

zu der Internetseite mussten 79,99 \$ per Kreditkarte gezahlt werden. Die Staatsanwaltschaft versuchte, die Kunden dieser Internetseite zu ermitteln. Sie schrieb daher die Institute an, die Mastercard- und Visa-Kreditkarten in Deutschland ausgeben, und forderte sie auf, alle Kreditkartenkonten anzugeben, die seit dem 1.3.2006 eine Überweisung von 79,99 \$ an die philippinische Bank aufwies, über die der Geldtransfer für den Betreiber der Internetseite abgewickelt wurde. Anschließend teilte die Staatsanwaltschaft noch die zwischenzeitlich bekannt gewordene »Merchant-ID«, die dem Zahlungsempfänger durch die Bank zugewiesene Ziffernfolge, für den Betreiber der Internetseite mit. Die Unternehmen übermittelten der Staatsanwaltschaft daraufhin die erbetenen Informationen, wobei in einem Fall zunächst ein Gerichtsbeschluss erwirkt werden musste. Insgesamt wurden so 322 Karteninhaber ermittelt.

2. Die Beschwerdeführer, die Inhaber von Kreditkarten sind, die von deutschen Banken ausgegeben wurden, beantragten beim Amtsgericht Halle die Feststellung, dass die Datenabfrage der Staatsanwaltschaft rechtswidrig gewesen sei. [...]

**II.** Mit den fristgerecht erhobenen Verfassungsbeschwerden rügen die Beschwerdeführer eine Verletzung ihres Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. [...]

*Aus den Gründen:*

[...]

**15** Die Verfassungsbeschwerden werden nicht zur Entscheidung angenommen, weil die Annahmenvoraussetzungen des § 93 a Abs. 2 BVerfGG nicht vorliegen. Die Verfassungsbeschwerden haben keine Aussicht auf Erfolg. Sie sind unbegründet. Die angegriffenen Entscheidungen verletzen die Beschwerdeführer nicht in ihren Grundrechten oder grundrechtsgleichen Rechten.

**16** Die Datenabfrage der Staatsanwaltschaft und die sie bestätigenden Gerichtsentscheidungen verletzen die Beschwerdeführer nicht in ihrem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

**17** 1. Die Abfrage der Kreditkartendaten durch die Staatsanwaltschaft war kein Eingriff in das Recht auf informationelle Selbstbestimmung der Beschwerdeführer, deren Kreditkartendaten bei den Unternehmen nur maschinell geprüft, mangels Übereinstimmung mit den Suchkriterien aber nicht als Treffer angezeigt und der Staatsanwaltschaft daher nicht übermittelt wurden.

**18** a) Das Grundrecht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (vgl. BVerfGE 65, 1, 43). Es sichert seinen Trägern insbesondere Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe der auf sie bezogenen, individualisierten oder individualisierbaren Daten (vgl. BVerfGE 65, 1, 43; 67, 100, 143; 84, 239, 279; 103, 21, 33; 115, 320, 341).

**19** b) Die Kreditkartendaten der Beschwerdeführer wurden in diesem Fall jedoch nicht durch eine staatliche Stelle oder auf deren Veranlassung erhoben, gespeichert, verwendet oder weitergegeben. Ihre bei den Kreditkartenunternehmen gespeicherten Daten wurden nicht an die Strafverfolgungsbehörden übermittelt oder dort zur weiteren Verwendung gespeichert. Durch den automatischen Suchlauf, den die Kreditkartenunternehmen

**GG Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1; StPO §§ 95 Abs. 1; 98 Abs. 2; 98 a; 160 Abs. 1; 161 Abs. 1; 161 a Abs. 1; BDSG § 28 Abs. 2.**

1. Es liegt kein Eingriff in das Recht auf informationelle Selbstbestimmung vor, soweit personenbezogene Daten auf Veranlassung der Strafverfolgungsbehörden bei einem automatischen Suchlauf sogleich anonym und spurenlos ausgeschieden werden und daher nicht im Zusammenhang mit dieser Ermittlungsmaßnahme behördlich zur Kenntnis genommen werden.

2. § 161 Abs. 1 StPO genügt den verfassungsrechtlichen Anforderungen an eine gesetzliche Ermächtigung, die freiwillige Auskunft von Kreditkartenunternehmen einzuholen, mittels welcher Kreditkarten näher spezifizierte Transaktionen vorgenommen wurden.

BVerfG, Kammerbeschl. v. 17. 2. 2009 – 2 BvR 1372/07 und 2 BvR 1745/07.

**I.** 1. Die Staatsanwaltschaft Halle leitete im Jahr 2006 ein Ermittlungsverfahren gegen Unbekannt ein, nachdem sie auf eine Internetseite aufmerksam geworden war, die den Zugang zu kinderpornographischen Inhalten vermittelte. Für den Zugang

auf Veranlassung der Staatsanwaltschaft durchführten, wurden die Daten der Beschwerdeführer maschinell geprüft, aber mangels Erfüllung der Suchkriterien schon bei den Unternehmen nicht als Treffer angezeigt. Ihre Daten wurden daher nie an die Staatsanwaltschaft weitergegeben, und die Staatsanwaltschaft hatte keine Möglichkeit, den Datenbestand der Kreditkartenunternehmen für eigene Abfragen zu benutzen. Für die Annahme eines Eingriffs genügt es nicht, dass die Daten bei den Unternehmen in einen maschinellen Suchlauf mit eingestellt wurden, da ihre Daten anonym und spurenlos aus diesem Suchlauf ausgeschieden wurden und nicht im Zusammenhang mit dieser Ermittlungsmaßnahme behördlich zur Kenntnis genommen wurden (vgl. BVerfGE 100, 313, 366; 107, 299, 328; 115, 320, 343).

20 2. Die Maßnahme der Staatsanwaltschaft beruhte auf der Ermächtigungsgrundlage des § 161 Abs. 1 StPO. Diese Vorschrift stellt eine ausreichende gesetzliche Grundlage für diese Ermittlungsmaßnahme dar.

21 a) Bei der vorliegenden Maßnahme handelte es sich nicht um eine Rasterfahndung im Sinne von § 98 a StPO oder eine ähnliche Maßnahme, die an den Voraussetzungen dieser Ermächtigungsgrundlage zu messen wäre. Datenermittlungen wie die hier vorliegende, welche die besonderen Merkmale einer Rasterfahndung nicht aufweisen und sich auf andere Ermächtigungsgrundlagen stützen lassen, werden dagegen durch § 98 a StPO nicht ausgeschlossen (»unbeschadet §§ 94, 110, 161«).

22 Die Rasterfahndung ist eine besondere Fahndungsmethode unter Nutzung der elektronischen Datenverarbeitung. Die Strafverfolgungsbehörde lässt sich von anderen öffentlichen oder privaten Stellen personenbezogene Daten übermitteln, um einen automatisierten Abgleich (Rasterung) mit anderen Daten vorzunehmen. Durch den Abgleich soll diejenige Schnittmenge von Personen ermittelt werden, auf welche bestimmte, vorab festgelegte und für die weiteren Ermittlungen als bedeutsam angesehene Merkmale zutreffen (vgl. BVerfGE 115, 320, 321). Es handelt sich dabei um einen automatisierten Vergleich personenbezogener Daten, die in Dateien anderer Stellen als Strafverfolgungsbehörden gespeichert sind, mit Hilfe fallspezifischer kriminalistischer Prüfungskriterien (vgl. Schäfer in: Löwe-Rosenberg, StPO, 25. Aufl. 2004, § 98 a Rdn. 2).

23 Dagegen liegt keine Rasterfahndung vor, wenn die Strafverfolgungsbehörde von privaten Stellen Auskünfte zu speziellen Täter-Daten erhält, also nicht die Gesamtdaten zum weiteren Abgleich mit anderen Dateien übermittelt bekommt (vgl. Schäfer in: Löwe-Rosenberg, StPO, 25. Aufl. 2004, § 98 a Rdn. 4; Jäger in: KMR-StPO, Stand: Juni 2008, § 98 a Rdn. 4; Hilger NStZ 1992, S. 457, 460). Kern der Rasterfahndung ist der Abgleich der herausgefilterten Datenbestände mehrerer Speicherstellen, der die Verknüpfung verschiedener Sachbereiche ermöglicht, um ein Persönlichkeitsprofil zu erstellen. Die Suchabfrage in Dateien derselben Speicherstelle ist keine Rasterfahndung (vgl. OLG Stuttgart, Beschl. v. 6. 9. 2000 – 2 Ws 109/00 –, NStZ 2001, S. 158, 159; OLG Köln, Beschl. v. 6. 10. 2000 – 2 Ws 413/00, 2 Ws 414/00 –, NStZ-RR 2001, S. 31; Nack, in: Karlsruher Kommentar zur StPO, 6. Aufl. 2008, § 98 a Rdn. 5; Meyer-Göfner StPO, 51. Aufl. 2008, § 98 a Rdn. 8; Jäger in: KMR-StPO, Stand: Juni 2008, § 98 a Rdn. 7; Wohlers in: SK-StPO, Stand: Mai 2008, § 98 a Rdn. 4). Die §§ 98 a, 98 b StPO gelten auch dann nicht, wenn die ersuchten Stellen selbst einen Datenabgleich durchführen (vgl. BTDrucks 12/989, S. 37; Hilger NStZ 1992, S. 457, 460 Fn. 60). Die Unternehmen haben hier der Staatsanwaltschaft nur eine Auskunft über bei ihnen gespeicherte Daten erteilt,

nachdem sie einen internen Suchlauf durchgeführt hatten. Ein Abgleich zwischen den Datensätzen verschiedener Speicherstellen fand nicht statt.

24 Die Wirkung und Eingriffsintensität der Anfrage der Staatsanwaltschaft und der dadurch veranlassten Übermittlung der Daten entspricht auch nicht der einer Rasterfahndung, so dass kein Anlass für eine entsprechende Anwendung der §§ 98 a, 98 b StPO besteht (so aber Schnabel DuD 31 (2007) S. 426, 427 f.). Bei der Rasterfahndung nach § 98 a StPO werden »Daten von Personen, die bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen«, mit anderen Daten maschinell abgeglichen. Über das technische Kriterium hinaus, ob dabei Datensätze einer oder mehrerer Speicherstellen abgefragt werden, hat die hier durchgeführte Abfrage eine materiell andere, deutliche geringere Eingriffsintensität. Bei der Rasterfahndung wird nach Personen gesucht, die mehrere allgemeine Merkmale aufweisen oder – bei der negativen Rasterfahndung – gerade nicht aufweisen, welche auf den Täter vermutlich zutreffen. Die Rasterfahndung dient so dem »Hinarbeiten« auf die Personen, die das nach kriminalistischen Erfahrungen festgelegte »Verdächtigenprofil« erfüllen (vgl. BTDrucks 12/989, S. 37). Durch den Abgleich auf Grundlage dieser allgemeinen Merkmale werden regelmäßig auch zahlreiche unbeteiligte Personen, die zufällig bestimmte tätertypische Merkmale erfüllen, zum Gegenstand der Überprüfung im Ermittlungsverfahren, obwohl im Übrigen keine tatsächlichen Anhaltspunkte für ihre Eigenschaft als Verdächtige vorliegen (vgl. BTDrucks 12/989, S. 37; Schäfer in: Löwe-Rosenberg, StPO, 25. Aufl. 2004, § 98 a Rdn. 12). Mit der hier durchgeführten Abfrage der Kreditkartendaten wurde dagegen gezielt nach Personen gesucht, die eine genau bezeichnete, nach dem damaligen Ermittlungsstand mit hinreichender Wahrscheinlichkeit strafbare Handlung vorgenommen haben: das Zahlen eines bestimmten Betrages per Kreditkarte an einen bestimmten Empfänger innerhalb eines bestimmten Zeitraums, wodurch sie sich wahrscheinlich den Besitz kinderpornographischer Schriften verschafften. Kreditkarteninhaber, zu denen keine solche Abbuchung gespeichert war, wurden dagegen nicht als »Treffer« angezeigt und waren in ihren Grundrechten nicht betroffen.

25 b) Die Maßnahme wurde daher zulässigerweise auf § 161 Abs. 1 StPO gestützt.

26 aa) § 161 Abs. 1 StPO stellt als Ermittlungsgeneralklausel die Ermächtigungsgrundlage für Ermittlungen jeder Art dar, die nicht mit einem erheblichen Grundrechtseingriff verbunden sind und daher keiner speziellen Eingriffsermächtigung bedürfen. Sie ermächtigt die Staatsanwaltschaft zu den erforderlichen Ermittlungsmaßnahmen, die weniger intensiv in Grundrechte des Bürgers eingreifen (vgl. Griesbaum in: Karlsruher Kommentar zur StPO, 6. Aufl. 2008, § 161 Rdn. 1; Erb in: Löwe-Rosenberg, StPO, 26. Aufl. 2008, § 161 Rdn. 2; Wohlers in: SK-StPO, Stand: Mai 2008, § 161 Rdn. 4). Die Staatsanwaltschaft kann auf dieser Grundlage in freier Gestaltung des Ermittlungsverfahrens die erforderlichen Maßnahmen zur Aufklärung von Straftaten ergreifen (vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 18. 9. 1995 – 2 BvR 103/92 –, NStZ 1996, S. 45). § 161 Abs. 1 StPO bildet auch die Rechtsgrundlage für die allgemeine Erhebung personenbezogener Daten (vgl. Erb in: Löwe-Rosenberg, StPO, 26. Aufl. 2008, § 161 Rdn. 3 b) und damit für eine Ermittlungsanfrage der Staatsanwaltschaft gegenüber privaten Stellen wie den hier betroffenen Kreditkartenunternehmen.

27 bb) Die Abfrage von Kreditkartendaten, die sich auf eine

konkret beschriebene Tathandlung beziehen, berührt die Kreditkarteninhaber, welche die Tatkriterien erfüllten und deren Daten daher an die Staatsanwaltschaft übermittelt wurden, zwar in ihrem Recht auf informationelle Selbstbestimmung. § 161 Abs. 1 StPO genügt den Anforderungen an eine Ermächtigungsgrundlage für einen Eingriff dieser Art und dieses Umfangs. Ein Auskunftersuchen der Staatsanwaltschaft, das darauf gerichtet ist, dass Private in den bei ihnen gespeicherten Daten maschinell nach Personen suchen, gegen die sich aufgrund konkret beschriebener Umstände der Verdacht einer Straftat richtet, kann auf diese Ermächtigungsgrundlage gestützt werden (a. A. *Petri StV* 2007, S. 266, 268). Eine darüber hinausgehende Spezialermächtigung ist nicht deswegen erforderlich, weil der Staat sich so Daten verschafft, die von den Dateninhabern nicht für seinen Zugriff bestimmt waren, oder weil die Ermittlungsmaßnahme heimlich erfolgte (a. A. *Hefendehl StV* 2001, S. 700, 703).

**28** Die Ermittlungsmaßnahme war nicht deswegen unzulässig, weil sie von den Kreditkarteninhabern unbemerkt erfolgte. Die Heimlichkeit eines polizeilichen Vorgehens ist kein Umstand, der nach der Strafprozessordnung für sich allein schon die Unzulässigkeit der ergriffenen Maßnahmen begründet (vgl. BGHSt 39, 335, 346; 42, 139, 150). Es gilt der Grundsatz der freien Gestaltung des Ermittlungsverfahrens, der auch das verdeckte Führen von Ermittlungen erlaubt (vgl. *Griesbaum* in: *Karlsruher Kommentar zur StPO*, 6. Aufl. 2008, § 161 Rdn. 12; *Erb* in: *Löwe-Rosenberg, StPO*, 26. Aufl. 2008, § 160 Rdn. 42 a). Ermittlungen in Heimlichkeit sind eine unabdingbare Voraussetzung des Erfolgs einer Reihe von Maßnahmen der Strafverfolgung, die nicht allein deshalb rechtsstaatswidrig sind (vgl. BVerfGE 109, 279, 325).

**29** Der Umstand allein, dass das Erfragen gespeicherter, nicht allgemein zugänglicher Daten in das Grundrecht auf informationelle Selbstbestimmung eingreift, führt nicht dazu, dass hierfür bereits eine über § 161 StPO hinausgehende Spezialermächtigung erforderlich wäre. Die Erforschung von Straftaten berührt ihrem Wesen nach immer Persönlichkeitsrechte des Beschuldigten und Dritter und ist schon begrifflich mit der Erhebung und Verarbeitung personenbezogener Daten verbunden. Jede polizeiliche Vernehmung, bei der ein Zeuge seine Kenntnisse über andere Personen und deren Verhalten mitteilt, ist eine Erhebung personenbezogener Daten (vgl. *Kramer NJW* 1992, S. 2732, 2735). Maßgeblich für die Frage der erforderlichen Ermächtigungsgrundlage ist daher die Eingriffsintensität. Grundrechtseingriffe weisen dann eine hohe Eingriffsintensität auf, wenn sie sowohl durch Verdachtlosigkeit als auch durch eine große Streubreite gekennzeichnet sind, wenn also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben (vgl. BVerfGE 100, 313, 376, 392; 107, 299, 320 f.; 109, 279, 353; 113, 29, 53; 113, 348, 383). Daran gemessen wies die hier vorgenommene Maßnahme nur eine geringe Eingriffsintensität auf. Die Staatsanwaltschaft erfragte hier aufgrund konkreter Tatstände – Abbuchungsbetrag, Zeitraum, Empfängerbank, Merchant-ID des Empfängers – bei privaten Stellen freiwillige Auskünfte über Personen, gegen die aufgrund dieser Umstände ein zureichender Tatverdacht bestand. Durch eine Datenübermittlung an die Strafverfolgungsbehörden betroffen war nur ein eng begrenzter und präzise beschriebener Personenkreis, der nach dem damaligen Ermittlungsstand durch sein Verhalten den Tatverdacht begründet hatte. Die Daten sonstiger Kreditkarteninhaber wurden dagegen nicht übermittelt.

**30** cc) Beschränkungen des Art. 2 Abs. 1 GG bedürfen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (vgl. BVerfGE 65, 1, 44; 113, 29, 50; 115, 166, 190). Hinreichend bestimmt ist ein Gesetz, wenn sein Zweck aus dem Gesetzestext in Verbindung mit den Materialien deutlich wird (vgl. BVerfGE 65, 1, 54). Diese Voraussetzungen erfüllt § 161 Abs. 1 StPO für Eingriffe der hier vorliegenden Art. Der den Datenzugriff begrenzende Verwendungszweck ist hinreichend präzise vorgegeben. Die Ermittlungsmethoden der Strafprozessordnung sind zwar im Hinblick auf die Datenerhebung und den Datenumfang weit gefasst. Die jeweiligen Eingriffsgrundlagen, so auch § 161 Abs. 1 StPO, stehen aber unter einer strengen Begrenzung auf den Ermittlungszweck der Aufklärung von Straftaten (vgl. BVerfGE 113, 29, 52). Auf die Ermittlung anderer Lebenssachverhalte und Verhältnisse erstrecken sich die Eingriffsermächtigungen nicht. Bei einer strafrechtlichen Ermittlung dürfen daher keine Sachverhalte und persönlichen Verhältnisse ausgeforscht werden, die für die Beurteilung der Täterschaft und für die Bemessung der Rechtsfolgen der Tat nicht von Bedeutung sind. Mit dieser strengen Begrenzung sämtlicher Ermittlungen und damit auch der Datenerhebung auf den Zweck der Tataufklärung begrenzt die Strafprozessordnung die Eingriffe in das Recht an den eigenen Daten grundsätzlich auf diejenigen, die für die Strafverfolgung im konkreten Anlassfall von Bedeutung sind (vgl. BVerfGE 113, 29, 52). Die strafprozessualen Ermächtigungen erlauben damit einen Eingriff in das Recht auf informationelle Selbstbestimmung, finden ihre Grenze aber in der Zweckbestimmung für das jeweilige Strafverfahren (vgl. BVerfGE 113, 29, 52). Voraussetzung für Ermittlungsmaßnahmen nach § 161 Abs. 1 StPO sind zureichende tatsächliche Anhaltspunkte einer Straftat (§ 152 Abs. 2 StPO). Eine Aufzählung aller kriminalistischen Vorgehensweisen, die von § 161 Abs. 1 StPO erfasst werden, ist dagegen nicht möglich und für Maßnahmen, die mit weniger intensiven Grundrechtseingriffen verbunden sind, auch nicht erforderlich.

**31** dd) Die Maßnahme hält sich auch innerhalb der Grenzen, die der Grundsatz der Verhältnismäßigkeit allen Ermittlungshandlungen setzt. Der Grundsatz der Verhältnismäßigkeit verlangt, dass die jeweilige Maßnahme einen verfassungsrechtlich legitimen Zweck verfolgt und zu dessen Erreichung geeignet, erforderlich und verhältnismäßig im engeren Sinne ist. Der Eingriff darf den Betroffenen nicht übermäßig belasten, muss diesem also zumutbar sein (vgl. BVerfGE 63, 131, 144).

**32** Die wirksame Strafverfolgung ist ein legitimer Zweck zur Einschränkung des Rechts auf informationelle Selbstbestimmung. Die Sicherung des Rechtsfriedens durch Strafrecht ist seit jeher eine wichtige Aufgabe staatlicher Gewalt. Die Aufklärung von Straftaten, die Ermittlung des Täters, die Feststellung seiner Schuld und seine Bestrafung wie auch der Freispruch des Unschuldigen sind die wesentlichen Aufgaben der Strafrechtspflege, die zum Schutz der Bürger den staatlichen Strafanspruch in einem justizförmigen und auf die Ermittlung der Wahrheit ausgerichteten Verfahren in gleichförmiger Weise durchsetzen soll. Strafnormen und deren Anwendung in einem rechtsstaatlichen Verfahren sind Verfassungsaufgaben (vgl. BVerfGE 107, 104, 118 f.; 115, 166, 192). Der Verhinderung und Aufklärung von Straftaten kommt daher nach dem Grundgesetz eine hohe Bedeutung zu (vgl. BVerfGE 100, 313, 388; 115, 166, 192).

**33** Zur Erreichung des Zwecks, die einer Straftat nach § 184 b Abs. 4 StGB verdächtigen Personen zu ermitteln, war die Maß-

nahme geeignet. Mildere, ebenso geeignete Mittel waren hier nicht ersichtlich. Ein Rechtshilfeersuchen an die Philippinen, um die Zahlungseingänge bei der dortigen Empfängerbank zu ermitteln, konnte die Staatsanwaltschaft aufgrund der unabsehbaren zeitlichen Verzögerung und unsicheren Erfolgsaussicht als weniger geeignet ansehen. Die Internetnutzer, die sich Zugang zu der Internetseite mit den kinderpornographischen Inhalten verschafft haben, konnten auch nicht über eine Anfrage bei den Anbietern von Internetzugangsdiensten ermittelt werden, da diese keine Daten über aufgerufene Internetseiten speichern. Auch der nach der hier zu beurteilenden Maßnahme, am 1. 1. 2008 in Kraft getretene § 113 a TKG n. F. verbietet in seinem Absatz 8 eine Speicherung der Daten über aufgerufene Internetseiten.

34 In der Abwägung mit dem Zweck, Täter zu ermitteln, die sich den Besitz kinderpornographischer Schriften verschafft haben, ist das Gewicht des Eingriffs in das Recht auf informationelle Selbstbestimmung, der mit der Abfrage der Kreditkartendaten verbunden war, geringer zu bewerten. Betroffen wurden dadurch regelmäßig nur Personen, die durch ihr Verhalten den hinreichenden Verdacht einer Straftat begründet hatten. Ermittelt wurden die Datenspuren, die mit Wahrscheinlichkeit durch die Tathandlung selbst hinterlassen wurden. Eine darüber hinausgehende Ausforschung fand nicht statt. Die bei Ermittlungsmaßnahmen unvermeidliche Gefahr, dass ein Unschuldiger zunächst verdächtig erscheinen könnte, etwa wenn mit einer gestohlenen Kreditkarte bezahlt wurde, Buchungen falsch gespeichert wurden oder sich ein Kunde bei demselben Anbieter zu demselben Preis nur Zugang zu legalen Inhalten verschafft hat, wird demgegenüber allenfalls wenige Fälle betreffen und führt nicht dazu, dass Daten über Kreditkartenzahlungen nicht zur Grundlage staatsanwaltschaftlicher Ermittlungen gemacht werden dürften. Der Umstand, dass Zahlungsvorgänge zum Gegenstand staatsanwaltschaftlicher Ermittlungen werden können, entspricht der Möglichkeit, bei anderen Vorgängen des täglichen Lebens die Aufmerksamkeit der Strafverfolgungsbehörden zu erregen. [...]

### Anmerkung

Die *Analyse von Finanztransaktionen* ist ein vergleichsweise junges und umstrittenes Ermittlungsinstrument im Werkzeugkasten der Strafverfolgungsbehörden, aber auch der Verwaltungsbehörden<sup>1</sup> und Nachrichtendienste<sup>2</sup>. Diese Verfassungsbeschwerde richtete sich gegen eine solche Analyse der Transaktionen von über 20 Millionen Kreditkarteninhabern, ohne dass dies zu einem Ermittlungsverfahren gegen die Beschwerdeführer führte.<sup>3</sup> Die 2. Kammer des 2. Senats des BVerfG verneinte in ihrem Nichtannahmebeschluss<sup>4</sup> bereits die grundrechtliche Betroffenheit, da die Daten der Beschwerdeführer »anonym und spurlos aus diesem Suchlauf ausgeschieden wurden und nicht im Zusammenhang mit dieser Ermittlungsmaßnahme behördlich zur Kenntnis genommen wurden«. Dies überzeugt genauso wenig wie die Beurteilung der Kammer zur originär strafprozessrechtlichen Frage, dass die Maßnahme auf die »Ermittlungsgeneralklausel« des § 161 Abs. 1 StPO gestützt werden könne.

### I. Zum Anfangsverdacht

Im Grundsatz werden Strafverfolgungsbehörden dann und nur dann tätig, wenn ihnen ein Anfangsverdacht einer Straftat bekannt geworden ist (§ 160 Abs. 1 StPO). Dieser Anfangsverdacht lag zwar zweifelsohne wegen des Verbreitens kinderpornogra-

phischer Schriften durch den Betreiber der Webseite mit kinderpornographischen Schriften vor (§ 184 b Abs. 1 StGB). Dieser nutzte allerdings einen auf den Philippinen befindlichen Server, so dass es den Strafverfolgungsbehörden aussichtslos erschien, seiner habhaft zu werden, obschon die internationale Zuständigkeit über § 6 Nr. 6 StGB gegeben war.

Stattdessen gingen die Strafverfolgungsbehörden bei diesem *Marktdelikt* gegen die gem. § 184 b Abs. 4 StGB strafbewehrte Nachfrage vor. Der nur im Ausgangsverfahren diskutierte Einwand, dass diesbezüglich noch kein Anfangsverdacht vorgelegen habe, denn den Ermittlungsbehörden sei zu diesem Zeitpunkt noch unbekannt gewesen, ob es wenigstens einen solchen Täter gebe,<sup>5</sup> ist nicht haltbar: Die Anzahl der Täter – keinen bei tatbestandslosem Verhalten, einen Einzeltäter oder mehrere Beteiligte – ist regelmäßig im Anfangsstadium strafrechtlicher Ermittlungen unbekannt. Der Anfangsverdacht i. S. d. § 160 Abs. 1 StPO dient allerdings materiell der *Konkretisierung des Ermittlungsgegenstandes*, um ausufernden, sich nur auf eine allgemeine Vermutung oder Verdachtslage stützenden Ermittlungen vorzubeugen. Eine solche, hinreichende Konkretisierung erfolgte hier auf den Verdacht einer auch zeitlich eingegrenzten Nutzung eines bestimmten Angebots kinderpornographischer Schriften.

### II. Die Analyse von Finanztransaktionen

Ein altbekanntes strafprozessuales Ermittlungsinstrument ist es, ein- und ausgehende Transaktionen eines »verdächtigen« Kontos auszuwerten. So wäre es theoretisch möglich gewesen, anhand der Zahlungseingänge auf das Konto des Webseiten-Betreibers die tatverdächtigen Kunden zu ermitteln. Dieser Weg erschien den Ermittlungsbehörden im konkreten Fall angesichts des internationalen Kontextes wenig erfolgversprechend,<sup>6</sup> so dass sie stattdessen den (elektronischen) »paper trail« nutzten,

- 1 Etwa bei der Aufsicht über den Wertpapierhandel, s. die nahezu sämtliche Wertpapiergeschäfte betreffende Übermittlungs- bzw. Meldepflicht des § 9 WpHG. Zur diesbezüglichen verwaltungsrechtlich ermöglichten Rasterfahndung mit »letztlich strafrechtlicher Finalität« vgl. VOGEL in: FS Jakobs, 731, 743.
- 2 Vgl. nur das »Terrorist Finance Tracking Program« der US-amerikanischen Nachrichtendienste sowie den diesbezüglichen Beschluss 2010/16/GASP/JI des Rates über die Unterzeichnung – im Namen der Europäischen Union – des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus, ABLEU L 8 v. 13. 1. 2010, S. 9 ff.
- 3 Zum tatsächlichen Geschehen im Rahmen der Ermittlungen unter dem Decknamen MIKADO vgl. nur PETRI StV 2007, 266, 266; SCHNABEL DuD 2007, 426, 426.
- 4 BVerfG, Beschl. v. 17. 2. 2009 – 2 BvR 1372/07; 2 BvR 1745/07 = NJW 2009, 1405 = JuS 2009, 664 m. Anm. JAHN = CR 2009, 381 m. Anm. SCHNABEL; s. ferner T. SCHAEFER NJW-Spezial 2009, 280.
- 5 SCHNABEL DuD 2007, 426, 428 f. Angesichts der beschränkten internationalen Zuständigkeit – § 6 Nr. 6 StGB verweist nur auf § 184 b Abs. 1 bis Abs. 3 StGB – konnte sich das Ermittlungsverfahren zudem grundsätzlich nur gegen Täter richten, die in Deutschland gehandelt hatten (§§ 3, 9 Abs. 1 StGB).
- 6 Ein solcher sonstiger Rechtshilfeverkehr mit den Philippinen erfolgt vertragslos (vgl. RIVAST, Anl. II, Stand: Januar 2003) und erfordert die Zulässigkeit der Rechtshilfeleistung nach philippinischem Recht (vgl. SCHOMBURG/HACKNER in: Schomburg/Lagodny/Gleiß/Hackner (Hrsg.), IRG, 4. Aufl. 2006, Vor § 68 Rdn. 27 ff.); s. ferner WILKITZKI in: Grütznert/Pötz/Kreß (Hrsg.), IRG, Vor § 68 Rdn. 3 ff.

den Finanztransaktionen zu Abrechnungs- und Dokumentationszwecken hinterlassen. Diese Datenbanken lassen sich in Sekundenschnelle nach beliebigen Kriterien durchsuchen, wie hier nach denjenigen Kunden, deren Kreditkartenkonten mit 79,99 US-\$ zugunsten einer bestimmten philippinischen Bank unter Angabe einer bestimmten Kennung belastet wurden.

Eine solche Analyse von Finanztransaktionen zeichnet sich durch verschiedene Merkmale aus: Zuvörderst zielt sie auf Daten ab, die sich durch eine *atypische Abfrage* aus einem Datenbestand generieren lassen. So lassen sich im Gegensatz zu einem »Kontoauszug« eines Kunden die Finanzströme auf ein institutsfremdes Konto nur mit besonderem Aufwand rekonstruieren. Zweitens finden vermehrt *unspezifische und insensitive Suchkriterien* Verwendung; im vorliegenden Fall wohnte der Suche anhand einer Händlerkennung<sup>7</sup> und nach einer unbestimmten Vielzahl von Personen das Risiko inne, dass Unschuldige als sog. falsch-positive Treffer ins Visier der Ermittlungsbehörden gerieten. Drittens enthält sie eine *Inpflichtnahme Privater* zur Vornahme eigener Recherchen.<sup>8</sup>

Damit verbunden ist eine Reduktion des Beweiswerts: Eine atypische Einzelfallauswertung des Datenbestands ist fehleranfälliger als ein alltäglich verifizierbarer Kontoauszug. Insensitive Suchkriterien verlangen nach weiteren Indizien zur Erhärtung eines Tatverdachts. Zudem bedeutet die Einschaltung Privater zu Strafverfolgungszwecken zugleich die Beteiligung eines Unsicherheitsfaktors, der, obschon strafbewehrt, eher als beamtenrechtlich eingebundene Strafverfolger versucht sein könnte, ent- oder belastend manipulierend tätig zu werden. Am schwersten wiegt aber die Vielzahl missbräuchlicher Finanztransaktionen, die bei geringen Wertsummen und unvorsichtigen Kunden auch langfristig unerkannt bleiben können.<sup>9</sup>

### III. Kein Grundrechtseingriff – aber dennoch Rechtsschutz?

Das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) gewährleistet nach st. Rspr. des BVerfG Schutz gegen die »Erhebung, Speicherung, Verwendung und Weitergabe der auf sie bezogenen, individualisierten oder individualisierbaren Daten.«<sup>10</sup> Zweifelsohne in diesem Grundrecht betroffen waren diejenigen 322 Kreditkarteninhaber, deren Name und Anschrift als Treffer des Suchlaufs den Ermittlungsbehörden mitgeteilt wurden.

Beschwerdeführer waren jedoch ausschließlich Kreditkarteninhaber, deren Transaktionen zwar automatisiert durchsucht wurden, allerdings den Suchkriterien nicht entsprachen und daher weder Mitarbeitern der Finanzinstitute als Treffer angezeigt noch den Ermittlungsbehörden mitgeteilt wurden. An Rechtsprechung des *1. Senats* anknüpfend<sup>11</sup> verneint die *Kammer* daher eine grundrechtliche Betroffenheit der Beschwerdeführer, mithin die zur Begründetheit der Verfassungsbeschwerde notwendige Beeinträchtigung (subjektiver) Grundrechte. Dem liegt die Wertung zugrunde, dass sich hier die objektiv gegebene, wenn auch nur temporäre, spuren- und folgenlose Verwendung von Daten zu einer subjektiven Beeinträchtigung nicht »verdichtet«<sup>12</sup> habe.

Ohne Verletzung verfassungsrechtlich geschützter, subjektiver Rechte erübrigen sich Erörterungen zur objektiven Rechtmäßigkeit der Maßnahme. Bei entsprechender Auslegung des Begriffs des »Betroffenen« wäre zudem bereits der Antrag der Beschwerdeführer gem. § 98 Abs. 2 StPO unzulässig gewesen.<sup>13</sup> Vor dieser Konsequenz – eine umfassende gerichtliche Nachprüfung zu

verwehren – schreckt aber auch die *Kammer* zurück, wie sich an den im Beschluss folgenden, weitaus umfangreicheren Erwägungen zur tauglichen Eingriffsgrundlage zeigt.

Im Einklang mit der Literatur und der weiten, modernen Eingriffsdogmatik<sup>14</sup> ist es daher vorzuziehen, in diesen Fällen einen – freilich geringen – Eingriff anzunehmen und damit *allen* Kreditkarteninhabern eine Möglichkeit zur rechtlichen Nachprüfung der Datenanalyse einzuräumen. Zur Begründung sei erstens darauf verwiesen, dass die Übermittlung der Treffer-Datensätze zugleich die negative Aussage beinhaltet, dass andere Kreditkarteninhaber *keine* solche Buchung durchgeführt haben.<sup>15</sup> Zweitens ist *a maiore ad minus* der hypothetische Ermittlungsverlauf zu beleuchten, falls die Finanzinstitute sich geweigert hätten, den Datenabgleich durchzuführen: Dann wäre eine (unverhältnismäßige) Herausgabe aller Daten zur nachfolgenden Analyse durch die Strafverfolgungsbehörden erforderlich gewesen. Die bloße Auslagerung an die Finanzinstitute senkt zwar die Eingriffsintensität erheblich, ändert aber an der grundrechtsrelevanten Datenverwendung nichts. Drittens ist bei jedem Suchlauf ein Risiko gegeben, dass aus vielfältigen Gründen falsch-positive Resultate gelistet werden. Wenn zudem – wie hier – die Anzahl der Treffer noch unbestimmt ist, daher aufgrund systemischer Fehler – wie eines Zahldrehers bei der Suchabfrage – tausende falsch-positive Treffer entstehen können und nicht nur eine Einzelfall-Verwechslung vorliegen kann, ist dies entgegen der *Kammer* nicht als allgemeines Lebensrisiko zu klassifizieren.

### IV. Eingriffsgrundlage und vorbeugender Rechtsschutz

Nach Auffassung der *Kammer* konnte diese Analyse von Finanztransaktionen auf die »Ermittlungsgeneralklausel« des § 161 Abs. 1 StPO gestützt werden. Dies begegnet Bedenken, auch wenn richtigerweise die Anwendbarkeit des § 98 a StPO verneint wurde.

#### 1. Keine Rasterfahndung i. S. d. § 98 a StPO

Der Anwendungsbereich der »Ermittlungsgeneralklausel« ist entgegen des missverständlichen Wortlauts des § 98 a StPO<sup>16</sup>

<sup>7</sup> Diese Kennung ist in ihrer Sensitivität nicht über alle Zweifel erhaben, da sich regelmäßig mehrere Händler eine solche Kennung teilen.

<sup>8</sup> S. auch VOGEL in: FS Jakobs, 731, 743.

<sup>9</sup> Auch in einem vergleichbaren Verfahren erhärtete sich die Verdachtslage nicht gegen alle Treffer, vgl. Mainpost, <http://tr.im/EcHr> (Stand: 3. 2. 2010). Infolgedessen ist stets zu erwägen, die Kreditinstitute in einem zweiten Schritt – und vor einer eingriffsintensiven Hausdurchsuchung bei dem Verdächtigen – zu befragen, ob bei den Treffern zugleich Anhaltspunkte für Manipulationen oder missbräuchliche Transaktionen existieren.

<sup>10</sup> BVerfGE 65, 1, 43; 67, 100, 143; 84, 239, 279; 103, 21, 33; 115, 320, 341.

<sup>11</sup> BVerfGE 100, 313, 366; 107, 299, 328; 115, 320, 343.

<sup>12</sup> BVerfGE 115, 320, 343.

<sup>13</sup> Auch bei Maßnahmen im Ermittlungsverfahren nach § 161 Abs. 1 StPO ist Rechtsschutz (analog) § 98 Abs. 2 StPO zu gewähren; vgl. OLG Stuttgart NStZ 2008, 359, 360; ERB in: Löwe-Rosenberg, StPO, 26. Aufl. 2008, § 160 Rdn. 67 f. Zum verfassungsrechtlichen Hintergrund (schnelle und sachnahe Rechtsschutzmöglichkeit) s. BVerfGE 96, 27, 39 ff.; BVerfG NJW 2003, 1514, 1515.

<sup>14</sup> S. fallbezogen SCHNABEL CR 2009, 384, 384 und grundsätzlich, statt vieler, SACHS in: Sachs (Hrsg.), GG, 5. Aufl. 2009, Vor Art. 1 Rdn. 83 ff., insb. 95.

<sup>15</sup> Vgl. BVerfGE 107, 299, 328.

<sup>16</sup> Vgl. nur SCHÄFER in: Löwe-Rosenberg, StPO, 25. Aufl. 2004, § 98 a Rdn. 4.

nur eröffnet, soweit es sich bei einer solchen Analyse von Finanztransaktionen nicht um eine Rasterfahndung im Sinne dieser spezielleren Norm handelt. Es ist jedoch entgegen der *Kammer* nicht der formelle Aspekt ausschlaggebend, dass ein Datenabgleich nicht von den Strafverfolgungsbehörden sondern von Dritten durchgeführt wurde, denn dies kann die staatliche Veranlassung der Maßnahme nicht durchbrechen.<sup>17</sup>

Das von der *Kammer* angeführte technische Argument, für eine Rasterfahndung seien Daten *mehrerer Speicherstellen* erforderlich,<sup>18</sup> widerspricht dem Wortlaut des § 98 a Abs. 1 StPO und kann auch inhaltlich nicht überzeugen. Entscheidend ist das sich aus der Kombination von Diversität und Umfang des Datenbestandes ergebende Gefahrenpotential, etwa im Hinblick auf die Erstellung eines Persönlichkeitsprofils. Ein dergestalt qualifizierter Datenbestand kann aber in Zeiten regen elektronischen Datenaustauschs bereits bei einem Unternehmen und dessen Speicherstellen anfallen – man denke nur an *Google* oder *Microsoft*, die Suchmaschinen und E-Mail-Dienste anbieten.

Den richtigen Weg weist hingegen das von der *Kammer* angeführte materielle Argument, dass die Rasterfahndung nach »Personen [suche], die mehrere allgemeine Merkmale aufweisen oder [...] gerade nicht aufweisen«. Suchparameter sind bei der Rasterfahndung tätertypische Merkmale.<sup>19</sup> So filterte die Ende 2001 durchgeführte Rasterfahndung im Zuge der Ermittlungen gegen den internationalen Terrorismus nach den tätertypischen Kriterien der Religionszugehörigkeit, der Anzahl der Kinder und des Studiums technischer Fächer.<sup>20</sup> Es ist offensichtlich, dass bei einem tätertypenbezogenen Ansatz falsch-positive Resultate noch weitaus häufiger anzutreffen sein dürften und *de facto* die Erstellung eines ermittlungsrelevanten Persönlichkeitsprofils bezweckt wird. Hier waren hingegen näher spezifizierte, mit der konkreten Tat in engem Zusammenhang stehende Kreditkartentransaktionen gesucht, was demzufolge nicht einer Rasterfahndung entspricht.<sup>21</sup> Allerdings sind andere Analyseformen von Finanztransaktionen denkbar, die gleichwohl eine Rasterfahndung darstellen, so bei einer umfänglichen Auswertung der SWIFT-Daten<sup>22</sup> oder auch bei einer breiter gefächerten Auswertung, welche Personen »szenetypische« Beträge in »szenetypische« Länder transferieren.<sup>23</sup>

## 2. Bitte um freiwillige Auskunft?

Der *Kammer* zufolge stellte die staatsanwaltschaftliche Bitte um Auskunft eine hinreichende Rechtsgrundlage für die verfahrensgegenständliche Analyse von Finanztransaktionen dar. An sich ist es Strafverfolgungsbehörden gestattet, Unternehmen wie Privatbanken<sup>24</sup> um *freiwillige* Auskunft zu bitten,<sup>25</sup> über die deren Mitarbeiter – nicht die Unternehmen als solche<sup>26</sup> – zeugenschaftlich vernommen werden können oder die sich auf Gegenstände beziehen, die sich in deren Gewahrsam befinden. Bei einer Analyse von Finanztransaktionen ist allerdings diese Auskunftsbitten milderer Mittel zu § 95 Abs. 1 StPO und nicht zu § 161 a Abs. 1 StPO, denn selbst »zuständigen« Mitarbeitern der Finanzinstitute sind die Transaktionen nicht von vornherein höchstpersönlich bekannt, vielmehr müssen auch diese die Treffer erst nach einer Datenabfrage wahrnehmen.<sup>27</sup> Zu einer solchen Vorbereitung durch eigene Ermittlungstätigkeiten sind Zeugen allerdings nicht verpflichtet.<sup>28</sup>

Ermittlungsbehörden dürfen jedoch Privatpersonen oder Unternehmen nur dann um freiwillige Mitarbeit bitten, wenn diese ihnen nicht von Rechts wegen verwehrt ist (*arg. ex. Art. 20 Abs. 3 GG*). Dies wäre etwa der Fall, wenn in dem erbetenen Verhalten eine – ggf. strafbewehrte (§§ 201 ff. StGB) – Verletzung des

persönlichen Lebens- und Geheimnisbereichs liegt, denn dann gebieten es alleine Eingriffsintensität, Systematik und auch Rechtssicherheit zugunsten des Ersuchten, auf spezielle Ermittlungsmaßnahmen und deren rechtfertigende Wirkung zurückzugreifen.

Im vorliegenden Fall ist jedoch lediglich das zivilrechtlich ausgestaltete<sup>29</sup> (vermeintliche) Bankgeheimnis betroffen, das nicht dem Schutz der §§ 201 ff. StGB unterliegt. Eine Einschränkung der Datenverwendung und -weitergabe ergibt sich hier aus § 28 Abs. 2 Nr. 2 b) BDSG, das gem. § 1 Abs. 2 Nr. 3 BDSG auf elektronisch gespeicherte Finanztransaktionen Anwendung findet. Grundsätzlich ist eine Weitergabe zur Verfolgung von Straftaten möglich, zusätzliche Voraussetzung ist aber, dass »kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat« (§ 28 Abs. 2 a. E. BDSG). Neben dem Interesse derjenigen Kreditkarteninhaber, deren Daten aufgrund falsch-positiver Treffer weitergegeben werden, tritt das Interesse aller 20 Millionen betroffenen Kreditkarteninhaber, das Risiko einer falsch-positiven Zuordnung auszuschließen. Jedenfalls in der Summe erreicht dies bei *freiwilliger* Herausgabe ein für § 28 Abs. 2 Nr. 2 b) BDSG relevantes Maß. Dass die Kreditinstitute der Bitte um freiwillige Auskunft widerstandslos Folge leis-

17 Eher metaphorisch zu verstehen (»Flucht ins Privatrecht«) SCHNABEL CR 2009, 384, 384; s. ferner PETRI StV 2007, 266, 268; LR-StPO<sup>25</sup>/SCHÄFER (Fn. 16) § 98 a Rdn. 6.

18 So allerdings auch die sich auf Entschädigungspflichten gem. § 17 a Abs. 4 ZSEG beziehenden Beschlüsse OLG Stuttgart NSTZ 2001, 158, 159; OLG Köln, NSTZ-RR 2001, 31, 31 und ferner MEYER-GOßNER StPO, 52. Aufl. 2009, § 98 a Rdn. 8; NACK in: Karlsruher Kommentar zur StPO, 6. Aufl. 2008, § 98 a Rdn. 5. Offen gelassen durch BGH-Ermittlungsrichter NSTZ 2002, 107, 107.

19 LR-StPO<sup>25</sup>/SCHÄFER (Fn. 16) § 98 a Rdn. 1.

20 AG Tiergarten DuD 2001, 691, 691.

21 A. A. SCHNABEL DuD 2007, 426, 427. KK-StPO/NACK (Fn. 18) § 98 a Rdn. 32 spricht sich bei einer »tatbezogenen Rasterfahndung« für die analoge Anwendung von § 98 a StPO aus.

22 S. oben bei und mit Fn. 2.

23 Denkbar sind etwa solche Analysen bezogen auf die Verbreitung kinderpornographischer Schriften (§ 184 b StGB), oder auch bezogen auf Steuerhinterziehung (§ 370 AO).

24 Soweit öffentlich-rechtlich organisierte Kreditinstitute nicht-hoheitlich, also im Rahmen allgemeiner Bankgeschäfte tätig werden, sind diese nicht als Behörden im Sinne des § 161 Abs. 1 StPO aufzufassen, da insoweit deren allgemeine Bankgeschäfte betroffen sind, vgl. LR-StPO<sup>26</sup>/ERB (Fn. 13) § 161 Rdn. 28; LR-StPO<sup>25</sup>/SCHÄFER (Fn. 16) § 96 Rdn. 31, jew. m. w. N. Die Gegenauffassung – s. nur MEYER-GOßNER (Fn. 18) § 161 Rdn. 4 m. w. N. – verwehrt den Kunden, die sich im Wettbewerb der Banken für öffentlich-rechtlich organisierte Banken entschieden haben, denselben datenschutzrechtlichen Schutz, der im Folgenden über die Verneinung des § 161 Abs. 1 StPO bei gleichzeitiger Verweisung auf § 95 StPO erreicht wird.

25 Statt vieler LR-StPO<sup>26</sup>/ERB (Fn. 13) § 161 Rdn. 13; MEYER-GOßNER (Fn. 18) § 161 Rdn. 2.

26 Der Zeuge ist schließlich ein PERSÖNLICHES Beweismittel, das über seine PERSÖNLICHE Wahrnehmung bekunden soll, s. nur KK-StPO/SENGE (Fn. 18) Vor § 48 Rdn. 1; s. ferner EISENBERG Beweisrecht der StPO, 6. Aufl. 2008, Rdn. 1000.

27 SCHNABEL CR 2009, 384, 384; vgl. hierzu nur EISENBERG (Fn. 26) Rdn. 1201 a. E.

28 EISENBERG (Fn. 26) Rdn. 1199 f.; LR-StPO<sup>26</sup>/IGNOR/BERTHEAU (Fn. 13) § 69 Rdn. 9 m. w. N.; KREHL NSTZ 1991, 416, 417; PETRI StV 2007, 266, 266; zur materiell-rechtlichen Seite vgl. nur FISCHER StGB 56. Aufl. 2009, § 161 Rdn. 6 m. w. N. Ausnahmen werden, soweit ersichtlich, grundsätzlich nur für Zeugen angenommen, die über Wahrnehmungen in amtlicher Tätigkeit aussagen sollen.

29 Vertiefend LR-StPO<sup>26</sup>/ERB (Fn. 13) § 161 Rdn. 27 m. w. N.

teten,<sup>30</sup> unterstreicht die faktische Notwendigkeit eines *vorbeugenden Rechtsschutzes* zum Schutz der Drittinteressen. Folgte man dem nicht und ließe wie die Kammer die freiwillige Nutzung und Übermittlung fremder personenbezogener Daten zu, wäre die datenschutzrechtliche Leitlinie einer restriktiven *Zweckbindung der Daten* jedenfalls insoweit zunichte, als Strafverfolgungsinteressen oder auch bloß die »Wahrung berechtigter Interessen Dritter« (§ 28 Abs. 2 Nr. 2 a) BDSG) gegenständlich sind.

### 3. Vorbeugender Rechtsschutz gem. § 98 Abs. 1 S. 1?

Im Gegensatz zur Bitte um freiwillige Auskunft dient das *Auskunftsersuchen* bzw. *-verlangen* unmittelbar der Abwendung einer Herausgabeverpflichtung gem. § 95 Abs. 1 StPO.<sup>31</sup> Es ist dennoch gleichermaßen ein Zwangsmittel, das ebenfalls die grundsätzliche Anordnungsbefugnis durch das Gericht wahren muss (§ 98 Abs. 1 S. 1 StPO).<sup>32</sup> Dies wird von Teilen der Rechtsprechung und der Literatur bestritten, da im Gegensatz zur von § 98 Abs. 1 S. 1 StPO erfassten Beschlagnahme gerade kein unmittelbarer Zwang angeordnet werde, sondern ohne Einschaltung des Gerichts mit den willensbeugenden Ordnungs- und Zwangsmitteln des § 95 Abs. 2 StPO nur gedroht werden könne.<sup>33</sup> Dies verkennt aber bereits den psychischen Druck der Androhung und die Regelungssystematik der Beschlagnahme- und Herausgabevorschriften.<sup>34</sup> Zudem wird ein Herausgabeverlangen gem. § 95 Abs. 1 StPO allein wegen des *nemo tenetur*-Grundsatzes und § 95 Abs. 2 S. 2 StPO regelmäßig gegenüber unverdächtigen und unbeteiligten Dritten angeordnet, während bei einem Verdächtigen die Durchsuchung und Beschlagnahme das primäre Mittel der Wahl ist. Zur Wahrung legitimer Drittinteressen ist daher vorbeugender Rechtsschutz bei einem auf § 95 Abs. 1 StPO gestützten Auskunfts- oder Herausgabeverlangen unabdingbar.<sup>35</sup> Dies gilt umso mehr, als dass auch nachträglicher Rechtsschutz gem. § 98 Abs. 2 StPO aufgrund des engen Eingriffsbegriffs der *Kammerentscheidung* nunmehr auf tönernen Füßen steht.

### V. Verhältnismäßigkeit des Einzelfalls

Schließlich bejaht die *Kammer* auch die Verhältnismäßigkeit der Maßnahme im Einzelfall und lässt damit das letzte Korrektiv verfassungsgerichtlicher Überprüfungen verstreichen. Es sei unbestritten, dass die gewählte Maßnahme ein höchst legitimes Ziel verfolgt, geeignet und angesichts der geringen Erfolgsaussichten eines Rechtshilfeersuchens<sup>36</sup> im Grundsatz auch erforderlich war.

Die Überprüfung betraf in tatsächlicher, wenn auch der *Kammer* zufolge nicht in grundrechtlicher Sicht<sup>37</sup> mehr als 20 Millionen Kreditkarteninhaber. Diese Streubreite, die Heimlichkeit der Ermittlungsmaßnahme bei Fehlen von verfahrensrechtlichen Korrektiven und das nunmehr bestehende Risiko, fälschlicherweise ins Visier der Ermittlungsbehörden zu geraten, mag die sinnvolle Nutzung von Finanzinstituten und insbesondere Kreditkarten zu Finanztransaktionen beeinträchtigen. Das zumindest wahrgenommene, freiheitsschädliche Überwachungsklima ist folglich bei der Beurteilung der Angemessenheit zu berücksichtigen.<sup>38</sup>

Am meisten erschreckt es aber, dass die *Kammer* gegen Ende ihrer Entscheidung bezüglich falsch-positiver Treffer von »allenfalls wenigen Fällen« und einer »unvermeidbaren Gefahr« spricht, mithin von Kollateralschäden – ein erster Riss im zerbrechlichen rechtsstaatlich-liberalen Strafrechtsverständnis,

dass falsch-positive Strafverfolgungen gegen Unschuldige weit aus schwerer wiegen als die falsch-negative Nichtverfolgung von Tätern? Bei einer Suche nach einer unbestimmten Vielzahl von Treffern (Suche 1:n) ist das Risiko nicht mit einer bloßen Verwechslung (Suche 1:1) zu vergleichen.<sup>39</sup> Betrachtet man zudem die öffentliche Stigmatisierung und den »bürgerlichen Tod«, den bereits das Bekanntwerden eines Ermittlungsverfahrens – gerade wegen des Besitzes kinderpornographischer Schriften (§ 184 b Abs. 4 StGB) – bedeuten kann, so kann man sich wahrlich glücklich schätzen, nicht als »falscher Treffer« gelistet worden zu sein.<sup>40</sup> Jedenfalls daher ist – entgegen der *Kammer* – die Angemessenheit des Mittels in Zweifel zu ziehen.

### VI. Konsequenzen

Der Auffassung der *Kammer* zufolge ist der *Grundsatz der Verfügbarkeit von Daten* innerstaatlich<sup>41</sup> bereits weitgehend verwirklicht: Sofern personenbezogene Daten aus der Hand gegeben wurden, bei einem unverdächtigen Dritten elektronisch verfügbar sind und diese einem tattypischen Kriterium entsprechen, stehe der Staatsanwaltschaft gem. § 161 Abs. 1 StPO die Möglichkeit zur Verfügung, von dem Dritten (freiwillige) Auskunft zu erhalten. Nur soweit der Schutzbereich eines speziellen Grundrechts – wie Art. 10 GG – betroffen sei oder eine Rasterfahndung vorliege, benötige man eine spezielle Eingriffsgrundlage. Damit verkümmert das Grundrecht auf informationelle Selbstbestimmung in seiner Gestalt als Abwehr- und Freiheitsrecht.

In systematisch stimmiger Weise ist die tatbezogene Analyse von Finanztransaktionen durch Kreditinstitute vielmehr als Auskunftsverlangen zur Vermeidung einer Herausgabe gem. § 95 Abs. 1 StPO zu sehen. Diese setzt gem. § 98 Abs. 1 StPO die Anordnung durch das Gericht – zumeist den Ermittlungsrichter am Amtsgericht – voraus; angesichts der langen Speicherdauer ist Gefahr im Verzug kaum vorstellbar. Auf diesem Wege werden zudem die mitbetroffenen Drittinteressen durch vorbeugenden Rechtsschutz hinreichend berücksichtigt. Richtigerweise steht auch allen Betroffenen – also auch denjenigen, deren Daten anonym und spurlos ausgeschieden wurden – die Möglichkeit der nachträglichen gerichtlichen Überprüfung gem.

30 Lediglich die Landesbank Berlin AG weigerte sich in einem ersten Schritt, neben den Kreditkartennummern auch die Klarnamen preiszugeben.

31 S. LR-StPO<sup>25</sup>/SCHÄFER (Fn. 16) § 94 Rdn. 67; § 95 Rdn. 6, je m. w. N.

32 KG NStZ 1989, 192, 192; CIOLEK-KREPOLD Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen, 2000, Rdn. 200 ff.; EISENBERG (Fn. 26) Rdn. 2373; KK-StPO/NACK (Fn. 18) § 95 Rdn. 3; LR-StPO<sup>25</sup>/SCHÄFER (Fn. 16) § 95 Rdn. 20 m. umfangr. Nachw.

33 Etwa LG Bonn BKR 2003, 914; MEYER-GOßNER (Fn. 18) § 95 Rdn. 2 m. w. N.; s. auch LR-StPO<sup>26</sup>/ERB (Fn. 13) § 161 Rdn. 28 a.

34 Überzeugend LR-StPO<sup>25</sup>/SCHÄFER (Fn. 16) § 95 Rdn. 20.

35 Verneint man mit der Gegenauffassung die Notwendigkeit einer gesonderten Anordnungsbefugnis für ein Auskunftsverlangen (Fn. 33), so ist die Differenzierung zwischen Auskunftsbitte und Auskunftsverlangen freilich hinfällig. So erklärt sich auch die Gegenauffassung von LR-StPO<sup>26</sup>/ERB (Fn. 13) § 161 Rdn. 28 a.

36 S. oben bei und mit Fn. 6.

37 S. oben III.

38 S. in concreto JAHN JuS 2009, 664, 665; PETRI StV 2007, 266, 269; SCHNABEL DuD 2007, 426, 427 und generell BVerfGE 100, 313, 381.

39 S. oben III. a. E.

40 Nur in Ausnahmefällen wie dem von HAUPT FAZ v. 5. 2. 2007, S. 9 geschilderten Vorfall dürfte die falsch-positive Zuordnung alsbald nach Beginn der Hausdurchsuchung aufzudecken sein.

41 Zum europäischen Rechtsrahmen s. nur MEYER NStZ 2008, 188.

§ 98 Abs. 2 StPO offen, bei Wahrung des Richtervorbehalts gem. § 304 ff. StPO (Beschwerde). Ob sich ein solcher Richtervorbehalt freilich auch in transnationalen Verfahren durchsetzen lässt, bleibt abzuwarten.<sup>42</sup>

Unabhängig von dieser strafprozessualen Frage erschüttert es, mit welcher Leichtigkeit die *Kammer* das Risiko falsch-positiver Treffer und damit das erhebliche Folgerisiko einer Durchsuchung von Wohn- und Geschäftsräumen überwindet. Ob dies einen Wandel in Richtung einer »Risikogesellschaft« einläutet, in der Ermittlungsmaßnahmen gegen Unschuldige weitaus eher hinzunehmen sind, wenn dadurch nur genügend Täter gefasst

werden können? Die zukünftige Rechtsprechung des *BVerfG* gilt es mit wacherem Auge als bisher zu verfolgen.

Wiss. Ang. *Dominik Brodowski* LL.M. (UPenn), Tübingen

<sup>42</sup> Vgl. hierzu die explizite Erwähnung der »Überwachung ... von Kontenbewegungen« im Grünbuch der Kommission »Erlangung verwertbarer Beweise in Strafsachen aus einem anderen Mitgliedstaat« (KOM(2009) 624 endgültig vom 11. 11. 2009, S. 5) als ein Beispiel für Beweismittel, die zukünftig nach dem Prinzip der gegenseitigen Anerkennung angeordnet werden könnten.