Der „Grundsatz der Verfügbarkeit“ von Daten zwischen Staat und Unternehmen*

Von Wiss. Mitarbeiter **Dominik Brodowski**, LL.M. (UPenn), München

Der europastrafrechtliche Grundsatz der Verfügbarkeit von Daten betrachtet die Möglichkeiten der Mitgliedstaaten der Europäischen Union, auf Daten zuzugreifen, die von einem anderen Mitgliedstaat für hoheitliche Zwecke vorgehalten werden. Das gleiche Rechtsprinzip ist jedoch bereits auf nationaler Ebene, insbesondere im Verhältnis zwischen Staat und Unternehmen zu diskutieren: Inwieweit sind Daten, die Bürger an Unternehmen oder sonstige Dritte preisgegeben haben, für Strafverfolgungszwecke verfügbar? Eine Analyse der strafprozessualen Eingriffsgrundlagen und der zu beachtenden Ausnahmevorschriften – etwa für Berufsgeheimnisträger – zeigt, dass insoweit ein Grundsatz der Verfügbarkeit bereits weitestgehend verwirklicht ist. Aus der Hand gegebene Daten stehen nahezu schrankenlos für Strafverfolgungszwecke zur Verfügung.

The principle of availability enshrined in European Criminal Law means that databases operated by the authorities in one state should be freely accessible to the authorities of other member states. The same principle deserves to be discussed within each criminal justice system, in the relation to data stored by private entities: How freely is data stored by private entities available in criminal investigations? In Germany, data entrusted to third parties is in nearly all cases available to the authorities. Therefore, such a principle of availability has already fully been materialized in German criminal procedure.

I. Die Bedeutung von Datenbeständen für die Strafverfolgung

Der außerordentlich hohe Börsen- bzw. Marktwert von Unternehmen wie Facebook oder Google beruht auf den immensen Beständen an persönlichen Daten, die diese Unternehmen angesammelt haben. Dass diese Datenbestände aber nicht nur in wirtschaftlicher Hinsicht, sondern auch für die Strafverfolgung von Bedeutung sind, sei zunächst anhand dreier Fallbeispiele exemplifiziert.

> *Beispiel 1*: Auf Bitten der Staatsanwaltschaft Halle durchsuchten im Sommer 2006 deutsche Banken alle Zahlungen mit Kreditkarten darauf, ob Kunden einen bestimmten Betrag auf ein verdächtiges Konto in Thailand überwiesen hatten. Mit einer solchen Überweisung konnte nämlich auf kinderpornographische Schriften zugegriffen werden. Die Banken ermittelten 322 Personen; etliche wurden später wegen des Besitzes kinderpornographischer Schriften verurteilt.[1]

> *Beispiel 2*: Der Ermittlungsrichter am AG Mannheim ordnete in einem Ermittlungsverfahren wegen Untreue die Beschlagnahme aller E-Mails an, die noch in einem bestimmten Postfach bei einem Internetprovider lagen und die aus dem Zeitraum August 2008 bis Dezember 2009 stammten. Der kooperative Internetprovider stellte der Polizei nun einen umfassenden Gastzugang zur Verfügung. Die Polizei betrachtete alle Nachrichten – auch solche aus dem Jahr 2010 – und konnte dem Verdächtigen so einen völlig anders gelagerten Betrug nachweisen.[2]

> (Hypothetisches) *Beispiel 3*: In Berlin filmt eine Überwachungskamera eine Person dabei, wie sie ein Auto in Brand setzt. Auf Bitten der Polizei gleicht Facebook das Foto mit sämtlichen auf Facebook gespeicherten Fotos mit einer automatischen Gesichtserkennung ab und benennt den Täter.

All diesen Beispielen ist gemein, dass Unternehmen nicht allein über eigene Daten verfügen, sondern Daten verdächtiger, aber auch unbeteiligter Dritter heranziehen und den Strafverfolgungsbehörden aushändigen. Inwieweit ist ein solches Verhalten der Unternehmen geboten, inwieweit ist es verboten?

II. Die Prinzipien der Zweckbindung und der Verfügbarkeit von Daten

Bevor auf diese konkreten Beispiele und die jeweiligen Eingriffsgrundlagen eingegangen werden kann, gilt es, den Bogen zu spannen zur *Verfügbarkeit* von Daten für Strafverfolgungsbehörden. Dieser Begriff hat seine Wurzeln in der Europäisierung des Strafrechts: Dem Grundsatz der Verfügbarkeit von Daten zufolge sollen Daten, die in einem Mitgliedstaat der EU bereits vorrätig sind, ohne größere formelle oder materielle Hindernisse auch in anderen Mitgliedstaaten für andere polizeiliche und strafprozessuale Zwecke zur Verfügung stehen.[3] Das gilt etwa für Fingerabdruckdaten, die in Deutschland vom Bundeskriminalamt vorgehalten werden.

Der europastrafrechtliche Grundsatz der Verfügbarkeit betrachtet somit das Verhältnis zwischen mehreren *Staaten* und thematisiert primär Zugriffe auf Daten, die von *staatlicher Seite* erhoben und gespeichert werden. Bezüglich solcher staatlich vorgehaltenen Daten ist wegen des gegenläufigen Prinzips der Zweckbindung von Daten aber bereits bei inner-

---

* Das Manuskript beruht auf einem Vortrag des *Verf.* auf dem Symposium der deutschen und türkischen Landesgruppe der AIDP „Cybercrime: Ein deutsch-türkischer Rechtsdialog“ an der Bilgi Universität, Istanbul. Der Vortragsstil wurde beibehalten.

[1] Vgl. BVerfGK 15, 71 m. Anm. *Brodowski*, JR 2010, 546; *Schaefer*, NJW-Spezial 2009, 280; *Schnabel*, CR 2009, 384.

[2] Vgl. LG Mannheim, StV 2011, 352 m. Anm. *Albrecht*, jurisPR-ITR 19/2011 Anm. 5.

[3] Vgl. *Böse*, Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, 2007; *Meyer*, NStZ 2008, 188; *Papayannis*, ZEuS 2008, 219; *Zöller*, ZIS 2011, 64, sowie den Rahmenbeschluss 2006/960/JI des Rates v. 18.12.2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, ABl. EU 2006 Nr. L 386, S. 89.

staatlichen Datenabfragen eine Vielzahl von Grenzen für Ermittlungsmaßnahmen zu beachten.[4]

In diesem auch verfassungsrechtlich überformten Spannungsfeld zwischen Verfügbarkeit und Zweckbindung staatlich erhobener Daten besteht viel Anlass zur Diskussion. Die zunehmende Verlagerung hoheitlichen Handelns auf Private – man denke allein daran, dass Post- und Telekommunikationsdienste noch vor wenigen Jahren hoheitlich organisiert waren – zwingt aber dazu, dieselbe Fragestellung auch für das Verhältnis zwischen Staaten und Unternehmen aufzuwerfen. Inwieweit ist eine Zweckbindung bei von Unternehmen erhobenen Daten zu beachten, inwieweit sind von Unternehmen erhobene Daten für die Strafverfolgungsbehörden verfügbar?[5]

III. Eingriffsgrundlagen

Nach deutschem und europäischem Verfassungsverständnis erfordern Zugriffe der Ermittlungsbehörden auf personenbezogene Daten eine gesetzliche Eingriffsgrundlage.[6] Die in Deutschland normierten Eingriffsgrundlagen seien im Folgenden daraufhin untersucht, ob innerstaatlich ein Grundsatz der Verfügbarkeit von Daten bereits verwirklicht ist.

1. Zeuge

Das klassische Beweismittel schlechthin – der Zeuge – scheidet dabei von vornherein aus: Er ist nämlich ein persönliches Beweismittel, der über seine persönliche Wahrnehmung bekunden soll.[7] Die allermeisten Daten, an welchen die Ermittlungsbehörden Interesse haben, werden von Mitarbeitern der Unternehmen jedoch nicht persönlich wahrgenommen, sondern nur automatisch von den Rechnern des Unternehmens verarbeitet. Zwar könnten Unternehmensangehörige die entsprechenden Informationen abfragen, und sich damit zu Zeugen „machen“, doch zu solchen eigenen Nachforschungen ist eine Privatperson oder ein Privatunternehmen nicht verpflichtet.[8]

2. Freiwillige Auskunft

Eine andere Frage ist allerdings, ob ein Zeuge oder ein Unternehmen eigene Nachforschungen tätigen darf – und ob die Staatsanwaltschaft darum bitten darf. Grundsätzlich ist ein solches kooperatives Zusammenwirken von Zeugen, Unternehmen und der Staatsanwaltschaft gestattet und sogar geboten – und in der Praxis auch oft zu verzeichnen. Die Grenze findet die Kooperation jedoch dann, wenn sie zur Kollusion wird, also zu nicht von der Rechtsordnung akzeptierten Nachteilen für Dritte führt.

a) Das ist zunächst dann der Fall, wenn sich die Zeugen oder die Mitarbeiter des Unternehmens *strafbar* machen würden: So dürfen sie etwa keine Auskunft geben über Telekommunikationsvorgänge, denn dann drohte ihnen eine Bestrafung nach § 206 Abs. 1 StGB.[9]

b) Aufgrund der Gesetzesbindung der Exekutive (Art. 20 Abs. 3 GG) ist es den Strafverfolgungsbehörden ebenfalls nicht gestattet, um *ordnungsrechtlich verbotenes* Verhalten zu bitten. Oftmals sind aber freiwillige Recherchen datenschutzrechtlich verboten. Maßstab hierfür ist § 28 Abs. 2 Nr. 2 lit. b BDSG, demzufolge die Datennutzung und -weitergabe zulässig ist, soweit dies zur Strafverfolgung erforderlich ist „und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat“. Rechtsprechung und Literatur verstehen letzteres aber nicht als starre Ausschlussklausel, sondern nehmen eine Interessenabwägung zwischen dem Strafverfolgungsinteresse des Staates einerseits und dem Recht auf informationelle Selbstbestimmung des einzelnen andererseits vor.[10]

Bei dieser Abwägung sind erstens die „schutzwürdigen Interessen“ grundsätzlich weit auszulegen und erfassen daher auch „wirtschaftliche oder berufliche Nachteile“.[11] Zweitens sind die besonderen Wertungen des Grundrechts auf Vertrau-

[4] Exemplarisch seien herausgegriffen die Limitierung der Verwertbarkeit von Zufallsfunden (etwa gem. § 477 Abs. 2 S. 2 StPO), das Erfordernis einer Aussagegenehmigung gem. § 96 StPO, das Steuergeheimnis (§ 30 AO) sowie die Unzulässigkeit der Verwertung von Daten aus dem Autobahnmauterfassungssystem für strafprozessuale Zwecke (§§ 4, 7, 9 Bundesfernstraßenmautgesetz, s. zur insoweit identischen Vorläufervorschrift des Autobahnmautgesetzes LG Magdeburg, NJW 2006, 1073 m. Anm. *Fraenkel/Hammer*, DuD 2006, 497).

[5] Während beim europastrafrechtlichen Prinzip die *wechselseitige* Verfügbarkeit im Vordergrund steht, dominiert im Verhältnis zwischen Staaten und Unternehmen der *einseitige* Zugriff des Staates auf von Unternehmen gespeicherte Daten. Auf diese Konstellation soll sich daher auch die folgende Darstellung beschränken.

[6] Aus verfassungsrechtlicher Sicht vgl. BVerfGE 65, 1 (43); 67, 100 (143); 84, 239 (279); 103, 21 (33); 115, 320 (341); BVerfGK 15, 71 (76 f.), sowie aus europäischer Sicht vgl. nur Art. 8 Abs. 2 Charta der Grundrechte der Europäischen Union (GRC), ABl. EU 2010 Nr. C 83, S. 389. Zur Auffassung der Kommission, als gesetzliche Grundlage reiche die Zuständigkeit der Strafverfolgungsbehörden zur Strafverfolgung, s. jedoch unten bei und mit Fn. 36.

[7] S. nur *Senge*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 6. Aufl. 2008, Vor § 48 Rn. 1; *Eisenberg*, Beweisrecht der StPO, 7. Aufl. 2011, Rn. 1000.

[8] Aus prozessualer Sicht s. *Eisenberg* (Fn. 7), Rn. 1199 f.; *Ignor/Bertheau*, in: Erb u.a. (Hrsg.), Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 2, 26. Aufl. 2008, § 69 Rn. 9 m.w.N.; *Krehl*, NStZ 1991, 416 f.; *Petri*, StV 2007, 266, aus materiell-rechtlicher Sicht s. nur *Lenckner/Bosch*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 161 Rn. 3 m.w.N.

[9] Mangels verbindlicher Anordnung besteht auch keine Rechtfertigung für ein solches Verhalten, ja es wäre sogar eine Umgehung der gesetzlich bestimmten, spezielleren Eingriffsgrundlagen der §§ 100a, 100b StPO.

[10] *Gola/Schomerus*, Bundesdatenschutzgesetz, Kommentar, 10. Aufl. 2010, § 28 Rn. 46 m.w.N.

[11] *Gola/Schomerus* (Fn. 10), § 28 Rn. 26.

lichkeit und Integrität informationstechnischer Systeme[12] zu beachten: In heutiger Zeit verlassen sich viele auf eine (vermeintlich?) sichere Datenspeicherung im Internet, etwa bei der Archivierung von E-Mails. Staatliche Akteure dürfen nun die Wertungen dieses Grundrechts nicht dadurch konterkarieren, dass sie die Preisgabe vertraulich abgespeicherter Informationen durch Dritte fördern. Drittens ist ein mehrpoliges Grundrechtsverhältnis zu berücksichtigen: Neben den Grundrechten des Beschuldigten und denjenigen des Unternehmens sind hier auch die Grundrechtspositionen aller anderen Kunden von Bedeutung. Denn auch deren Daten werden regelmäßig durchsucht, so etwa bei der Suche nach verdächtigen Überweisungen auf ein bestimmtes Konto. Geschieht dabei ein Fehler – und dies kann leicht geschehen –, so werden auch die Daten unbescholtener Kunden übermittelt.[13]

c) Was folgt daraus? Unternehmen ist es datenschutzrechtlich verwehrt, quasi in vorauseilendem Gehorsam freiwillig umfangreiche Hilfe zur Strafverfolgung zu leisten, wenn sie dabei auf umfassende und besonders schützenswerte Datenbestände zurückgreifen müssten oder wenn eine besondere Gefahr dafür besteht, dass diese Herausgabe einen unschuldigen Dritten belasten könnte. Stattdessen sollten Unternehmen ihre umfassende Bereitschaft zur Mitwirkung bekunden, jedoch erst dann Auskunft erteilen, wenn ein förmliches Auskunfts- bzw. Herausgabeverlangen vorliegt (s. näher unten 5.).

3. Telekommunikation

Einen Sonderfall stellen diejenigen Daten dar, die während einer laufenden Telekommunikation anfallen. Diese genießen besonderen Schutz jedenfalls bis zu demjenigen Zeitpunkt, in dem sie beim Empfänger ankommen und dieser die Chance hat, diese zu löschen.[14] Bis dahin sind Zugriffe auf die Inhalte der Telekommunikation[15] nur unter besonderen Voraussetzungen gestattet. So muss etwa der Verdacht einer Katalogtat (§ 100a Abs. 2 StPO) bestehen und die Tat muss „auch im Einzelfall schwer" wiegen. All dies ist aber keine Durchbrechung eines Prinzips der Verfügbarkeit, denn dieser Grundsatz bezieht sich nur auf ohnehin vorrätige, d.h. zuvor gespeicherte Daten. Eine Telekommunikationsüberwachung bezieht sich hingegen auf Daten, die noch übertragen werden und zu diesem Zeitpunkt daher gerade nicht oder nicht dauerhaft gespeichert vorliegen.

Werden aber Daten aus einer Telekommunikation anschließend dauerhaft abgespeichert – etwa in einem E-Mail-Archiv –, so ist ein Zugriff nach der Rechtsprechung des Bundesverfassungsgerichts nicht am engen Maßstab einer Telekommunikationsüberwachung zu messen, sondern bloß an einer Beschlagnahme.[16]

4. Rasterfahndung

Ein weiterer Sonderfall ist die Rasterfahndung, § 98a StPO. Dabei handelt es sich um die Suche nach potentiellen Tätern aufgrund bestimmter allgemeiner, tätertypischer Merkmale, wie etwa Alter, Herkunft, Beruf, Studiengang, Religionszugehörigkeit und Anzahl der Kinder.[17] Ein solches data mining gilt inzwischen als vielversprechendes Mittel nicht nur bei der Terrorismusbekämpfung: So gab und gibt es Bestrebungen der Europäischen Union, „verdächtige" Flugbewegungen[18] und Überweisungen[19] laufend zu überwachen. Ein solches Durchforsten von Daten ist aber mit erheblichen Grundrechtsgefährdungen verbunden: So handelt es sich dabei um die Erstellung eines umfassenden Persönlichkeitsprofils, was nach deutschem Verfassungsverständnis grundsätzlich unzulässig ist.[20] Bedeutsamer ist jedoch das erhebliche Risiko falsch-positiver Treffer, also dass bloß irgendwie auffällige Personen zu Unrecht in den Verdacht geraten, eine Straftat begangen zu haben. Das macht es notwendig, eine Rasterfahndung nur in engen Grenzen zuzulassen.

Die neuere Rechtsprechung des Bundesverfassungsgerichts konterkariert das aber: Eine Rasterfahndung soll dann nicht vorliegen, wenn bloß Daten eines Unternehmens abgefragt werden, oder wenn das Unternehmen die Suchabfrage selbst durchführt.[21] Demzufolge wäre es etwa keine Rasterfahndung, wenn eine inländische Bank befragt würde, welche deutschen Kunden in den vergangenen Jahren Überweisungen von mehr als 10.000 Euro in die Schweiz getätigt haben – um sodann Ermittlungsverfahren wegen Steuerhinterziehung ein-zuleiten.

5. Auskunftsverlangen

Unternehmen können schließlich dazu verpflichtet werden, diejenigen Festplatten bzw. Datenträger auszuhändigen, auf denen beweisrelevante Daten gespeichert sind (§ 95 Abs. 1 StPO). Zur Abwendung eines solchen weitgehenden Herausgabeverlangens hat sich in der Praxis durchgesetzt, dass das Unternehmen statt dessen Auskunft über diese Daten erteilt, also eine Kopie der beweisrelevanten Daten an die Strafverfolgungsbehörden übermittelt. Ein solches Auskunftsverlangen der Strafverfolgungsbehörden ist aber dennoch ein ho-

[12] Grundlegend BVerfGE 120, 274 m. Anm. u. Bespr. *Böckenförde*, JZ 2008, 925; *Hillgruber*, JZ 2008, 861; *Sachs/Krings*, JuS 2008, 481.
[13] Vgl. *Brodowski*, JR 2010, 546 (548 f.).
[14] BVerfGE 120, 274 (307 f.); 113, 166 (183 ff.).
[15] Verkehrsdaten – das sind Daten, aus denen sich ergibt, wer wann mit wem kommuniziert hat – sind zwar theoretisch etwas leichter zu erheben (§ 100g StPO). Praktisch ergibt sich jedoch das Problem, dass diese Daten derzeit höchstens eine Woche lang gespeichert werden, nachdem die deutsche Umsetzung der Vorratsdatenspeicherung von Telekommunikations-Verbindungsdaten für verfassungswidrig und nichtig erklärt wurde, BVerfGE 125, 260.
[16] BVerfGE 124, 43; zur Übertragung auf Datenspeicherung in der „Cloud" vgl. *Obenhaus*, NJW 2010, 651 (654).
[17] *Schäfer*, in: Erb u.a. (Fn. 8), § 98a Rn. 1; *Brodowski*, JR 2010, 546 (548).
[18] KOM (2011) 32 endg. v. 2.2.2011.
[19] KOM (2011) 429 endg. v. 13.7.2011.
[20] BVerfGE 65, 1 (53).
[21] BVerfGK 15, 71 (77 f.).

heitlicher Eingriff, also ein Zwangsmittel und keinesfalls mit einer Bitte um freiwillige Auskunft zu verwechseln.

Umstritten sind die Anforderungen an ein Auskunftsverlangen: Teile der Rechtsprechung und der Literatur begnügen sich mit einer Anordnung durch Staatsanwaltschaft oder Polizei, obwohl eine Beschlagnahme – die durch eine Herausgabe und Auskunft ja abgewendet wird – einem präventiven Richtervorbehalt unterliegt.[22] Das überzeugt nicht, denn es wird dem Zwangscharakter dieser Maßnahme nicht gerecht, bei der zudem auch mit Ordnungsgeld und ersatzweise Ordnungshaft gedroht werden kann. Zudem ist zu berücksichtigen, dass in diesen Fällen regelmäßig Drittinteressen betroffen sind. Aus diesen Gründen ist daher gemäß § 98 Abs. 1 StPO eine richterliche Anordnung zu fordern, die nur bei Gefahr im Verzug durch die Staatsanwaltschaft und deren Ermittlungspersonen ersetzt werden kann.[23]

6. Durchsuchung und Beschlagnahme

Zuletzt kommt noch eine Durchsuchung (§ 103 StPO)[24] und Beschlagnahme von Daten – bzw. der Datenträger, auf denen diese Daten gespeichert sind – in Betracht (§ 94 StPO). Allerdings ist es unverhältnismäßig, bei unbescholtenen Unternehmen sogleich eine Durchsuchung und Beschlagnahme anzuordnen – man denke etwa daran, was es bedeuten würde, die Rechenzentren einer Großbank zu beschlagnahmen, nur um die Verdächtigen im *Fallbeispiel 1* festzustellen. Vielmehr hat der Staat zunächst darauf zu vertrauen, dass sich Unternehmen rechtmäßig verhalten und ein richterlich angeordnetes Auskunftsverlangen befolgen.[25] Nur bei einer Weigerung oder bei Verdacht eines Zusammenwirkens mit dem Beschuldigten darf eine Durchsuchung und Beschlagnahme durchgeführt werden.[26]

IV. Ausnahmen und Gegenrechte

Wer Daten oder Informationen an Unternehmen preisgibt, muss daher im Ausgangspunkt stets damit rechnen, dass Strafverfolgungsbehörden auf diese ohne größeren Aufwand zugreifen können. Unternehmen sind – nach hier bestrittener Auffassung auch ohne richterlichen Beschluss – verpflichtet, Auskunft über bei ihnen gespeicherte Daten zu erteilen und diese Daten nach bestimmten Merkmalen zu durchsuchen. Wirken Unternehmen nicht freiwillig mit – was in der Praxis ausgesprochen selten geschieht –, so können sie mit Zwangsmitteln zur Herausgabe verpflichtet werden, oder aber die Datenträger können bei einer Durchsuchung beschlagnahmt werden.

Allerdings gilt es nun zu prüfen, welche Ausnahmen gelten, wann also von Unternehmen gespeicherte Daten ausnahmsweise nicht zu Strafverfolgungszwecken zur Verfügung stehen.

1. Berufsgeheimnisträger

Nach § 97 StPO dürfen Daten, die Rechtsanwälte, Wirtschaftsprüfer, Journalisten, Ärzte und Psychologen (Berufsgeheimnisträger) – bzw. deren Unternehmen – im Rahmen ihrer beruflichen Tätigkeit gespeichert haben, nur beschlagnahmt werden, wenn diese selbst im Verdacht stehen, eine Straftat begangen oder sich an einer Straftat beteiligt zu haben. Dieser Schutz entfällt aber dem Wortlaut des § 97 Abs. 2 S. 1 StPO zufolge, wenn die Daten nicht mehr „im Gewahrsam“ des Berufsgeheimnisträgers sind. Dabei ist auf die primäre Verfügungsberechtigung über die Daten abzustellen – und nicht auf die Datenträger, also Festplatten –, um den Schutzzweck der Norm zu verwirklichen: den Schutz des Vertrauensverhältnisses zu diesen Berufsgeheimnisträgern. Daher sind auch solche Daten geschützt, die bei externen Dienstleistern – etwa auf einer Internetfestplatte bzw. in der sogenannten „Cloud“ – abgespeichert sind.[27]

2. Datenspeicherung im Ausland

International tätige Unternehmen haben oft ihre Rechenzentren auf mehrere Standorte verteilt. Wenn sich nun die Anfrage deutscher Strafverfolgungsbehörden auf Daten bezieht, die – vielleicht zufälligerweise – im Ausland gespeichert sind, so zeigen sich gerade Großunternehmen meistens kooperativ, transferieren diese Daten ins Inland und händigen sie den Strafverfolgungsbehörden aus. Doch ist dies rechtmäßig?

Völkerrechtlich unzulässig ist es, wenn Strafverfolgungsbehörden Unternehmen dazu *verpflichten*, Auskunft auch über solche Daten im Ausland zu erteilen.[28] Das wird deutlich, wenn man die hypothetische Alternative betrachtet, wenn das Unternehmen die Auskunft verweigern würde: Dann müsste eine Beschlagnahme des Datenträgers *im Ausland* er-

[22] LG Bonn BKR 2003, 914; *Meyer-Goßner*, Strafprozessordnung, Kommentar, 55. Aufl. 2012, § 95 Rn. 2 m.w.N.; vgl. auch *Erb*, in: Erb u.a. (Fn. 8), § 161 Rn. 28a.

[23] So i.E. auch KG NStZ 1989, 192; *Ciolek-Krepold*, Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen, 2000, Rn. 200 ff.; *Eisenberg* (Fn. 7), Rn. 2373; *Nack*, in: Hannich (Fn. 7), § 95 Rn. 3; *Schäfer* (Fn. 17), § 95 Rn. 20 m.w.N.

[24] Da sich diese gegen einen Unverdächtigen richtet, ist sie nur unter einschränkenden Voraussetzungen (§ 103 StPO) zulässig, d.h. es müssen „Tatsachen vorliegen, aus denen zu schließen ist, daß die gesuchten“ Daten sich „in den zu durchsuchenden Räumen befinden“. Das aber schließt nur Durchsuchungen „ins Blaue hinein“ aus.

[25] *Schäfer* (Fn. 17), § 103 Rn. 8; *Meyer-Goßner* (Fn. 22), § 103 Rn. 1a m.w.N.

[26] Aus diesem Grund war es entgegen LG Darmstadt (Beschl. v. 7.8.2011 – 25 Gs 1000 AR 200594/11) rechtswidrig, dass auf Grundlage eines französischen Rechtshilfeersuchens Computersysteme der in Deutschland erstarkenden Piratenpartei beschlagnahmt wurden, weil man auf Daten zugreifen wollte, die dort von verdächtigen Dritten abgespeichert wurden. Stattdessen hätte ein Auskunftsverlangen ergehen müssen.

[27] *Nack* (Fn. 23), § 97 StPO Rn. 8.

[28] LG Hamburg StV 2009, 70 (71); *Meyer-Goßner* (Fn. 22), § 110 Rn. 7a; *Brodowski*, JR 2010, 402 (411); *Gaede*, StV 2009, 96 (101 f.); *Gercke*, StraFo 2009, 271 (272 f.); *Obenhaus*, NJW 2010, 651 (654); s. hierzu auch *Kudlich*, GA 2011, 193 (208).

folgen. Das aber darf aus völkerrechtlicher Sicht nur über den ausländischen Staat geschehen. Da ein Auskunftsverlangen eine Beschlagnahme nur ersetzt, aber gleichermaßen ein Zwangsmittel darstellt, kann für dieses nichts anderes gelten – auch nicht zwischen den Mitgliedstaaten der Europäischen Union.[29]

Dürfen Unternehmen aber freiwillig Auskunft erteilen über Daten, die im Ausland gespeichert sind? Das ist dann zulässig, wenn eine „rechtmäßige und freiwillige Zustimmung" der Person vorliegt, die „rechtmäßig befugt" ist, die Daten zu transferieren.[30] Abzustellen ist dabei erneut auf denjenigen, der primär verfügungsberechtigt über die Daten ist. Das ist bei Daten über Finanztransaktionen die Bank, aber etwa bei Internet-Festplatten oder einer Datenspeicherung in der „Cloud" der jeweilige Kunde. In letzterem Fall ist daher der justizförmige Weg zu wahren und ein Rechtshilfeersuchen zu stellen.

3. Verhältnismäßigkeit

Alle Eingriffe erfordern schließlich aus verfassungsrechtlicher Sicht, dass sie verhältnismäßig sind: Datenabfragen bei Unternehmen verfolgen ohne weiteres ein legitimes Ziel – die Strafverfolgung – und sind regelmäßig auch geeignet und erforderlich. Bei der Angemessenheit des Datenzugriffs ist aber in mehrerlei Hinsicht Vorsicht geboten:

Erstens ist zu hinterfragen, inwieweit auf die Vertraulichkeit der Kommunikation eingewirkt wird, selbst wenn sich der Zugriff nur auf archivierte Kommunikation bezieht – denn wer löscht heutzutage noch seine E-Mails? Exzessive staatliche Zugriffe auf Kommunikation führen nämlich beim Bürger zu einem generellen Gefühl des Überwacht-Seins. Das aber kann zur Gefahr übermäßig konformen, angepassten Verhaltens und auch zur reduzierten Teilhabe am freiheitlich-demokratischen Gemeinwesen führen.[31] Dies gilt es zu vermeiden, zumal ein freies und freiheitliches Internet ein notwendiger Ausgleich ist für die zunehmende Mobilität und Flexibilität von Personen: Wenn Personen sich nämlich nicht mehr in ihre Wohnungen zur geschützten Kommunikation mit nahen Angehörigen und Freunden zurückziehen können, so benötigen sie trotzdem einen Kommunikationspfad, in dem sie frei – und regelmäßig auch frei von staatlicher Überwachung – kommunizieren können. Das Internet bietet diese besondere Chance, und diese gilt es zu bewahren.

Zweitens ist das mehrpolige Grundrechtsverhältnis – auch zu mitbetroffenen Dritten – zu berücksichtigen. Das gilt umso mehr, je atypischer die Datenabfragen werden und je höher daher das Risiko unbeteiligter und unbescholtener Dritter wird, selbst in das Visier strafrechtlicher Ermittlungen zu geraten.[32] Im Sinne eines rechtsstaatlich-liberalen Strafrechtsverständnisses wiegen Strafverfolgungen gegen Unschuldige nämlich weitaus schwerer als die Nichtverfolgung von Tätern. Daher ist ein data mining, etwa bei Finanztransaktionen, bei Verbindungsdaten oder bei Flugdaten nur unter ganz besonders strikten Voraussetzungen und Verfahrenssicherungen für zulässig zu erachten.

Drittens dürfen solche Zugriffe nicht mit dem Hinweis darauf bagatellisiert werden, es handele sich nur um von Unternehmen und nicht von staatlicher Seite erfasste und gespeicherte Daten. Gefahren für die Privatsphäre gingen daher von diesen Unternehmen und gerade nicht von Seiten des Staates aus. Diese Argumentation ist nicht tragfähig: Zum einen führte sie dazu, dass staatliche Behörden (zu) exzessive Datenspeicherungen wenigstens duldeten, wenn nicht sogar implizit befürworteten, anstatt diesen entschlossen entgegenzutreten. Zum anderen ließe sie außer Acht, dass durch eine staatliche (Zweit-)Nutzung von Datenbeständen eine gänzlich andere, weitaus intensivere Grundrechtsgefährdung vorliegt.

V. Anwendung auf die drei Fallbeispiele

Was bedeutet all dies nun für die drei eingangs genannten Fallbeispiele?

Im *Fall 1* – der Suche nach Finanztransaktionen, die ein bestimmtes Konto zum Ziel hatten – akzeptierte das Bundesverfassungsgericht das Vorgehen; es verlangte nicht einmal einen präventiven Richtervorbehalt. Das Risiko, dass Unschuldige verfolgt werden können, bezeichnete es trotz der höchst ungewöhnlichen und daher risikobehafteten Datenabfrage als „unvermeidlich"[33]. Mit der hier vertretenen Auffassung überzeugt das nicht, denn die freiwillige Mitwirkung der Banken war datenschutzrechtlich unzulässig und durfte daher von der Staatsanwaltschaft auch nicht eingefordert werden. Stattdessen wäre zumindest ein richterliches Auskunftsersuchen notwendig gewesen.

Ebenfalls bedenklich ist der *Fall 2*: Dass sich die Polizei über die Begrenzungen des richterlichen Beschlusses hinwegsetzte, demzufolge nur auf E-Mails eines bestimmten Zeitraums zugegriffen werden sollte, und sichtlich gezielt nach Zufallsfunden suchte, begründet einen derart schwerwiegenden Verfahrensmangel, dass ein Beweisverwertungsverbot zu bejahen ist. Eine andere Auffassung vertritt freilich das zuständige Landgericht Mannheim.[34]

[29] Sowohl die Europäische Beweisanordnung (ABl. EU 2008 Nr. L 350 v. 29.12.2008, S. 72) als auch die geplante Europäische Ermittlungsanordnung (zuletzt Ratsdok. 18918/11) sehen keine unmittelbare Beweiserhebung eines Staates im Hoheitsgebiet eines anderen Staates vor, sondern nur eine erleichterte Zusammenarbeit beider Staaten. Allein bei Telekommunikationsüberwachungen, die grenzüberschreitend und ohne Mitwirkung des anderen Staates durchgeführt werden können, gestattet das europäische Beweiserhebungsrecht die unmittelbare Durchführung einer transnationalen Beweiserhebung, kombiniert allerdings mit einer Notifikationspflicht und der Möglichkeit des betroffenen anderen Staates, dieser zu widersprechen (Art. 20 Rechtshilfeübereinkommen-2000 [ABl. EU 2000 Nr. C 197 v. 12.7.2000, S. 3]; Art. 27d Europäische Ermittlungsanordnung-E).

[30] So die Formulierung des Art. 32 lit. b Übereinkommen des Europarats über Computerkriminalität v. 23.11.2001 (BGBl. II 2008, S. 1242) – SEV 185, der kodifiziertes Völkergewohnheitsrecht darstellen dürfte.

[31] Vgl. BVerfGE 65, 1 (43).

[32] *Brodowski*, JR 2010, 546 (547, 549).

[33] BVerfGK 15, 71 (82).

[34] LG Mannheim StV 2011, 352.

Im *Fall 3* – der Gesichtserkennung mittels Facebook – würde nur auf Daten eines einzelnen Unternehmens zugegriffen. Zudem scheint sich die Rechtspraxis bei einer freiwilligen Mitwirkung des Unternehmens über die Frage hinwegzusetzen, ob die maßgeblichen Daten zuvor im Ausland gespeichert waren. Daher wage ich die Prognose, dass die Rechtsprechung auch dieses Vorgehen als rechtmäßig erachten würde.

VI. Fazit

Daten, die Privatpersonen Unternehmen zur Speicherung oder Verarbeitung anvertraut haben, sind für die Strafverfolgungsbehörden ohne größere Schwierigkeiten verfügbar; ein Grundsatz der Verfügbarkeit ist in diesem Verhältnis umfassend verwirklicht. Dieses Ergebnis folgt angesichts der in Deutschland vorherrschenden Rechtsprechung: Die freiwillige Mitwirkung von Unternehmen erachtet sie in weiten Teilen als unproblematisch, selbst wenn das Unternehmen hierzu auf im Ausland gespeicherte Daten zugreift. Eine Rasterfahndung sieht sie nur dann für gegeben an, wenn Datenbestände *mehrerer* Unternehmen abgeglichen werden. Das Risiko der Strafverfolgung Unschuldiger wird als „unvermeidliche Gefahr“[35] heruntergespielt. Auch auf Verfahrenssicherungen – also auf einen präventiven Richtervorbehalt – verzichtet jedenfalls ein Teil der Rechtsprechung. An diesen Maßstäben würde auch der nunmehr von der Europäischen Kommission vorgelegte Vorschlag für eine Richtlinie über den Datenschutz in der Strafverfolgung[36] nichts ändern, denn dieser gestattet es den Strafverfolgungsbehörden generell, Daten zur Wahrnehmung ihrer gesetzlicher Aufgabe – also der Strafverfolgung – zu erheben und zu verarbeiten. Hingegen sind in diesem Entwurf keine über weiche Generalklauseln hinausgehenden nennenswerten Verfahrenssicherungen oder materiellen Einschränkungen vorgesehen.

All dies stimmt bedenklich: Es thematisiert nur unzureichend das mehrpolige Grundrechtsverhältnis, in dem auch die Grundrechtspositionen derjenigen zu berücksichtigen sind, die als unbescholtene Bürger von einer Strafverfolgungsmaßnahme mitbetroffen sind. Nicht zu unterschätzen sind ferner die aufgezeigten Kollateralschäden für das freiheitlich-demokratische Gemeinwesen. Schließlich ist auch grundsätzlich zu hinterfragen, ob es nur positiv ist, wenn der Staat auf nahezu sämtliche Datenbestände schrankenlos zugreifen kann. Es spricht nämlich vieles dafür, anerkannte Institute wie dasjenige der beleidigungsfreien Sphäre[37] auch normativ zu stärken und behutsam auf andere Vertrauensverhältnisse und Kommunikationsinhalte zu erstrecken.

Was ist angesichts der aufgezeigten Risiken einer zu weitgehenden Verfügbarkeit von Daten zu fordern? Erstens eine Zurückhaltung der Strafverfolgungsbehörden bei sämtlichen Maßnahmen – wie etwa bei data mining –, die mit einem hohen Risiko verbunden sind, dass Unschuldige ins Visier der Strafverfolger geraten. Zweitens ist der präventive Richtervorbehalt bei Auskunftsverlangen zu stärken. Drittens darf die Verhältnismäßigkeitsprüfung nicht zu einer bloßen Formsache verkommen, sondern muss von Polizei, Staatsanwaltschaft und (Ermittlungs-)Richtern ernst genommen werden. Viertens vertragen Demokratie und Freiheitlichkeit kein Ende der Privatsphäre – daher ist auf Datenbestände von Unternehmen von staatlicher Seite nur zurückhaltend zuzugreifen, um nicht mit schlechtem Beispiel voranzuschreiten. Vielmehr ist es staatliche Pflicht, die so oft unterschätzte Bedeutung der Privatheit von Daten zu unterstreichen.

[35] BVerfGK 15, 71 (82).

[36] Vorschlag für [eine] Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM (2012) 10 endg. v. 25.1.2012.

[37] S. nur *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 8), Vorbem. §§ 185 ff. Rn. 9 m.w.N.