreten Verwertung als Tat nach § 17 Abs. 2 Nr. 2 StGB fest entschlossen und eine Anstiftung damit ausgeschlossen ist. Vielmehr hängt sein Tatentschluss für die konkrete Übergabe davon ab, dass ihm ein Geldbetrag für die Überlassung des Datenträgers gezahlt wird. Man kann dies deutlich daran festmachen, dass Herr Kieber die Daten auch an andere Staaten verkauft hat, also nicht von vorneherein konkret geplant hat, an wen die Daten verkauft werden sollen. In diesem Fall erfüllt erst die von den beteiligten Beamten gegebene Zahlungszusage die Bedingung, die der Bankmitarbeiter sich für seinen Tatentschluss selbst gesetzt hat.<sup>47</sup> Damit ist auch eine Strafbarkeit wegen Anstiftung zu bejahen.

---

45 Heine, in: Schönke/Schröder (o. Fn. 24), vor §§ 25 ff. Rn. 46 ff.

46 So auch Sieber, NJW 2008, 881, 884 f.; Spemath, NSTZ 2010, 307, 309 f.; Trüg/Habetha, NJW 2008, 887, 889.

47 So Schünemann, NSTZ 2008, 305, 308; und im Anschluss Ignor/Jahn, JUS 2010, 390, 393; dagegen Ostendorf, ZIS 2010, 301, 304 f.