Stellungnahme

zum Regierungsentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*

Ermittlungstaktische und beweisrechtliche Bedeutung von Verkehrsdaten

– ein Einblick in die Ermittlungs- und Verfahrenspraxis der Strafverfolgungsbehörden und Gerichte

Verfasser: *Richter am Bundesgerichtshof Dr. Nikolaus Berger, Leipzig/Hamburg* **

Während sich die Diskussion über eine erneute Einführung von Höchstspeicherfristen für Verkehrsdaten zunächst darauf konzentriert hatte, ob vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs überhaupt rechtliche Realisierungsmöglichkeiten für dieses Ermittlungsinstrument bestehen und solche durch die Bundesregierung im Regierungsentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 15. Juni 2015 (BT-Drs. 18/5171) – mit guten Gründen – anerkannt worden sind, scheint sich der Schwerpunkt der öffentlich geführten Kontroverse zu verlagern:

Nunmehr drängt die Frage in den Vordergrund, ob die Möglichkeit eines anlassbezogenen Zugriffs der Strafjustiz auf die bei den (privaten) Telekommunikationsprovidern anfallenden und von ihnen anlasslos zu speichernden Verkehrsdaten überhaupt einen hinreichenden Nutzen hat, der einen mit einer solchen Datenspeicherung auf Vorrat verbundenen Eingriff in grundrechtlich geschützte Rechtsgüter – auch nicht Tatverdächtiger – und ihren Aufwand rechtfertigen kann. Angesprochen ist damit die Frage der Verhältnismäßigkeit, die der Regierungsentwurf u.a. dadurch gewährleisten will, dass Vorratsdaten von den Strafverfolgungsorganen nur zur Aufklärung „besonders schwerer Straftaten“, die auch im Einzelfall besonders schwer wiegen, und auch nur erhoben werden dürfen, „soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert

---

* Anhörung des Ausschusses für Recht und Verbraucherschutz am 21. September 2015

** Der *Verf.* ist Mitglied des 5. (Leipziger) Strafsenats des BGH; bis Juni 2013 war er Mitglied des 2. Strafsenats des BGH und über vier Jahre Ermittlungsrichter beim BGH.

oder aussichtslos wäre“ (§ 100g Abs. 2 Satz 1, Abs. 3 StPO RegE). Immer wieder ist zu lesen und zu hören, dass retrograd zu erhebende Verkehrsdaten, die vor Beginn eines Ermittlungsverfahrens in zeitlicher Nähe zu einer Straftat angefallen sind, in der Praxis der Strafverfolgungsorgane keine oder allenfalls eine untergeordnete Bedeutung zukomme, sodass selbst eine zeitlich eng begrenzte Vorratsdatenspeicherung gegen das verfassungsrechtliche Übermaßverbot verstoße. Hierzu wird als Referenz regelmäßig auch ein Gutachten der kriminologischen Abteilung des Freiburger Max-Planck-Instituts für ausländisches und internationales Strafrecht aus dem Jahr 2011 zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung herangezogen.[1]

Deshalb soll hier anhand von Beispielsfällen aus jüngerer Zeit, wie sie im Alltag richterlicher Berufspraxis[2] vorkommen, die ermittlungstaktische Bedeutung der Verkehrsdaten für die Tataufklärung durch die Strafverfolgungsbehörden und für die Beweisführung der Strafgerichte dargestellt werden (**I.**). Dazu sollen die in den Strafverfahren abgeurteilten Taten bzw. (soweit ein rechtskräftiges Verfahrensergebnis noch nicht vorlag) die den Ermittlungsverfahren zugrundeliegenden Tatvorwürfe mit groben Strichen skizziert und der Einsatz der Verkehrsdaten und seine Folgen für den Verfahrensausgang dargelegt werden. Die Darstellung erhebt nicht den Anspruch einer empirischen Untersuchung. Vielmehr soll anhand von konkreten Fällen veranschaulicht werden, wie die Erhebung von Verkehrsdaten einerseits zu Beginn eines Ermittlungsverfahrens als ebenso sicherer wie effizienter Ermittlungsansatz und andererseits im Hauptverfahren vor Gericht als beweiskräftiges Indiz für einen Tatnachweis oder auch zu einer Verdachtsentkräftung zugunsten eines Beschuldigten bei der Aufklärung schwerster Straftaten beitragen kann.

---

[1] „Schutzlücken durch Wegfall der Vorratsdatenspeicherung? – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten“, Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg, 2. erweiterte Fassung, 2011.

[2] Zusätzlich zu Fällen, die Gegenstand von Revisionsverfahren beim BGH waren und auch mit dem StR-Aktenzeichen des betreffenden Verfahrens gekennzeichnet sind, haben maßgeblich zu der Sammlung exemplarischer Fälle mit weiteren Verfahren aus dem Bezirk des Hanseatischen Oberlandesgerichts Hamburg Staatsanwalt Dr. Gerwin Moldenhauer und Richter am Oberlandesgericht Marc Wenske beigetragen; ihnen danke ich für ihre Unterstützung.

Weiter wird zu den – empirisch nicht belastbaren – Erkenntnissen des Max-Planck-Instituts Stellung genommen und kurz beleuchtet, welchen Schwierigkeiten eine begrüßenswerte Evaluation einer Wirksamkeit der Neuregelung der Verkehrsdatenspeicherung ausgesetzt sein dürfte (**II.**). Eine überwiegend zustimmende Stellungnahme wird der Verfasser im Rahmen seines Fazits (**III.**) geben.

I. Einblick in die Ermittlungspraxis deutscher Strafverfolgungsbehörden

1. Verfahrensbeispiele

Nachstehend werden aus verschiedenen Deliktsbereichen der Schwerkriminalität Beispielsfälle knapp mit Verfahrensgegenstand und Bedeutung der Verkehrsdaten als Ermittlungsansatz und/oder Beweistatsache für die Beweiswürdigung dargestellt. Es handelt sich – wie nochmals zu unterstreichen ist – nicht um systematisch erhobene oder ganz außergewöhnliche Fälle, sondern um alltägliche Strafverfahren im Bereich der Schwerkriminalität, mit denen die Staatsanwaltschaften der Länder und die Landgerichte regelmäßig befasst sind. Verfahren aus der Senatstätigkeit des *Verf*., die im laufenden Kalenderjahr abgeschlossen wurden, sind den Deliktsgruppen jeweils vorangestellt worden, um nicht zuletzt schon durch deren bloße Anzahl die Relevanz eines Zugriffs auf retrograd zu erhebende Verkehrsdaten für die Verbrechensaufklärung zu illustrieren.

a) Raubdelikte

(1) Verfahrensgegenstand: Das Landgericht Hamburg verurteilte die Angeklagten rechtskräftig wegen Raubes (§ 249 StGB) in Tateinheit mit gefährlicher Körperverletzung (§ 224 Abs. 1 Nr. 4 StGB) zu Freiheitsstrafen von fünf Jahren und von drei Jahren sechs Monaten.[3] Die beiden aus Rumänien stammenden, sich illegal an verschiedenen Wohnorten in Deutschland aufhaltenden Täter hatten in Hamburg einen 78-jährigen Rentner aus einem Bus bis in den

[3] LG Hamburg, Urteil vom 17.3.2015, Az. 611 KLs 18 - 14-3100 Js 341/14; BGH, Beschluss vom 1.9.2015 – 5 StR 349/15.

Hausflur seines Wohnhauses verfolgt, um ihm seinen Goldschmuck zu rauben. Einer der Täter versetzte dem Geschädigten überraschend von hinten einen Faustschlag ins Gesicht und beide traten sodann auf das bewusstlos zu Boden gegangene Opfer ein, das u.a. eine Kieferfraktur und ein Schädel-Hirn-Trauma erlitt. Mit einer Beute von rd. 1.300 Euro flohen sie anschließend in unterschiedliche Richtungen vom Tatort, wobei einer der Täter die U-Bahn benutzte und sich auf seiner Flucht telefonisch mit dem Komplizen zu einer Beuteteilung am Hauptbahnhof verabredete.

Ermittlungstaktische Bedeutung von Verbindungsdaten: Beide Täter waren zunächst bei der Beobachtung des späteren Opfers im Bus von der dortigen Videokamera abgebildet worden. Einer der Täter wurde auf seinem Fluchtweg auch von den Überwachungskameras an der dem Tatort nahegelegenen U-Bahn-Haltestelle sowie der U-Bahn aufgenommen. Dem Videofilm war zu entnehmen, dass er dabei mehrfach telefonierte. Nach Ausmessung von drei für den Tatort und den Fluchtweg relevanten Funkzellen wurde vom Ermittlungsrichter die Herausgabe der dort in dem Tat- und Fluchtzeitfenster von 30 Minuten angefallenen und auf der Grundlage des § 96 Abs. 1 TKG gespeicherten Verkehrsdaten angeordnet. Zur Verhältnismäßigkeit führte der Ermittlungsrichter in seinem Beschluss gemäß § 100g Abs. 1 Nr. 1, Abs. 2 i.V.m. § 100b Abs. 1 Satz 1, Abs. 2 StPO aus, dass es mittels einer Auswertung der Funkzellendaten auf Überschneidungen möglich sei, den Täteranschluss festzustellen; Rechte Dritter seien nicht erheblich betroffen, da die erlangten Daten nur bei einer Übereinstimmung aufgeschlüsselt würden. Anhand der von Providern mitgeteilten Verkehrsdaten konnte festgestellt werden, dass insgesamt 13 Mobiltelefonnummern in zwei der drei untersuchten Funkzellen Verbindungen im Abfragezeitraum hatten. Bei einem weiteren gezielten Abgleich mit den Daten aus den Videoaufzeichnungen der Hochbahn blieb nur eine Mobilnummer übrig, die dem mit der U-Bahn Flüchtenden zugeordnet werden konnte. Über den von diesem Anschluss während der U-Bahnfahrt viermal angerufenen Mobilanschluss ließ sich die Mobilfunknummer des Mittäters ermitteln. Allein dessen Anschluss war auch in der Folgezeit noch aktiv.

Insbesondere durch eine ermittlungsrichterlich angeordnete Überwachung der unter dieser Mobilnummer geführten Telekommunikation nach § 100a Abs. 1, Abs. 2 Nr. 1k StPO ergaben sich Hinweise auf die Identität des diesen Anschluss nutzenden (zweiten) Täters, der nach seiner Identifizierung rd. zehn Wochen nach der Tat festgenommen werden konnte. Er gestand bereits in seiner ersten polizeilichen Vernehmung die Tat und benannte später auch seinen Mittäter.

Andere von den Ermittlungsbehörden hier zusätzlich gewählte Maßnahmen zur Täteridentifizierung (u.a. eine Öffentlichkeitsfahndung und ein Abgleich der sichergestellten DNA-Spuren mit der DNA-Analyse-Datei) waren leergelaufen. Ohne den kurzfristigen Rückgriff auf die bei Netzbetreibern noch vorhandenen Verkehrsdaten nach § 96 TKG hätte das Verbrechen nicht aufgeklärt werden können. Beweisrechtlich, also zum späteren Tatnachweis in der Hauptverhandlung vor dem Landgericht, spielten die zu Identifizierungszwecken erhobenen Verkehrsdaten keine nennenswerte Rolle mehr.

Im Hinblick auf die im Regierungsentwurf (RegE) vorgesehene Wiedereinführung einer Pflicht zur Speicherung von Mobilfunk-Verkehrsdaten in § 113b TKG (RegE) und zur Möglichkeit ihrer Erhebung in § 100g Abs. 2 StPO (RegE) ist anzumerken: Hätte sich im Laufe der Ermittlungen noch innerhalb der Vierwochenfrist des § 113b Abs. 1 Nr. 2 TKG (RegE) der Verdacht einer Tatserie mit gleichartig brutal ausgeführten, aber noch keinen Qualifikationstatbestand erfüllenden Verbrechen des Raubes ergeben, hätten die Ermittlungsbehörden selbst bei noch vorhandenen Vorrats-Standortdaten etwa für die betreffenden weiteren Tatorte darauf keinen Zugriff erhalten können, weil eine Funkzellenabfrage nach § 100g Abs. 3 Satz 2 StPO (RegE) nur zur Aufklärung der im Straftatenkatalog in § 110g Abs. 2 Satz 2 Nr. 1g StPO (RegE) enthaltenen qualifizierten Raubdelikte ermittlungsrichterlich hätte angeordnet werden können.

(2) Verfahrensgegenstand: Den Angeklagten lag in einem Verfahren der Staatsanwaltschaft Hamburg ein besonders schwerer Raub zur Last (§ 250 Abs. 2 Nr. 1 StGB).[4] Nach dem Anklagevorwurf forderten sie den Geschädigten auf, sein Mobiltelefon herauszugeben, und schlugen ihm – als er sich weigerte – mit einer Flasche derart auf den Kopf, dass er bewusstlos zu Boden stürzte. Anschließend entwendeten die Angeklagten dem Opfer das Mobiltelefon und veräußerten es noch am selben Tage.

Beweisrechtliche Bedeutung von Verbindungsdaten**:** Die Angeklagten schwiegen im Ermittlungsverfahren. Der hinreichende Tatverdacht wurde in der Anklageschrift gestützt auf die Aussage einer Zeugin, die das Mobiltelefon wenige Stunden nach der Tat von den Angeklagten gekauft und noch in folgenden Nacht verschenkt haben sollte. Bei dem Beschenkten konnte die Tatbeute schließlich im Rahmen einer Durchsuchung aufgefunden werden. Die Aussage der Zeugin wurde bestätigt durch Verkehrsdaten: Mit Hilfe der Gerätenummer (IMEI-Nummer) des gestohlenen Mobiltelefons konnte ermittelt werden, dass die beschenkte Person das dem Geschädigten entwendete Mobiltelefon mit seiner eigenen SIM-Karte betrieben hatte.

(3) Verfahrensgegenstand**:** Die Staatsanwaltschaft Hamburg legte den Angeklagten einen schweren Raub zur Last (§ 250 Abs. 1 Nr. 1b StGB).[5] Nach dem Anklagevorwurf klingelten sie an der Tür einer bettlägerigen älteren Dame. Nach Öffnen der Tür durch die Angestellte eines Pflegedienstes drückte einer der Täter ihr eine Hand auf den Mund, um sie am Schreien zu hindern. Sodann drängte er sie in das Innere der Wohnung und befragte sie nach Bargeld. Anschließend wurde die Angestellte gefesselt und geknebelt und die Täter flüchteten mit Bargeld.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Die schweigenden Angeklagten – die persönliche Kontakte zum Pflegedienst unterhielten – wurden erheblich belastet durch die Ergebnisse der Ver-

[4] Az. 3411 Js 497/14; nachfolgend: Urteil des LG Hamburg vom 3.6.2015, Az. 628 KLs 3/15.
[5] Az. 4290 Js 52/11; nachfolgend: Urteil des LG Hamburg vom 8.7.2014, Az. 617 Ns 15/13.

kehrsdatenauswertung ihrer Mobiltelefone. Danach wurden zwischen ihnen insbesondere zur Tatzeit und unmittelbar danach mehrere Telefonate geführt; die Geovisualisierung der Verbindungsdaten – eine graphische Aufbereitung der verschiedenen Standorte von Funkzellen, in denen die Mobilfunkanschlüsse eingeloggt waren – zeigte, dass sich ein Angeklagter zur Tatzeit in unmittelbarer Nähe des Tatorts aufgehalten hatte.

(4) Verfahrensgegenstand: Das Landgericht Hamburg hat den Angeklagten rechtskräftig vom Vorwurf des besonders schweren Raubes (§ 250 Abs. 2 StGB) freigesprochen.[6] Die Staatsanwaltschaft hatte mit ihrer Anklage dem Angeklagten vorgeworfen, gemeinsam mit zwei Mittätern einen Pizza-Boten nachts in einen Hinterhalt gelockt, dort überfallen und ihm mit Gewalt und unter Vorhalt von Waffen Bargeld, Papiere und Mobiltelefone geraubt zu haben. Als Nutzer der Mobilfunknummer, die zur vorgeblichen Essensbestellung beim Pizza-Service verwendet wurde, war der Angeklagte ermittelt worden.

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hatte im Ermittlungsverfahren und in der Hauptverhandlung vor der Strafkammer geschwiegen. Besondere Bedeutung kam in diesem „Indizienprozess“ namentlich den erhobenen Verkehrsdaten betreffend den Mobilanschluss zu, von dem aus eine Pizzabestellung aufgegeben worden war. Die verwendete Telefonnummer war mit einer sog. Pre-Paid-Karte ausgegeben worden; die hierbei vom Käufer angegebenen Personalien erwiesen sich als fiktiv. Gleichwohl sprach zunächst alles für eine Nutzung des Anschlusses allein durch den Angeklagten, denn sämtliche im Wege der Verkehrsdatenerhebung gesicherte Verbindungen dieses Anschlusses in der Zeit vor der Tatbegehung wiesen Bezüge zum familiären Umfeld oder zum Freundeskreis des Angeklagten auf. Nur die Gesprächspartner vereinzelter Verbindungen ließen sich nicht mehr rekonstruieren. Der Schluss von diesen Verkehrsdaten auf die Täterschaft des Angeklagten konnte allerdings nur dann tragfähig sein, wenn mit Gewissheit auszuschließen war, dass eine andere Person Zugriff auf den Anschluss hatte.

[6] LG Hamburg, Urteil vom 13. Dezember 2013, Az: 624 KLs 11/12 – 4181 Js 1/12

Bis zum letzten Hauptverhandlungstag am 13. Dezember 2013 schien die Beweisaufnahme die Schlussfolgerung von den Verkehrsdaten auf die Täterschaft des Angeklagten nahezulegen. Einem im Rahmen des Schlussvortrags des Verteidigers gestellten Beweisantrag betreffend den Standort des Tathandys drei Tage vor der am 28. Dezember 2011 begangenen Tat kam die Strafkammer nach. Die Auswertung des Standortes zu diesem Zeitpunkt ergab, dass der Anschluss eingeloggt war in einer Funkzelle im nördlichen Schleswig-Holstein, nicht aber – was angesichts zahlreicher übereinstimmender und glaubhafter Zeugenaussagen zum Aufenthalt des Angeklagten an diesem Tage zu erwarten gewesen wäre – in Hamburg. Zusammen mit dem Umstand, dass der Mobiltelefonanschluss am Abend unmittelbar vor der Tat am Wohnort der Freundin eines weiteren Tatverdächtigen eingeloggt war, der engen Kontakt zur Familie des Angeklagten hatte, schwächte dies „das Beweiszeichen in ganz empfindlicher Weise“. Denn es konnte, wie die Strafkammer in den Urteilsgründen ausgeführt hat, „nunmehr nicht sicher ausgeschlossen werden, dass ein Dritter möglicherweise auch am Tatabend Zugang zu dem Mobilfunkanschluss hatte“.

b) Erpressungsdelikte

(1) Verfahrensgegenstand: Der Angeklagte ist vom Landgericht Hamburg rechtskräftig u.a. wegen versuchter räuberischer Erpressung in zwei Fällen (§§ 253, 255, 249 Abs. 1, 22, 23 StGB) zu einer Gesamtfreiheitsstrafe von drei Jahren verurteilt worden.[7] Der Verurteilung zugrunde lagen u.a. Todesdrohungen, die der Angeklagte im Rahmen von Streitigkeiten über gegen ihn erhobene Forderungen aus seiner Tätigkeit als Box-Promoter u.a. per SMS an zwei seiner Gläubiger zur Abwendung von Zwangsvollstreckungsmaßnahmen übermittelte. Die geschädigten Gläubiger gingen auf die Drohungen nicht ein, wobei einer von ihnen bereits am Tag nach der Tat Strafanzeige erstattete. Daher konnten die gemäß § 96 TKG gespeicherten Verkehrsdaten u.a. des zur Übermitt-

[7] LG Hamburg, Urteil vom 1.9.2014, Az. 603 KLs – 6500 Js 21/13; BGH, Beschluss vom 19.5.2015 – 5 StR 154/15.

lung der Drohungen genutzten Mobilfunkanschlusses nach § 100g Abs. 1 StPO noch erhoben werden.

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hatte zunächst geschwiegen und sich später dahin eingelassen, dass jemand anderes die betreffenden Nachrichten versandt haben müsse. Die Strafkammer hat den Angeklagten auf Grund folgender, maßgeblich auf die Verkehrsdaten gestützter beweiswürdigender Erwägungen als überführt angesehen:

> *„(...) Der Angeklagte wird insbesondere belastet durch die ... Verbindungsdaten zu der Rufnummer 49176XXX. Von dieser Rufnummer aus sind um 19:53 und um 20:04 Uhr die SMS an den Zeugen Ko. und den Zeugen Sch. versandt worden. Aus den Verbindungsdaten zu der genannten Rufnummer ergibt sich, dass die SMS von einem Endgerät mit der IMEI-Nummer 35151XXX versandt wurde. Diese IMEI-Nummer ist einem Mobiltelefon Nokia E72 zugeordnet. Das Gerät wurde ausweislich des Durchsuchungsberichts der Beamtin Schoe. vom 7. Mai 2013 ... bei der Durchsuchung des Wohnhauses des Angeklagten ... sichergestellt. ... Das Mobiltelefon Nokia E 72 mit der IMEI-Nummer 35151XXX wurde auch vor und nach der Tat von dem Angeklagten genutzt. Das bestreitet der Angeklagte nicht. Die Zuordnung des Mobiltelefons zum Angeklagten wird bestätigt erstens durch den ausgelesenen SMS-Speicher des Geräts, dessen Auswertung nach Angaben des Zeugen K. ergeben hat, dass das Mobiltelefon vom Angeklagten genutzt wurde, insbesondere waren keine ausgehenden SMS gespeichert, die nicht von ihm herrührten...*
>
> *Die SIM-Karte mit der Rufnummer 49176XXX und das Endgerät mit der IMEI-Nummer 35151XXX waren ... zum Zeitpunkt der Versendung der SMS an die Zeugen Ko. und Sch. nach dem mit dem Zeugen K. erörterten Ergebnis der Verkehrsdatenauswertung eingeloggt bei einer Funkzelle LAC 10109/ Cell-ID 26360 mit den Koordinaten ... des Providers O. ... Diese Funkzelle deckt nach der Funkzellenausmessung des Landeskriminalamtes ... auch den Bereich H.-Straße in G., der Wohnanschrift des Angeklagten, ab.*
>
> *Zur Tatzeit am 6. Januar 2013 waren nach der Auswertung der Verkehrsdaten und der Funkzellenabmessung in der H.-Straße in G. durch das Landeskriminalamt ... auch die anderen vom Angeklagten regelmäßig genutzten Mobilfunkgeräte in Funkzellen eingeloggt, die ebenfalls den Wohnort des Angeklagten abdecken. Hochwahrscheinlich befand sich der Angeklagte demnach zuhause, als die*

SMS versandt wurden, jedenfalls aber an einem Ort in der Nähe, von dem die SMS versandt worden sein könnten. Die grundsätzliche Nutzung der im Folgenden genannten Geräte und SIM-Karten und deren Zuordnung zu seiner Person hat der Angeklagte in der Hauptverhandlung bestätigt... Das iPad mit der IMEI-Nummer 01292XXX ... war im Laufe des Tattages bis 16:32 Uhr und dann wieder um 19:39 Uhr eingeloggt in der Funkzelle LAC Cell-ID 1022,25, Koordinaten ..., einem Funkturm in T., der nach der Messung des LKA ... auch die Wohnanschrift des Angeklagten abdeckt. Das iPhone mit der IMEI-Nummer 0130XXX mit der zugehörigen SIM-Twin-Karte mit derselben Rufnummer 0172XXX war ab 19:43 Uhr teils in den genannten Funkturm in T. eingeloggt, teils in die Funkzelle des Providers V. mit der Zellkennung LAC/Zell-ID 409/15001, einem Funkmast in W. mit den Koordinaten ..., der nach der Funkzellenausmessung ... gleichfalls die Wohnanschrift des Angeklagten abdeckt. ... Ein weiteres iPhone mit der IMEI-Nummer 01265XXX und der SIM-Karte mit der Rufnummer 0172XXX war ab 19:03:22 Uhr eingeloggt in die Funkzelle in W."

(2) Verfahrensgegenstand: Die Staatsanwaltschaft Hamburg legt dem Angeklagten eine besonders schwere räuberische Erpressung zur Last (§§ 253, 255, 250 Abs. 2 Nr. 1 StGB).[8] Nach dem Anklagevorwurf stellte er ein Scheinangebot über den Verkauf eines Kraftfahrzeugs auf der Internetplattform „mobile.de" zum Preis von 40.000 Euro ein. Er einigte sich telefonisch mit einem Interessenten über den Verkauf und verabredete sich mit ihm und dessen Lebensgefährtin. An dem abgelegenen Treffpunkt hielt der Angeklagte dem Kaufinteressenten einen Revolver an den Kopf, verlangte Bargeld und drohte für den Fall einer Weigerung, den Geschädigten und dessen Lebensgefährtin zu erschießen. Der Geschädigte händigte ihm das Geld aus.

Beweisrechtliche Bedeutung von Verbindungsdaten: Noch am Tatabend eingeleitete Fahndungsmaßnahmen blieben erfolglos. Eine Identifizierung des Angeklagten als Täter gelang erst neun Monate später auf Grund eines Hinweises nach Veröffentlichung des Tatgeschehens und eines Phantombildes bei der Sendung „Aktenzeichen XY". Dieser Hinweis wurde durch die zuvor erhobenen Verkehrsdaten bestätigt. Denn anhand der Verkehrsdaten zu der vom Täter gegenüber dem Geschädigten verwendeten Rufnummer konnte ermittelt werden,

[8] StA Hamburg, Az. 3400 Js 39/15

wo sich der Nutzer des Anschlusses vor der Tat aufgehalten hatte. Dies war überwiegend ein Bereich Hamburgs in der Nähe zur Wohnanschrift des Angeklagten, auf den die Zeugenhinweise abzielten.

c) Mord- und Totschlagsdelikte

(1) Verfahrensgegenstand: Die Angeklagte ist vom Landgericht Saarbrücken wegen Anstiftung zum Mord sowie wegen versuchter Anstiftung zum Mord (§§ 211, 26 StGB) rechtskräftig zu lebenslanger Freiheitsstrafe als Gesamtstrafe verurteilt worden.[9] Der abgeurteilten Anstiftung zum Mord lag zugrunde, dass die Angeklagte den von ihr als Täter rekrutierten F. gegen Geldzahlung dafür gewann, den ursprünglich mit ihr befreundeten Geschäftspartner P. zu töten. Sie wollte sich hierdurch von erheblichen Schulden bei P. befreien und zugleich Zugriff auf eine im Todesfall an einen ihrer Familienangehörigen auszuzahlende Lebensversicherungssumme erhalten. Zur Vorbereitung der Tat verabredete die Angeklagte ein Treffen zwischen dem mit der Tötung beauftragten F. und dem späteren Tatopfer P., dem die Angeklagte als Legende vortäuschte, bei dem Termin ihre Schulden durch eine Zahlung von F. an P. begleichen zu wollen. Die Angeklagte stimmte mit beiden Männern durch diverse Telefonate und Kurznachrichten ab, dass die vorgebliche Geldübergabe am Abend des 23. Mai 2013 auf einem leerstehenden, dem F. zugänglichen Anwesen stattfinden sollte. Dort tötete F. den P. Zu der umfänglichen (im Ergebnis aber erfolglosen) Tatspurenbeseitigung des F. gehörte, dass er das Handy des Tatopfer P. in einem Fluss beseitigte und die Angeklagte aufforderte, ihre Handydaten zu löschen; auch führte er an seinem eigenen Handy einen „Datenreset“ durch. Die von F. mit dem Fahrzeug des Opfers an einen abgelegenen Ort transportierte Leiche des P. wurde zwei Wochen nach der Tat entdeckt und führte zur Bildung einer Mordkommission „P.“, der es gelang, die nach § 96 TKG gespeicherten Verkehrsdaten der bei Tatbegehung und der Nachtat-Kommunikation verwandten Mobilfunkgeräte sowie der tatrelevanten Funkzellen noch zu erheben.

[9] LG Saarbrücken, Urteil vom 4.2.2015, Az. 2 Ks 1/14 – 7 Js 901/13; BGH, Beschluss vom 18.8.2015 - 5 StR 249/15.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die Angeklagte bestritt in der Hauptverhandlung vor der Strafkammer ihre Tatbeteiligung. Seine Überzeugung davon, dass die Angeklagte den Mordauftrag erteilt hatte, bildete sich das Landgericht im Wesentlichen aufgrund der geständigen Aussage des bereits rechtskräftig für den Mord an P. verurteilten und nunmehr als Zeuge vernommenen F. Angesichts der hier gegebenen besonderen Aussagekonstellation[10] hielt es das Landgericht – zu Recht – für bedeutsam, dass die Angaben des Belastungszeugen F. durch die Auswertung der Telekommunikationsverbindungsdaten bestätigt wurden. Hierzu führte das Landgericht in seiner Beweiswürdigung u.a. aus:

> *„Die verlesenen Daten belegen allein für den Tattag, dass zwischen der Angeklagten und dem Opfer 18 Telekommunikationsverbindungen wechselseitigen Ursprungs zu verzeichnen waren und zwischen der Angeklagten und dem Zeugen F. 13 derartige Verbindungen. … Hingegen gibt es keine unmittelbaren Verbindungen zwischen dem Zeugen F und dem P. Insbesondere um den Zeitpunkt der Tötung herum ist feststellbar, dass die Angeklagte wechselseitig und jeweils in unmittelbarem Zusammenhang den P. und den F. mit SMS-Nachrichten kontaktierte und auf diese Weise beide zum Tatort hin „fernsteuerte“ sowie beide über deren jeweiligen Aufenthaltsort bzw. Eintreffzeitpunkt informierte. … Insofern sind sämtliche, objektiv festgestellten Telekommunikationsverbindungen zwischen dem F. und der Angeklagten am Tatabend vollständig in Einklang zu bringen mit dem von dem Zeugen F. geschilderten Tatablauf; dies in zeitlicher wie auch in örtlicher Hinsicht. Denn auch die Funkzellenauswertung bestätigt das von dem Zeugen F. angegebene Bewegungsprofil, beginnend mit dem Weg hin zur B.straße, der Verweildauer am Tatort sowie der sich anschließenden Fahrt nach H. … Auch die Angaben des Zeugen F., er habe die Angeklagte spätestens bei dem unmittelbar nach der Tötung stattfindenden Treffen in H. hiervon unterrichtet, finden ihre Bestätigung in der Auswertung der Telekommunikationsdaten. So gab es im Zeitraum zwischen dem 19.12.2012 und dem 23.5.2013 zwischen der Angeklagten und dem Mordopfer P. 374 Telekommunikationsverbindungen. Allein … 18 (fallen) auf den 23.5.2013, den Tag der Ermordung. Die von der Angeklagten am 23.5.2013 um 20:06 Uhr ver-*

[10] Ihr war in einem ersten Verfahren vor dem LG Saarbrücken nicht hinreichend Rechnung getragen worden und hatte im ersten Revisionsdurchgang vor dem 5.Strafsenat zu einer Aufhebung des landgerichtlichen Urteils geführt, vgl. BGH, Beschluss vom 27.8.2014 – 5 StR 259/14 – bei juris

sandte SMS-Nachricht an den in der für die B.straße in S. maßgeblichen Funkzelle eingeloggten Anschluss des Mordopfers, der sich unmittelbar, 35 Sekunden später, eine SMS-Nachricht an den Zeugen F. anschloss, stellt jedoch die allerletzte dieser 374 Verbindungen dar, die sodann abrupt aufhören. Auch E-Mail-Verkehr findet ab diesem Zeitpunkt nicht mehr statt. Die Kammer ist daher überzeugt, dass weitere Verbindungen unterblieben, weil die Angeklagte vom Tod des P. wusste."

(2) Verfahrensgegenstand: Der Angeklagte ist vom Landgericht Chemnitz wegen Totschlags (§ 212 StGB) zu einer Freiheitsstrafe von neun Jahren verurteilt worden.[11] Der in D. lebende Angeklagte und seine Freundin H., die mit dem späteren Tatopfer in Ch. eine Scheinehe führte, stachen gemeinsam im Rahmen einer streitigen Auseinandersetzung in der Wohnung des Opfers auf dieses jeweils mit einem Messer ein und verletzten es tödlich. Nachdem sie gemeinsam geflüchtet waren, bemerkte die gesondert Verfolgte H., dass sie während der Tat ihre goldene Kette verloren hatte. Sie bat den Angeklagten, nochmals in die Wohnung zu gehen und das Schmuckstück zu holen. Der Angeklagte brach daraufhin etwa 30 Minuten nach dem Verlassen des Tatortes über eine Balkontür erneut in die Wohnung ein, ohne jedoch die später unter dem Leichnam sichergestellte Kette zu finden.

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte bestritt in der Hauptverhandlung vor der Strafkammer seine Tatbeteiligung und behauptete, er habe schon vor dem Tod des Geschädigten dessen Wohnung verlassen – nämlich etwa drei Stunden vor dem festgestellten Tatzeitpunkt. Zu dem nachfolgenden Einbruch in die Tatwohnung erklärte er, hierzu von H. gedrängt worden zu sein, nachdem sie „ihn dann kontaktiert (habe)".

Ihre Überzeugung davon, dass der Angeklagte (Mit-)Täter des Totschlags war, stützte die Strafkammer maßgeblich auch auf die Auswertung der Telekommunikationsdaten. Danach war aufgrund fehlender Telefonverbindungen zwischen den Handys der Beteiligten ausgeschlossen, dass H. nach einer von ihr allein begangenen Tat den Angeklagten telefonisch hätte kontaktiert haben

[11] LG Chemnitz, Urteil vom 27.11.2014, Az. 1 Ks 210 Js 1692/14; BGH, Beschluss vom 3.6.2015 – 5 StR 145/15.

können, um ihn nach mehrstündigen Aufenthalt in der für ihn fremden Stadt Ch. nochmals zu treffen und zur Suche nach dem verlorenen Schmuckstück aufzufordern. Zudem ergab die Verkehrsdatenauswertung, dass sich der Angeklagte jedenfalls noch über zwei Stunden nach seinem angeblichen Verlassen des späteren Tatortes mit seinem Handy in der die Wohnanschrift des Tatopfers abdeckenden Funkzelle befand.

(3) Verfahrensgegenstand: Die Angeklagte ist vom Landgericht Berlin wegen Mordes in Tateinheit mit Raub mit Todesfolge (§§ 211, 251 StGB) zu einer Freiheitsstrafe von zwölf Jahren verurteilt worden.[12] Der aus Serbien stammende Angeklagte reiste mit seinem Komplizen N. häufiger nach Deutschland und ins angrenzende Ausland zur gemeinsamen Begehung von Straftaten. Im April 2013 beschlossen sie zusammen mit den Mittätern T. und M., in Berlin einen Juwelier unter Einsatz eines Revolvers mit selbst gebautem Schalldämpfer zu überfallen. Der Angeklagte suchte mit M. am Vormittag des 29. April 2013 das für den Überfall ausgewählte Geschäft auf, wo M. den Juwelier sogleich erschoss. Der Angeklagte nahm Schmuckstücke aus den Auslagen an sich und floh zusammen mit seinen drei Komplizen nach Serbien, wo man die Beute für 43.000 Euro veräußerte.

Ermittlungstaktische Bedeutung von Verbindungsdaten: Die Kriminalpolizei ermittelte im Anschluss an das Verbrechen durch eine Abfrage der Verkehrsdaten, die in der den Tatort abdeckenden Funkzelle angefallen waren, serbische Telefonnummern, die zur Tatzeit genutzt worden waren. Die Datenerhebung ergab, dass um 10.58 und um 10. 59 Uhr zwei Verbindungen mit der Rufnummer 00381-65543XXXX in Tatortnähe stattgefunden hatten. Im Rahmen eines Rechtshilfeersuchens wurden die serbischen Behörden um Hilfe bei der Ermittlung der Anschlussinhaber gebeten. Die serbische Polizei teilte mit, dass sie vier Personen wegen des Raubmordes für tatverdächtig halte und benannte den Angeklagten und seine drei Mittäter. Der Angeklagte wurde als Anschlussinhaber der angefragten Telefonnummer 00381 65543XXXX bezeichnet.

[12] LG Berlin, Urteil vom 8.10.2014, Az. 234 Js 228 / 14 Ks 7/14; BGH, Beschluss vom 25.2.2015 – 5 StR 119/15.

Nachfolgend gab das serbische Innenministerium bekannt, der Angeklagte und die drei Tatverdächtigen N., M. und T. als seine Begleiter seien am 19. April 2013 aus Serbien aus- und am 30. April 2013 wieder eingereist. Im Rahmen eines weiteren Rechtshilfeersuchens legte der Angeklagte vor einem serbischen Ermittlungsrichter ein Geständnis ab und stellte sich in Kenntnis des gegen ihn erlassenen Haftbefehls den deutschen Strafverfolgungsbehörden.

Ohne den kurzfristigen Rückgriff auf die bei Netzbetreibern noch vorhandenen Verkehrsdaten nach § 96 TKG hätte das Verbrechen nicht aufgeklärt werden können. Zum späteren Tatnachweis in der Hauptverhandlung vor dem Landgericht spielten die zu Identifizierungszwecken erhobenen Verkehrsdaten keine Rolle mehr.

(4) Verfahrensgegenstand: Das Landgericht Köln hat den Angeklagten – nunmehr rechtskräftig – in dem aufsehenerregenden Fall eines „Mordes ohne Leiche“ gemäß § 211 StGB zu lebenslanger Freiheitsstrafe verurteilt.[13] Der Verurteilung lag als Sachverhalt zugrunde, dass der Angeklagte spätestens Ende März 2007 beschloss, seine von ihm getrennt lebende philippinische Ehefrau L. zu töten. Er wollte die Folgen der Trennungssituation für seine Umgangsmöglichkeit bezüglich des gemeinsamen Kindes nicht hinnehmen und befürchtete weitere Zahlungsverpflichtungen. Vor dem Hintergrund von Plänen seiner Ehefrau, zu einem Verwandtenbesuch auf die Philippinen zu reisen, sah er die Möglichkeit, ihr Verschwinden als freiwilligen Aufenthaltswechsel darzustellen. Am 18. April 2007 telefonierte das spätere Tatopfer L. mit einer Freundin. Sie beendete das Telefonat um 14.45 Uhr mit dem Hinweis, dass ihr Ehemann erscheine. Der Angeklagte suchte zu diesem Zeitpunkt L. auf und tötete sie noch am selben Tag, um das Sorgerecht für das gemeinsame Kind zu erhalten und Unterhaltszahlungen an L. einzusparen. Einzelheiten zum Tatort und zur Art und Weise der Tatausführung der Tötung blieben ungeklärt. Bis zu seinem Ar-

[13] LG Köln, Urteil vom 10.1.2013, Az. 111 Ks 1/12; BGH, Urteil vom 30.12.2014 – 2 StR 439/13, NStZ 2015, 291 s. auch zur vorhergehenden Urteilsaufhebung im 1. Revisionsdurchgang BGH, Urteil vom 22.12.2011 – 2 StR 509/10, BGHSt 57, 71.

beitsbeginn am nächsten Morgen beseitigte der Angeklagte auch die Leiche seiner Ehefrau so, dass sie bis heute nicht gefunden wurde.

Beweisrechtliche Bedeutung von Verbindungsdaten: Nach dem spurlosen Verschwinden der Ehefrau des Angeklagten am 18. April 2007 versuchte die Polizei zunächst lediglich aufgrund einer Vermisstenanzeige ihren Aufenthaltsort zu ermitteln. Erst nachdem sich Mitte August 2007 erhebliche Widersprüche in den Angaben des Angeklagten zu der von ihm vorgetäuschten Legende des Verschwindens ergeben hatten, wurde ein Ermittlungsverfahren wegen des Verdachts eines Tötungsdelikts eingeleitet. Erst ab Ende September 2007 wurden retrograde Verbindungsdaten zu dem Handy des Tatopfers und weiteren verdachtsrelevanten Handys erhoben und Funkzellenauswertungen für Empfangsbereiche durchgeführt, in denen die Tatausführung und eine spätere Leichenbeseitigung nahelag.

Trotz der aufgrund der verstrichenen Zeit teilweise vorgenommenen Datenlöschung bei dem Provider des Mobilfunkanschlusses des Tatopfers L. ergab die Auswertung der noch verfügbaren Verkehrsdaten, dass ihr seit dem Nachmittag des 18. April 2007 ausgeschaltet gewesenes Handy am frühen Morgen des 19. April 2007 für wenige Minuten noch einmal eingeschaltet war, bevor es für immer das Netz verlor. Das Handy der L. befand sich dabei in einer Funkzelle, die Teile eines Hafenbeckens sowie ein Baustellengelände abdeckte, auf dem zu diesem Zeitpunkt die Bodenplatte einer Tiefgarage noch nicht vollständig gegossen war; nach der Wertung des Landgerichts handelte es um ideale Ablageorte für eine Leiche. Ebenfalls am frühen Morgen des 19. April 2007 befand sich auch das Handy des Angeklagten in der betreffenden Funkzelle. Ausweislich der Funkzellenkontakte dieses Mobiltelefons hatte der Angeklagte noch vor Beginn seiner Frühschicht seine Wohnung verlassen und war kurz darauf dorthin zurückgekehrt. Diese Standortdaten wertete das Landgericht in diesem „Indizienprozess“ als Beweiszeichen dafür, dass der Angeklagte bis in die frühen Morgenstunden damit beschäftigt war, die Leiche und Spuren seiner ermordeten Frau verschwinden zu lassen.

Nach Wegfall der Vorratsdatenspeicherung aufgrund der Entscheidung des BVerfG vom 2. März 2010 hätten retrograd die nicht schon zu Vertragszwecken gespeicherten Standortdaten zu den verfahrensrelevanten Mobilfunkanschlüssen nicht mehr erhoben werden können. Bei der nunmehr im Regierungsentwurf (RegE) vorgesehene Vierwochen-Frist für eine Speicherung von Standortdaten in § 113b Abs. 1 Nr. 2 TGK (RegE) wäre wegen des späten Beginns der Ermittlungen wegen eines Tötungsdelikts im vorliegenden Fall ein wesentlicher Teil der beweisrelevanten Verkehrsdaten bereits gelöscht gewesen.

(5) Verfahrensgegenstand: Das Landgericht Würzburg verurteilte den Angeklagten in dem sog. „Autobahnschützen"-Fall wegen vierfachen versuchten Mordes, gefährlicher Körperverletzung und vorsätzlichen gefährlichen Eingriffs in den Straßenverkehr zu einer Gesamtfreiheitsstrafe von zehn Jahren und sechs Monaten.[14] Über 760-mal schoss der Täter in den Jahren 2008 bis 2013 deutschlandweit aus seinem LKW im fließenden Verkehr zumeist auf andere LKW und auf Transporter. Eine PKW-Fahrerin wurde schwer verletzt. Tatorte waren überwiegend Autobahnen.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Zunächst kamen die Ermittlungsbehörden durch eine massenhafte Erfassung von Autokennzeichen an mehreren Autobahnabschnitten dem Angeklagten auf die Spur. Daraufhin wurden zu der Mobilfunknummer des Verdächtigen die Verkehrsdaten erhoben, wobei den Ermittlungsbehörden der „glückliche" Umstand zugute kam, dass der Verdächtige den Mobilfunkanschluss eines Anbieters hatte, der die abrechnungsrelevanten Daten 90 Tage lang speicherte. Die erhobenen Daten glichen sie mit den Funkzellen mutmaßlicher Tatörtlichkeiten und Tatzeiten auf Hunderten von Kilometern deutscher Autobahnen ab. So ließen sich mit Hilfe der Standortdaten weitestgehend Übereinstimmungen mit den relevanten Tatstrecken und Tatzeiten feststellen und konnte die Anwesenheit des Angeklagten an einigen eindeutig festgestellten Tatorten zur Tatzeit

[14] LG Würzburg, Urteil vom 30.10.2014, Az. 801 Js 9341/13.

auch noch retrograd dokumentiert werden. Dadurch erhärtete sich der Tatverdacht.

Im weiteren Verfahren machte der Angeklagte zum äußeren Tatgeschehen weitgehend geständige Angaben. Beweisrechtlich hatte daher die zur Identifizierung des Täters beitragende Erhebung der Verkehrsdaten in der Hauptverhandlung vor dem Landgericht nur noch insoweit Bedeutung, als die Datenauswertung die teilgeständige Einlassung des Angeklagten bestätigte.

(6) Verfahrensgegenstand: Das Landgericht Flensburg verurteilte den Angeklagten, dem ursprünglich mit der Anklage ein versuchter Totschlag zur Last gelegt worden war, wegen gefährlichen Eingriffs in den Straßenverkehr (§ 315b StGB) in Tateinheit mit gefährlicher Körperverletzung (§ 224 StGB) zu einer Freiheitsstrafe.[15] Der zur Tatzeit als „Präsident" der Rockerbande „Hells Angels" in Flensburg fungierende Angeklagte erfuhr in der Nacht zum 23. September 2009 per Mobiltelefon, dass sich diverse Mitglieder der verfeindeten Rockerbande „Bandidos" auf dem Rastplatz einer nahegelegenen Autobahnraststätte aufhielten. Er führte in den nächsten Minuten diverse Mobilfunkgespräche mit dem Ziel, möglichst schnell viele Mitglieder der „Hells Angels" an die Autobahn heranzuführen, denn der von den Kutten tragenden „Bandidos" begangene Gebietsverstoß sollte nicht hingenommen werden. Nachdem die Mitglieder der „Bandidos" zur Weiterfahrt aufgebrochen war, folgten ihnen der Angeklagte und weitere Mitglieder der „Hells Angels" mit mehreren Fahrzeugen. Der Angeklagte überholte den Konvoi der „Bandidos" und streifte dabei vorsätzlich eines von deren Motorrädern. Dessen Fahrer stürzte hierdurch und wurde lebensgefährlich verletzt. Wenige Minuten nach der Tat und seiner Flucht vom Tatort meldete sich der Angeklagte mobiltelefonisch bei einem befreundeten Inhaber einer Kfz-Reparaturwerkstatt, um sein baldiges Erscheinen anzukündigen.

[15] LG Flensburg, Urteil vom 29.4.2011, Az. I Ks 1/10 – 109 Js 18703/09; BGH, Beschluss vom 11.1.2012 – 4 StR 523/11, BeckRS 2012, 03177.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Im Ermittlungsverfahren und in der Hauptverhandlung machten sämtliche unmittelbaren Tatzeugen von ihrem Recht zur Auskunftsverweigerung Gebrauch. Der Tatnachweis beruhte im Wesentlichen auf der Auswertung der retrograden Verkehrsdaten des Mobilfunkverkehrs des Angeklagten, der zwei Mobiltelefone mit sich führte und verwendete, und weiterer den „Hells Angels“ zuzuordnender Personen. Diese nach § 113a TKG a.F. gespeicherten Verkehrsdaten unterfielen der früheren (Übergangs-)Regelung der Vorratsdatenspeicherung[16] und konnten aufgrund der seinerzeit noch gültigen Speicherpflicht der Mobilfunkbetreiber noch erhoben werden. Insbesondere belegten die Geodaten, die bei Gesprächsverbindungen oder Verbindungsversuchen abgespeichert wurden, ein eindeutiges und synchrones Bewegungsbild der beiden Mobiltelefone des Angeklagten. Ohne den seinerzeit noch möglichen Rückgriff auf Vorratsdaten, deren Beweiswert auch im Revisionsverfahren noch thematisiert wurde,[17] hätte das Gewaltdelikt nicht aufgeklärt werden können.

(7) Verfahrensgegenstand: Das Landgericht Darmstadt verurteilte den Angeklagten wegen Mordes in Tateinheit mit Raub mit Todesfolge (§§ 211, 251 StGB) und mit unerlaubter Ausübung der tatsächlichen Gewalt über eine Kriegswaffe (§ 22a Abs. 1 KWKG) sowie wegen weiterer Waffendelikte zu einer lebenslangen Freiheitsstrafe als Gesamtstrafe und stellte die besondere Schwere der Schuld fest (§§ 211, 57a Abs. 1 Ziff.2 StGB).[18] Der Angeklagte lockte das Opfer unter dem Vorwand einer angeblichen Lieferung gestohlener Computer nachts auf ein abgelegenes Grundstück in Offenbach. Nachdem er den Interessenten erschossen und dessen Bargeld entwendet hatte, versenkte er die Leiche mit Unterstützung eines Mitarbeiters seines Unternehmens in einem Fluss. Die Leiche wurde erst nach einigen Wochen entdeckt.

[16] Im Erhebungszeitpunkt galt die durch die einstweilige Anordnung des BVerfG vom 11.3.2008 (1 BvR 256/08, BVerfGE 121, 1) vorläufig modifizierte gesetzliche Regelung des § 100g StPO.
[17] BGH, Beschluss vom 11.1.2012, aaO.
[18] LG Darmstadt, Urteil vom 1.12.2005, Az. 11 Ks - 1200 Js 82718/04; BGH, Beschluss vom 17.1.2007 – 2 StR 208/06.

Beweisrechtliche Bedeutung von Verbindungsdaten: Ausgangspunkt der Ermittlungen war eine Vermisstenanzeige der Ehefrau des Opfers. Sie war es auch, die den ersten Hinweis auf den Täter gab. Aufgrund der Gesamtumstände ging die Staatsanwaltschaft schon vor der Entdeckung der Leiche von einem Tötungsdelikt aus und leitete ein Ermittlungsverfahren ein. Zu den ersten Ermittlungsschritten gehörte die Erhebung der Verkehrsdaten zu den Mobilfunktelefonen des Opfers und des Täters. Im Ergebnis konnte der Täter aufgrund der Verbindungs- und vor allem der Standortdaten überführt und der Tatort festgestellt werden, an dem später eine Patronenhülse gefunden wurde. Die Aussagen des anfänglich als Gehilfen verdächtigen Mitarbeiters des Angeklagten bestätigten das Ergebnis der Auswertung der Verkehrsdaten. Ohne die Verkehrsdaten wäre der Tatnachweis nicht zu führen gewesen. Zudem entlasteten sie den Mitarbeiter, der seine Tatbeteiligung von Anfang an bestritten hatte, für dessen Tatbeteiligung aber anfangs gewichtige Beweiszeichen sprachen. Mittels der Standortdaten konnten die bestehenden Verdachtsmomente ausgeräumt und das Verfahren gegen ihn sodann eingestellt werden. Die Verkehrsdaten waren in diesem Fall mithin für eine umfassende Aufklärung sowohl be- als auch entlastender Tatumstände von entscheidender Bedeutung. Hervorzuheben ist, dass sich auch hier die noch vorhandene Möglichkeit einer Verkehrsdatenerhebung zugunsten eines Beschuldigten auswirkte.

d) Bandendiebstahl

(1) Verfahrensgegenstand: Das Landgericht Braunschweig hat die Angeklagten rechtskräftig wegen mehrfachen schweren Bandendiebstahls (§ 244a Abs. 1 StGB) und weiterer Diebstahlsdelikte zu mehrjährigen Gesamtfreiheitsstrafen verurteilt.[19] Sie hatten sich zusammengeschlossen, um jeweils nachts in Nord- und Ostdeutschland in die Geschäftsräume insbesondere von Postgebäuden einzubrechen. Bei der sich über einen zweimonatigen Zeitraum erstreckenden Serie von insgesamt 17 Einbrüchen erbeuteten sie in 13 Fällen Bargeldbeträge in drei- und vierstelliger Höhe.

[19] LG Braunschweig, Urteil vom 27.1.2015, Az. 1 KLs 72/14 – 201 Js 330161/14; BGH, Beschluss vom 15.8.2015 – 5 StR 274/15.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Zu den ersten drei innerhalb einer Nacht in Niedersachsen begangenen Einbrüchen hatte die Polizei für die Tatorte jeweils eine Funkzellenabfrage veranlasst und die erhobenen Daten untereinander verglichen. Für den ersten und den dritten Tatort waren jeweils für zwei Mobilfunknummern Gesprächsverbindungen verzeichnet. Eine Anschlussinhaberabfrage ergab, dass die Anschlüsse auf eine nicht existente Person angemeldet waren. Aus den Verkehrsdaten für die beiden Handys, die mit den festgestellten Mobilfunknummern verwendet worden waren, ergab sich – bezogen auf deren IMEI-Nummern –, dass in eines der Geräte tagsüber eine auf einen der Angeklagten registrierte SIM-Karte eingelegt war; außerdem zeigten die erhobenen Verkehrsdaten auf, dass beide Handys in der Tatnacht auch in eine Funkzelle in der Nähe des zweiten Tatorts eingeloggt waren. Damit konnte eine Verbindung zwischen den drei Einbrüchen hergestellt werden. In der Folgezeit konnte über Telefonate des bereits identifizierten Tatverdächtigen auch der Nutzer des zweiten Handys ermittelt und weiter festgestellt werden, dass beide Angeklagten auch bei Begehung von drei weiteren Einbrüchen untereinander und mit anderen Tatbeteiligten telefonierten. Nach dem 17. Einbruch konnten die Angeklagten schließlich auf frischer Tat festgenommen werden.

Ohne den kurzfristigen Rückgriff auf die bei Netzbetreibern noch vorhandenen Verkehrsdaten nach § 96 TKG hätte die Tatserie nicht aufgeklärt werden können. Beweisrechtlich hatten die zur Identifizierung der Täter führenden Verkehrsdaten in der Hauptverhandlung vor dem Landgericht nur noch insoweit Bedeutung, als sie die übereinstimmenden Geständnisse der Angeklagten bestätigten.

(2) Verfahrensgegenstand**:** Das Landgericht Kiel hat die Angeklagten rechtskräftig wegen mehrfachen schweren Bandendiebstahls (§ 244a Abs. 1 StGB) zu Gesamtfreiheitsstrafen verurteilt.[20] Die fünf aus Albanien stammenden Verurteilten verübten in der Umgebung von Kiel eine Reihe von Wohnungseinbrüchen.

Ermittlungstaktische Bedeutung von Verbindungsdaten: Im Rahmen von Ermittlungen gegen eine weitere albanische Tätergruppierung wurde die Polizei auf die von den Angeklagten gebildete Bande aufmerksam. Anhand einer Verkehrsdatenerhebung zu zwei von den Angeklagten genutzten Handys ließen sich hinreichend konkrete Erkenntnisse zu den an der Bandenabrede Beteiligten gewinnen, sodass als weitere Ermittlungsmaßnahmen eine Überwachung der Telekommunikation und Observationen ermittlungsrichterlich angeordnet werden konnten. Im Rahmen einer Observation wurden sie auf frischer Tat ertappt. In der Hauptverhandlung vor dem Landgericht legten die Angeklagten überwiegend Geständnisse ab. Zum Tatnachweis spielten die zu Identifizierungszwecken erhobenen Verkehrsdaten keine nennenswerte Rolle mehr.

(3) Verfahrensgegenstand**:** Die Angeklagten sind vom Landgericht Hamburg rechtskräftig unter anderem wegen schweren Bandendiebstahls in mehreren Fällen (§ 244a Abs. 1 StGB) sowie wegen unerlaubter Ausübung der tatsächlichen Gewalt über eine Kriegswaffe (§ 22a Abs. 1 KWKG) zu mehrjährigen Gesamtfreiheitsstrafen verurteilt worden.[21] Sie hatten sich zusammengeschlossen, um gewerbsmäßig in Geschäftsräume in Hamburg und Umgebung einzubrechen. Hierbei gingen sie arbeitsteilig vor (einige Täter nahmen die Einbrüche vor, andere sicherten die Umgebung ab), waren am Tatort maskiert und entfernten sich mit der Beute unter Einsatz eines Sattelschleppers. Hierbei entstand jeweils erheblicher Schaden von bis zu 250.000 Euro.

[20] LG Kiel, Urteile vom 1.12. und 9.12.2014, Az. 10 KLs 21/14 u. 47/14 – 593 Js 11540/14; BGH, Beschlüsse vom 4.8.2015 – 5 StR 279/15 u. 280/15.
[21] LG Hamburg, Urteil vom 28.2.2012, Az. 616 KLs 17/11 - 6600 Js 30/11.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Die Überwachungskameras eines der geschädigten Betriebe zeichneten zwar das Tatgeschehen auf. Anhand der Überwachungsbilder war allerdings eine Identifizierung der Täter wegen deren Maskierung nicht möglich. Auf dem Videofilm war indes erkennbar, dass die Täter während der Tatbegehung mehrfach und auch länger telefonierten. Vor diesem Hintergrund wurde die Funkzelle des Tatorts ausgemessen und von den Providern die in der tatortrelevanten Funkzelle gespeicherten Verbindungsdaten auf richterliche Anordnung hin mitgeteilt. Anhand dieser Daten konnte ermittelt werden, dass sich am Tatort und in dessen unmittelbarer Umgebung bei Tatbegehung vier Täter aufgehalten hatten, die untereinander in verschiedener Weise miteinander mehrfach in telefonischem Kontakt gestanden hatten. Ferner konnten die IMEI-Nummern festgestellt und anschließend ermittelt werden, mit welchen Rufnummern die Geräte nach Austausch von SIM-Karten im Zeitpunkt der Ermittlungen betrieben wurden. Hierdurch ließen sich die Identitäten der Täter aufklären; die so überführten Angeklagten gestanden in der Hauptverhandlung die Taten überwiegend.

(4) Verfahrensgegenstand**:** Das Landgericht Münster verurteilte die Angeklagten rechtskräftig wegen einer Vielzahl von Diebstahls- und Computerbetrugsdelikten zu mehrjährigen Gesamtfreiheitsstrafen.[22] Die Angeklagten verübten zahlreiche Einbruchsdiebstähle, im Wesentlichen in öffentliche Gebäude wie Kindergärten, Schulen oder kirchliche Einrichtungen. Jeweils einer der Angeklagten hatte die Aufgabe, seinen Mittäter zum Tatort zu fahren und ihn zu sichern, während der Komplize in die jeweiligen Tatobjekte einbrach. Die Angeklagten sorgten in den Fällen, in denen sie beteiligt waren, auch für den Absatz der Beute. Während der Ausführung der einzelnen Taten stand der den Einbruch ausführende Mittäter jeweils über Mobiltelefon mit seinen Komplizen in ständiger Verbindung, um gegebenenfalls unverzüglich gewarnt werden zu können.

[22] LG Münster, Urteil vom 7.12.2009, Az. 8 KLs 81 Js 187/09 (17/09); BGH, Beschluss vom 4.11.2010 – 4 StR 404/10, NJW 2011, 467.

Beweisrechtliche Bedeutung von Verbindungsdaten: Im weiteren Verfahren machten die Angeklagten weitgehend geständige Angaben, die teilweise allgemein gehalten waren. Beweisrechtlich hatte daher die ursprünglich zur Identifizierung der Täter erfolgende Erhebung der Verkehrsdaten in der späteren Hauptverhandlung noch insoweit Bedeutung, als sie die teilgeständige Einlassung des Angeklagten bestätigten. Diese nach § 113a TKG a.F. gespeicherten Verkehrsdaten unterfielen der früheren (Übergangs-)Regelung der Vorratsdatenspeicherung und konnten aufgrund der seinerzeit gerade noch gültigen Speicherpflicht der Mobilfunkbetreiber noch erhoben und verwertet werden. [23]

e) Betäubungsmittelhandel

Verfahrensgegenstand: Das Landgericht Hamburg hat die Angeklagten rechtskräftig u.a. wegen Handeltreibens mit Betäubungsmitteln in nicht geringer Menge in mehreren Fällen zu mehrjährigen Freiheitsstrafen verurteilt (§ 29a BtMG).[24] Sie erwarben gemeinschaftlich insgesamt etwa 150 kg Marihuana in den Niederlanden, verbrachten das Rauschgift sodann nach Hamburg und verkauften es dort weiter. Dabei gingen sie arbeitsteilig vor: Drei Täter waren an den Beschaffungsfahrten in die Niederlanden beteiligt, während ein weiterer Täter jeweils die Abwicklung und Organisation von Hamburg aus übernommen hatte. Zur Abstimmung untereinander griffen sie maßgeblich auf Telekommunikationsmittel zurück, wobei verschiedene SIM-Karten mit niederländischen und deutschen Rufnummern sowie verschiedene Endgeräte eingesetzt wurden.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die Angeklagten haben auch vor Gericht zur Tat keine Angaben gemacht. Im Zuge der Ermittlungen wie auch im gerichtlichen Verfahren kam den Erkenntnissen aus den Verkehrsdaten deshalb zentrale Bedeutung zu. Zunächst ließ sich für die Rufnummer, die auf Grund einer ermittlungsrichterlich nach § 100a StPO angeordneten Überwachung und Aufzeichnung der Telekommunikation einem konkreten Beschuldigten zugeordnet werden konnte, mit Hilfe von in den Niederlanden im

[23] Siehe oben Fn.16 und zum vorliegenden Fall auch BGH, Beschluss vom 4.11.2010 – 4 StR 404/10, aaO.: Die Revisionsrüge der Verwertung der Standortdaten blieb erfolglos.
[24] LG Hamburg, Urteil vom 26.5.2011, Az. 626 KLs 2/11 u. 7/11 - 6004 Js 232/10.

Wege der Rechtshilfe erhobenen Standortdaten nachweisen, dass sich der Nutzer des Telefons zu den fraglichen Zeiten (der Beschaffungsfahrten) jeweils in den Niederlanden aufgehalten hatte. Weiter war anhand der in Deutschland für die den Angeklagten zuzuordnenden Mobilfunkanschlüsse ein Rückschluss auf ihre Abwesenheit vom Bundesgebiet möglich. Denn während der Zeiträume der vorgeworfenen Beschaffungsfahrten waren keine Daten im deutschen Mobilfunknetz angefallen. Dies korrespondierte mit einer Abrede, die im Zuge der Gesprächsüberwachung – nach § 100a StPO – mitgeschnitten worden war. Hiernach war zwischen den Angeklagten vereinbart worden, ihre Mobiltelefone während der Beschaffungsfahrten auszuschalten und in Hamburg zu belassen. Für in früheren Zeiträumen naheliegend durchgeführte Beschaffungsfahrten konnte auf Verkehrsdaten der von den Angeklagten in Deutschland verwendeten Mobiltelefone nicht mehr zurückgegriffen werden.

f) Betrug – „Enkeltrick“

Verfahrensgegenstand: Der Angeklagte wurde durch das Landgericht Hamburg rechtskräftig wegen des mehrfach begangenen Verbrechens eines banden- und gewerbsmäßig begangenen Betrugs (§ 263 Abs. 5 StGB) in der Begehungsweise eines „Enkeltricks“ zu einer Gesamtfreiheitsstrafe von drei Jahren und acht Monaten verurteilt.[25] Bei dieser sehr verbreiteten Betrugsart rufen mobile, häufig aus dem Ausland operierende Täter bei betagten Personen an und spiegeln ihnen vor, in einem verwandtschaftlichen Verhältnis zu ihnen zu stehen und dringend Geld zu benötigen. Häufig erleiden die Opfer schwerwiegende finanzielle und seelische Schäden. Im vorliegenden Fall erbeutete die Bande knapp 70.000 Euro. Der Angeklagte reiste jeweils aus seiner Heimat Litauen in das Bundesgebiet ein, um bei den Geschädigten in deren Wohnungen Bargelder abzuholen.

[25] LG Hamburg, Urteil vom 14.12.2012, Az. 622 KLs 20/12 - 6500 Js 75/12.

Beweisrechtliche Bedeutung von Verbindungsdaten: In dem zunächst gegen unbekannt geführten Verfahren konnten durch Auswertung der Funkzellendaten deutsche und litauische Rufnummern ermittelt werden, die im Zusammenhang mit den Taten standen. Hinsichtlich dieser Nummern und den dazugehörigen IMEI-Nummern wurde die Herausgabe der Verkehrsdaten angeordnet. Aus diesen Daten ergab sich, dass sich der Nutzer der litauischen Rufnummer im Ausland befand und eine Vielzahl von Gesprächen mit einer deutschen Mobilfunknummer führte, wobei der Standort des Nutzers dieser Rufnummer durch dessen Geodaten innerhalb Deutschlands festgestellt werden konnte. Anhand dessen gelang namentlich der Nachweis, dass sich der Angeklagte zu den jeweiligen Tatzeiten jeweils in Tatortnähe aufgehalten hatte.

g) Brandstiftung

Verfahrensgegenstand: Das Landgericht Hannover hat den Angeklagten rechtskräftig wegen schwerer Brandstiftung (§ 306a Abs. 1 StGB) zu einer Freiheitsstrafe von drei Jahren und sechs Monaten verurteilt.[26] Der Angeklagte hatte sich am Abend des 2. November 2009 gegen 19.00 Uhr in die Wohnung des kurzzeitig abwesenden Geschädigten begeben, wo er mit dessen Einverständnis bis zum Vortage gewohnt hatte. Er wollte die Wohnung durch Brandlegung zerstören. Um fahrlässiges Handeln des Geschädigten vorzutäuschen, schaltete er in der Küche eine Herdplatte an, auf die er einen brennbaren Gegenstand legte. Danach legte er in der Schlafecke des Wohnraums Feuer, das, wie beabsichtigt, auf das Bett übergriff; Hitzeschäden und Rauchgasablagerungen machten die gesamte Wohnung unbenutzbar. Während der Löscharbeiten erschien der Angeklagte und erklärte einem Polizeibeamten, er sei gekommen, um Medikamente zu holen, die er bei seinem Auszug zurückgelassen habe.

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hatte sich in der Hauptverhandlung dahin eingelassen, er sei erstmals nach Beginn der Löscharbeiten am Gebäude eingetroffen. Um die von ihm benötigten Medi-

[26] LG Hannover, Urteil vom 23.4.2010, Az. 46 KLs 6503 Js 92914/09 (31/09); BGH, Urteil vom 13.1.2011 – 3 StR 332/10, BGHSt 56, 127.

kamente zu holen, habe er eine Bahn um 18.55 Uhr ab H. genommen; daher könne er nicht schon zur Zeit der Brandentstehung in S. gewesen sein. Daraufhin hatte das Landgericht mit Beschluss vom 15. Februar 20010 – und damit kurz vor der Aufhebung der (Übergangs-)Regelung zur Vorratsdatenspeicherung durch Urteil des BVerfG vom 2. März 2010 – die Erhebung der beim Mobilfunkprovider gespeicherten Verkehrsdaten des Mobiltelefonanschlusses des Angeklagten angeordnet. Zur Begründung führte es aus, ohne die Datenerhebung, welcher der Angeklagte zugestimmt habe, werde die Aufklärung seines Aufenthalts zur Tatzeit wesentlich erschwert.

Nach Auswertung der erhobenen Standortdaten, die das Mobilfunkunternehmen – eigener Auskunft zufolge – lediglich noch aufgrund seiner gesetzlichen Verpflichtung nach § 113a TKG vorgehalten und für eigene Zwecke nicht mehr benötigt hatte, hielt das Landgericht die Einlassung des Angeklagten für widerlegt. Dabei hat es sich unter anderem darauf gestützt, dass das Mobiltelefon des Angeklagten bereits ab 19.00 Uhr mehrfach an einem zwischen der Wohnung des Geschädigten und dem Bahnhof S. stehenden Funkmast eingeloggt war. Zugleich stellten die Standortdaten ein gewichtiges Indiz dafür dar, dass sich der Anklagte zur Tatzeit am Tatort aufhielt. Damit hätte ohne die (gerade noch) verfügbaren Vorratsdaten der Tatnachweis durch das Landgericht nicht geführt werden können, was im weiteren Verfahren zur Folge hatte, dass mit der Revision in erster Linie die Verwertung der Standortdaten – allerdings erfolglos – gerügt wurde.

2. Zusammenfassende Überlegungen

Die Reihe von Verfahren, in denen beispielhaft die Erhebung von Verkehr- und insbesondere von Standortdaten zur Verbrechensaufklärung in unterschiedlichen Bereichen der Schwerkriminalität beitrug, ließe sich unbegrenzt fortsetzen. Denn bisher waren trotz des Beweismittelverlusts, zu dem der Wegfall gespeicherte Vorratsdaten nach der Entscheidung des BVerfG vom 2. März 2010 geführt hat, in vielen Fällen glücklicherweise noch die von den Providern

zu geschäftlichen Zwecken nach § 96 TKG gespeicherten Verkehrsdaten vorhanden, wodurch bei Aufklärung von Seriendelikten sich zugleich weitere schwere Straftaten der Wiederholungstäter verhindern ließen.[27] Dies darf allerdings nicht darüber hinwegtäuschen, dass in einer Vielzahl von Fällen durch die Aufhebung der gesetzlichen Regelung zur Vorratsdatenspeicherung schwerste Delikte nicht aufgeklärt werden konnten, wie eine Untersuchung des BKA aus dem Jahr 2011 zu den Auswirkungen des Wegfalls der Mindestspeicherungsfristen erschreckend anschaulich gezeigt hat.[28]

Die vorstehend dargestellten 20 Verfahrensskizzen belegen, dass sich Verkehrsdaten teilweise als Indizien zum unmittelbaren Tatnachweis eignen; in der überwiegenden Anzahl der Fällen dienen sie als erster Ermittlungsansatz und wirken sie als Hebel für weitere Ermittlungsschritte. Die Daten liefern grundsätzlich Hinweise auf weitere Personen, die im unmittelbaren zeitlichen und örtlichen Zusammenhang mit der Tat im Kontakt zum Verdächtigen standen, und tragen so dazu bei, die Täterstrukturen aufklären. Ferner können sie Schlüsse auf die jeweilige Anwesenheit eines Verdächtigen an bestimmten Orten zu bestimmten Zeiten tragen, Rückschlüsse auf dessen Reisewege – etwa

[27] Ein anschauliches jüngeres Beispiel aus der Medienberichterstattung liefert etwa der vor dem Landgericht Münster verhandelte Fall, in dem zwei Autobahnbrückenwerfer am 22.6.2015 wegen sechsfachen versuchten Mordes in Tateinheit mit gefährlichem Eingriff in den Straßenverkehr zu langjährigen Gesamtfreiheitsstrafen verurteilt wurden. Nach dem letzten Wurf der aus Langeweile begangenen Tatserie (mit einer Betonplatte) konnte über Funkzellenabfragen an den verschiedenen Tatorten, Abgleich der erhobenen Daten und Handyortung einer der Täter ermittelt werden, der im Rahmen seines alsbald abgelegten Geständnisses auch seinen Mittäter benannte. Siehe hierzu:
http://www.faz.net/aktuell/gesellschaft/kriminalitaet/holzstaemme-auf-die-a1-gericht-bestraft-jungenstreich-als-mordversuch-13662147.html und
http://www.wn.de/Muensterland/2025976-Haftstrafe-fuer-Brueckenwerfer-Kein-Streich-mehr-sondern-versuchter-Mord

[28] Vgl. zusammenfassend und mwN Münch, ZRP 2015, 130: Danach wurden insgesamt Auskunftsersuchen für 5082 Anschlüsse im Zeitraum vom 2.3.2010 bis 26.4.2011 erfasst und ausgewertet; im Bereich der Strafverfolgung konnte in 83 % der Fälle (3521 Anschlüsse) die Straftat nicht mehr aufgeklärt werden. Zutr. merkt Münch, aaO, hierzu an, dieses Ergebnis verdeutliche, dass Verkehrsdaten bei der Strafverfolgung häufig den ersten, sichersten und zugleich effizientesten Ermittlungsansatz darstellen. Wie die hier aufgeführten Beispielsfälle zeigen, gilt dies nicht nur für die nach dem Aufgabenzuschnitt des BKA (§ 4 BKAG) geführten Ermittlungsverfahren. Siehe zu teilweise spektakulären nicht mehr aufklärbaren Fällen auch die Presseinformation des BKA vom 8. Oktober 2010 „Die Bedeutung von Mindestspeicherfristen für Gefahrenabwehr und Strafverfolgung“,
http://www.bka.de/nn_234028/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/101008PresseinformationMindestspeicherfristen.html

bei unerlaubter Drogeneinfuhr oder Schleuserhandlungen – zulassen oder über die jeweils zu einer Telefonnummer feststellbaren Gesprächsverbindungen die Identität eines Anschlussnutzers nachvollziehbar belegen; dies alles, ohne dass hierbei auf Gesprächsinhalte zugegriffen wird, deren Überwachung erst als weiterer Ermittlungsschritt und nur unter den strengen Voraussetzungen des § 100a StPO richterlich angeordnet werden kann zur Klärung eines hinreichend konkretisierten Tatverdachts hinsichtlich einer der dort genannten schweren Katalogstraftaten.

Ein Rückgriff auf gespeicherte Verkehrsdaten kann auch die Aufklärung von Tatserien erleichtern. So ermöglichen etwa Kreuzvergleiche zwischen verschiedenen Funkzellen und unterschiedlichen Tatorten eine Überprüfung, ob jeweils dasselbe Mobiltelefon bzw. derselbe Mobilanschluss dort eingeloggt war. Oftmals hängt die Durchführung tatzeitnaher Ermittlungen, bei denen ein durch Datenlöschung eintretender Beweismittelverlust vermieden werden kann, allerdings von Zufälligkeiten wie etwa dem Anzeigeverhalten eines Tatopfers oder sonstigen Umständen einer Tatentdeckung ab, in deren Anschluss erst neben einer Sicherung und Auswertung von Tatortspuren eine Verkehrsdatenerhebung erfolgen kann. Zu diesen von den Ermittlungsbehörden schon nicht steuerbaren Umständen kommt bisher die Zufälligkeit hinzu, für welche Zeitdauer der jeweilige Funknetzbetreiber aus geschäftlichen oder betriebstechnischen Gründen die beim ihm anfallenden Verkehrsdaten speichert; die Zeitspanne reicht von mehreren Tagen bis zu mehreren Monaten. Mit der beabsichtigten Neuregelung der Vorratsdatenspeicherung wird dem vorgebeugt, indem die Telekommunikationsanbieter gemäß § 113b Abs. 1 Nr. 2 TGK (RegE) verpflichtet werden, Standortdaten für vier Wochen zu sichern.

Die Verfahrensskizzen zeigen ferner, dass den durch eine Verkehrsdatenauswertung gewonnenen Erkenntnissen eine entscheidend entlastende Wirkung zukommen kann. Gerade bei dem Rückschluss auf den Nutzer eines tatrelevanten Mobiltelefons ist einem Beschuldigten durch die Verkehrsdaten das Vorbringen verdachtsentkräftender Umstände – etwa in Form einer Alibibe-

hauptung (vgl. vorstehend die Fälle zu I.1.b [4], 1.c [6]) – in verschiedener Hinsicht möglich.

3. Bedeutung von Verkehrsdaten auf weiteren Deliktsfeldern

Über die vorstehend anhand von Verfahren aus dem Alltag der Ermittlungsbehörden und Strafgerichte beschriebene Bandbreite von dort bearbeitenden Erscheinungsformen der Schwerkriminalität hinaus gibt es zahlreiche Deliktstypen, in denen Verkehrsdaten wegen spezifischer Tatbegehungsweisen eine besondere Bedeutung als bisweilen einziger Ermittlungsansatz zukommt.[29]

a) Kinderpornographie in Kommunikationsnetzen

Hinzuweisen ist zunächst auf die besondere Bedeutung von Bestandsdaten zu IP-Adressen im Kontext mit der effektiven Verfolgung einer Verbreitung von Kinderpornographie im Internet. Der Austausch von kinderpornografischem Material wurde inzwischen weitgehend ins Internet verlagert. Deutsche Ermittlungsbehörden erfahren hiervon und den damit begangenen Straftaten auf unterschiedliche Weise. Regelmäßig werden durch ausländische und internationale Polizeidienststellen (wie FBI und Europol) beispielsweise zu deutschen Nutzern die sie betreffenden Daten von sichergestellten Servern oder anderweitig ermittelte Informationen übersandt. Polizeiliche Aufgabe ist es dann zu versuchen, die Personen hinter den IP-Adressen zu ermitteln und so aufzuklären, wer sich kinderpornografisches Material bestellt oder dieses verbreitet hat. Allein vom National Center for Missing & Exploited Children (NCMEC) werden aus den USA monatlich mehrere hundert Fälle an das BKA übersandt. Infolge Löschung bzw. Nichtspeicherung der Verkehrsdaten (d. h. der dynamischen IP-Adressen) ist es kaum möglich, den Besteller ausfindig zu machen. Oft fehlt so der einzige Ermittlungsansatz und die Täter bleiben unentdeckt. Dies dürfte zu-

29 Siehe hierzu die Übersichten des BKA, aaO (Fn. 28).

künftig mit Blick auf jüngste Gesetzesänderungen weiter an Bedeutung gewinnen.[30]

Die Konsumenten von Kinderpornographie werden sich naheliegend einer neu geschaffenen Zugriffsmöglichkeit auf Verkehrsdaten auch nicht dadurch entziehen, dass sie den Datenabruf von Internet-Cafés aus betreiben; sie suchen erfahrungsgemäß die Privatheit und werden den eigenen Internet- bzw. Telefonanschluss auch weiterhin nutzen. Die Ausweitung der Speicherung ist naheliegend geeignet, über die bereits bestehenden Ermittlungsinstrumente der §§ 95, 96 TKG, § 15 TMG und § 100j StPO hinaus (Abfrage von Nutzer-, Bestands- und Verkehrsdaten mittels Auskunftsersuchen nach §§ 161, 163 StPO), eine zahlenmäßig breitere Aufklärung – gerade auch in der Pyramide der Täter nach oben hin – zu ermöglichen. Insbesondere ist eine erleichterte Aufklärung der Hintergründe und Ursprünge („Wer hat die Datei wann zuerst hochgeladen?“) sowie – jedenfalls in Einzelfällen – die Ermittlung des Aufenthaltsortes eines abgebildeten Kindes absehbar.

b) Internetbasierte Kriminalität

Ein hier ebenfalls nur zu streifender, für die Ermittlungsbehörden höchst relevanter Kriminalitätsbereich, in dem Aufklärungsmöglichkeiten bei fehlenden Mindestspeicherfristen kaum bestehen, sind die über das Internet als Tatmittel begangenen Delikte.[31] Schwerwiegendere Kriminalitätserscheinungen in diesem Bereich sind insbesondere gewerbs- und bandenmäßige über das Internet und ergänzend unter Zuhilfenahme von Telekommunikationseinrichtungen begangene (Computer-) Betrugstaten und Cyberangriffe zur Schädigung von Unternehmen, öffentlichen Einrichtungen und Privatleuten insbesondere über sogenannte Botnetze.

[30] Vgl. Neunundvierzigstes Gesetz zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht v. 21. Januar 2015, BGBl. I, S. 10 ff.
[31] Vgl. den Überblick des BKA in: Cybercrime, Bundeslagebild 2012; instruktiv einführend hierzu auch der Lexikon-Artikel „Internetkriminalität“ bei Wikipedia.

Indem sich Täter beispielsweise mit fremden oder gefälschten Zugangsdaten bei Internet-Providern einloggen, können sie unbefugt so genannte SIM-Locks bei Mobiltelefonen entsperren und erhalten so Zugang zu Telefonanschlüssen, unter deren Verwendung weitere Straftaten begangen werden.[32] Ließe sich hier die verwendete IP-Adresse ermitteln, könnten die bei der Zugangserschleichung zu Telefonanschlüssen anfallenden Logdaten ausgewertet und Täter identifiziert werden. Um Straftaten aufklären zu können, die Cyberkriminelle über „gekaperte" Rechner begangen haben, zu denen sie sich über mittels Trojaner eingeführter Schadsoftware Zugang verschafften, und zugleich die Botnetze zu vernichten, ist es unentbehrlich zu wissen, welche Geräte Teil des Netzes sind. Wenn bekannt ist, wer hinter der IP-Adresse eines Bot steht, wer Inhaber eines zum Zwecke des Identitätsdiebstahls infizierten Geräts ist, können die Opfer kontaktiert werden, die ihre missbrauchten Geräte durch „Reinigen" aus dem Botnetz trennen und ggf. noch verhindern können, dass von den Tätern mit ausgespähten Online-Zugangsdaten zu Bank- und Kreditkartenkonten Abhebungen durchgeführt werden. Andernfalls können selbst bei Überführung eines Täters, der Botnetze über seinen Rechner und angemietete Server steuert, die durch das Ausspähen ihrer Daten (§ 202a StGB) Betroffenen nicht informiert werden, die durch noch nicht ermittelte Komplizen des Täters weiterhin mit Schäden infolge eines Bankdatenmissbrauchs (§ 152b StGB, § 263a StGB) bedroht sind.[33]

c) Terroristische Straftaten

Nicht zuletzt weist das BKA – aus ermittlungsrichterlicher Sicht völlig zu Recht – auch darauf hin, dass (jenseits gefahrenabwehrrechtlicher Aspekte) die Strafverfolgung gerade auch terroristischer Straftaten, etwa solche von Mitgliedern oder Unterstützern des sog. Islamischen Staats, ohne Verkehrsdatenspei-

[32] vgl. zu Beispielsfällen Presseinformation des BKA vom 8. Oktober 2010 „Die Bedeutung von Mindestspeicherfristen für Gefahrenabwehr und Strafverfolgung", aaO.

[33] Dies zeigte sich beispielhaft in einem vom Landgericht Berlin mit Urteil vom 12.2.2014 (Az. 536 KLs 8/13 – 255 Js 750/13) entschiedenen Fall (vgl. BGH, Beschluss vom 29.7.2014 – 5 StR 233/14, bei juris), in dem der Angeklagte, der ua wegen Geldwäsche, Computerbetrugs und gewerbsmäßiger Fälschung von Zahlungskarten zu einer mehrjährigen Gesamtfreiheitsstrafe verurteilt wurde, zur Begehung seiner Straftaten insgesamt vier Botnetze betrieben hatte.

cherung deutlich erschwert oder gar unmöglich sei.[34] Mit Hilfe dieser Daten können die Anrufziele der etwa in den Irak oder nach Syrien ausgereisten Verdächtigen, die zuvor in Deutschland häufig in Kontakt zu anderen Personen der islamistischen Szene gestanden haben, erhellt und hierdurch Erkenntnisse über die Strukturen und Beteiligtenkreise im Bundesgebiet gewonnen werden. Indem Unterstützer ermittelt und strafrechtlich verfolgt werden, lässt sich islamistischer Terrorismus effektiv durch das Strafrecht bekämpfen und generalpräventiv terroristischen Straftaten vorbeugen. Namentlich lassen sich Urheber im Internet hochgeladener, gewaltverherrlichender Videos ermitteln.

Hingegen geht die Erwägung fehl, wonach die Terroranschläge von Paris im Januar 2015 die Ungeeignetheit der Verkehrsdaten zur Abwehr terroristischer Gewalttaten belegen könne. Die in Frankreich mit besonders langer Speicherfrist vorrätig gehaltenen Verkehrsdaten konnten den Anschlag zwar nicht verhindern; dies schaffen andere repressive und eben nicht gefahrenabwehrrechtliche Ermittlungsinstrumente, wie etwa Wohnraumdurchsuchungen, jedoch ebenfalls nicht. Ermöglicht wird aber insbesondere durch die Erhebung von Verbindungsdaten der von den Tätern verwendeten Mobilfunkanschlüsse eine Aufhellung ihres Umfeldes, ihrer Kontaktpersonen und Unterstützer. So konnten die französischen Sicherheitsbehörden anhand gespeicherter Verbindungsdaten Kontakte der Terroristen untereinander und zu anderen Islamisten schnell nachvollziehen, was bei der schnellen Aufklärung und Bewertung einer möglichen weiteren Bedrohung half.

Insofern lässt sich ausmalen, welche wichtigen Hinweise nach Aufdeckung der NSU-Terrorzelle im November 2011 die Verbindungs- und Standortdaten zu den mehreren weitgehend zerstört sichergestellten Handys der Gruppe hätten liefern können, wären diese Daten noch in nennenswertem Umfang gespeichert und durch die seinerzeit von den Ermittlungsrichtern des BGH nach § 100g StPO erlassenen Anordnungen zu erheben gewesen. Die einen Unterstützerkreis der Gruppe betreffenden Fragen aufzuklären, wie es gegenwärtig im

[34] Münch, ZRP 2015, 131 f.

Strafprozess vor dem OLG München mühselig mit teilweise unwilligen Zeugen versucht wird, wäre sicher leichter gefallen.

Ein aktuelles Beispiel aus dem Bereich der Bekämpfung terroristischer Straftaten in Deutschland, bei dem der nicht nur für die Strafverfolgung, sondern vor allem auch für die Gefahrenabwehr wichtige Erfolg offenbar auch durch einen Zugriff auf Verkehrsdaten ermöglicht worden ist, stellt der Fall des in der Nacht zum 30. April 2015 verhafteten Salafisten-Paares dar, das in den Wochen zuvor eine funktionsfähige Rohrbombe gebaut und im Keller seines Hauses zusammen mit Waffenteilen und Munition gelagert hatte. Das Paar wohnte in der Nähe der Strecke eines traditionell zum 1. Mai veranstalteten Frankfurter Radrennens. Der Beschuldigte Halil D., der Kontakt zu mehreren aus dem Kriegsgebiet in Syrien zurückgekehrten Islamisten hielt, hatte in den Tagen vor seiner Festnahme mehrfach auch entferntere, als Beobachtungs- und Anfeuerungsorte für Zuschauer geeignete Plätze entlang der Strecke des Radrennens näher inspiziert, das nach Aufdeckung seines kriminellen Tuns abgesagt werden musste. Der *Spiegel* hob in seinem Bericht[35] über den Lauf des Ermittlungsverfahren auch das erhebliche Glück hervor, das bei dem Aufklärungserfolg der Ermittlungsbehörden und ihrer Verhinderung eines mutmaßlich geplanten Terroranschlags in Deutschland erneut im Spiel war:

> *„Glück, dass eine Baumarktkassiererin so aufmerksam war. Glück, dass es nicht nur ein Überwachungsvideo gab, sondern auch einen Fingerabdruck, und dass die Daten der Funkzelle noch nicht gelöscht waren.“*

Sich auf derartiges Glück nicht mehr im bisherigen Ausmaß verlassen zu müssen, wird naheliegend nach einer Wiedereinführung der Vorratsdatenspeicherung die künftige Ermittlungsarbeit zur Verhinderung drohender und Aufklärung begangener terroristischer Gewaltdelikte erleichtern.

[35] Ausgabe Nr. 20 vom 9.5.2015, S. 34, 36.

II. Gutachten des Max-Planck Instituts aus dem Jahre 2011

1. Fehlende Belastbarkeit des gutachterlichen Ergebnisses

Vor dem Hintergrund der vorstehend geschilderten eigenen praktischen Erfahrungen und der hierdurch begründeten Erwartung betreffend einer Speicherpflicht mit einer Höchstspeicherfrist für Verkehrsdaten kann der *Verf.* die vorsichtige Bewertung der praktischen Bedeutung einer Vorratsdatenspeicherung durch das Max-Plack-Institut für ausländisches und internationales Strafrecht (MPI) in Freiburg aus dem Jahre 2011 nicht teilen.

Nach dessen „Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten“ soll diesem Ermittlungswerkzeug in den vom MPI ausgewählt betrachteten Deliktsbereichen – namentlich mit Blick auf die vor und nach Einführung der Höchstspeicherfrist angeblich gleichgebliebenen Aufklärungsquoten – keine signifikante Bedeutung zukommen. Dem Auftragsgutachten zugrunde liegt u.a. eine Auswertung von etwa 80 Gesprächen mit Strafrechtspraktikern aus Polizei, Staatsanwaltschaft und Strafjustiz sowie etwa 50 vom Bundeskriminalamt geführter Ermittlungsverfahren.

Neben den vom MPI selbst zur Belastbarkeit seiner Erhebungen formulierten Bedenken[36] in Bezug auf eine schmale Datenbasis bestehen solche auch mit Blick auf den gewählten gutachterlichen Ansatz. Der Vergleich von Aufklärungsquoten vor und nach Einführung der Speicherfristen lässt schon nicht erkennen, ob es während der Erhebungszeiträume nicht auch andere Ursachen für eine stabile Aufklärungsquote gegeben hat. Ferner können die ausgewerteten Verfahrensakten des BKA keinen zuverlässigen Überblick über sämtliche Kriminalitätsbereiche vermitteln, in denen Verkehrsdaten einen Ermittlungsansatz bieten; befasst sich das BKA bei seinen Ermittlungen nach dem durch § 4 BKAG vorgegebenen Katalog von Straftaten, bei denen es die polizeilichen

[36] Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg, 2. Aufl. 2011, S. 7 ff.; vgl. zu den vom MPI getroffenen Schlussfolgerungen trotz schmaler Datenbasis auch 218, 221 f.

Aufgaben auf dem Gebiet der Strafverfolgung wahrnimmt, doch nur mit sehr ausgewählten Deliktsphänomen, etwa dem Terrorismus, der Spionage oder besonders umfangreicher Bandenkriminalität. Zu letzterer hat das MPI lediglich zwölf Verfahren auswerten können.[37]

Auch die vom MPI ausgewählten Deliktsbereiche erweisen sich als unvollständig. Zunächst erfassen sie solche (etwa das Stalking), um die es gegenwärtig in der Diskussion über den Regierungsentwurf nicht mehr geht. Zum anderen behandelt das Gutachten solche Bereiche nicht, die nach Einschätzung des *Verf.* besonders relevant sind. Gerade bei schweren Raub- und Erpressungstaten haben sich die Verkehrsdaten – wie die vorstehenden Skizzen illustrieren – als effizientes Ermittlungsinstrument und die hieraus gewonnenen Erkenntnisse als gewichtiges Beweismittel erwiesen. Die Bundesregierung erfasst diese Delikte mit Recht in § 100g Abs. 2 Nr. 1 Buchst. g StPO (RegE). Gerade bei der Erpressung belässt es das MPI-Gutachten aber bei einem Hinweis auf die polizeiliche Kriminalstatistik und die hiernach „seit Anfang des Jahrtausends stabile Aufklärungsquote“; eine Untersuchung der Effektivität dieses Instruments auch am Einzelfall fehlt.[38]

Überdies erscheint es unverständlich, wenn die Kriminalitätserscheinung des „Enkeltrickbetrugs“, die zwar „nur“ 0,2% der Betrugstaten ausmachen soll, aber doch häufig die Verbrechensqualifikation eines banden- und gewerbsmäßigen Betrugs nach § 263 Abs. 5 StGB erfüllt, als ein „Randphänomen“ beschrieben wird, was – etwa deshalb? – nicht mit dem Aufwand einer Verkehrsdatenspeicherung verfolgt werden sollte. Ebenso wenig weiterführend ist die Überlegung, durch das Absehen von einer Auswertung von Datenträgern zur Verfolgung der Kinderpornographie könnten die dort verausgabten Haushaltsmittel geschont und stattdessen in die Täterprävention investiert werden.[39] Solches erscheint gerade mit Blick auf das Legalitätsprinzip und die erst jüngst vom Gesetzgeber verabschiedete Verschärfung dieses Teilbereichs des Straf-

[37] MPI, a.a.O., S. 114.
[38] MPI, a.a.O., S. 113.
[39] MPI, a.a.O., S. 221.

rechts[40] bemerkenswert. Überdies verstellt der Vorschlag den Blick darauf, dass ältere Verkehrsdaten insbesondere den Ursprung und den Weg, den eine Bilddatei zurückgelegt hat, zu erhellen und damit Aufklärungsquoten zu steigern vermögen.

Vor allem erstaunt allerdings, dass die im Gutachten dokumentierten Ergebnisse der Praktiker-Interviews ganz überwiegend die hier geäußerte Einschätzung teilen, dass gespeicherte Verkehrsdaten ein Ermittlungsinstrument von erheblicher Bedeutung für die Verbrechensaufklärung sind. Eine Stimme wird dem durch das Gutachten indes nicht verliehen.

2. Möglichkeiten empirischer Erhebungen

Abschließend sei zu Möglichkeiten empirischer Erhebungen in diesem Bereich über die vom MPI in seinem Gutachten selbst dargestellten Problemstellungen hinaus auf Folgendes hingewiesen:

Die Bedeutung des Ermittlungsinstruments „Verkehrsdaten“ lässt sich regelmäßig nicht am Verfahrensergebnis, dem rechtskräftigen Strafurteil, erkennen. Denn Verkehrsdaten sind oftmals nur ein erster Hebel, um die Identität der Täter zu ermitteln, Strukturen zwischen ihnen und anderen Tatbeteiligten zu erhellen und sodann gegebenenfalls mit Hilfe anderer, eingriffsintensiverer Maßnahmen (etwa Überwachung der Telekommunikationsinhalte oder Durchsuchungen) nähere Erkenntnisse zu erzielen. Ein solches weiteres Ermittlungsergebnis oder sogar ein – etwa in Ansehung erdrückender Beweislage – abgelegtes Geständnis ist dann schon vielfach Beweisgrundlage für die Annahme eines hinreichenden Tatverdachts bei Anklageerhebung und noch häufiger für die Überzeugungsbildung des Tatgerichts (§ 261 StPO). Dementsprechend wird in Fällen, in denen die erhobenen Verkehrsdaten nur als erster Ermittlungsansatz eine Rolle spielten, der ursprüngliche Einsatz dieses Ermittlungsinstruments in dem das tatgerichtliche Verfahren abschließenden Urteil nicht mehr erwähnt.

[40] Vgl. Neunundvierzigstes Gesetz zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht v. 21. Januar 2015, BGBl. I, S. 10 ff.

Eine belastbare empirische Untersuchung müsste sich daher in einem repräsentativen Umfang mit Verfahren aus sämtlichen relevanten Deliktsbereichen befassen und hier jeweils den konkreten Ablauf der Ermittlungen untersuchen und den Ablauf der gerichtlichen Beweisaufnahme und Überzeugungsbildung bewerten. Um die Erforderlichkeit einer Verkehrsdatenabfrage und der Effizienz zur Tataufklärung jeweils beurteilen zu können, dürften ermittlungstaktische Kenntnisse und Erfahrungen bei den Gutachtern unabdingbar sein.

III. Fazit

1. Die Möglichkeit einer Verkehrsdatenabfrage ist nach den praktischen Erfahrungen des *Verf*. ein aus der ermittlungstaktischen Arbeit der Strafverfolgungsbehörden nicht wegzudenkendes Ermittlungsinstrument. Die Annahme des BVerfG[41], dass „hierdurch Aufklärungsmöglichkeiten geschaffen (werden), die sonst nicht bestünden und angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind“, hat sich auch nach seinem Urteil vom 2. März 2010 – trotz der durch Wegfall der Vorratsdatenspeicherung entstandenen Schutzlücke – in unzähligen Strafverfahren bestätigt.
2. Die geschäftsmäßige Speicherung der Verkehrsdaten durch die betreffenden Telekommunikationsunternehmen (§ 96 TKG) bietet keine ausreichende Grundlage für eine rechtsstaatliche Aufklärung schwerer Straftaten. Die vom Regierungsentwurf vorgesehene Wiedereinführung einer Speicherpflicht von Telekommunikationsunternehmen ist notwendig, um zu vermeiden, dass die Ergebnisse von Strafverfahren zufallsbedingt von

[41] BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08, u.a., BVerfGE 125, 260, Rn. 207; ähnlich der EuGH, in seinem Urteil vom 8.4.2014 – C-293/12, NJW 2014, 2169, 2171:
„Zu der Frage, ob die Vorratsspeicherung der Daten zur Erreichung des mit der Richtlinie 2006/24 verfolgten Ziels geeignet ist, ist festzustellen, dass angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die nach dieser Richtlinie auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und insoweit daher ein nützliches Mittel für strafrechtliche Ermittlungen darstellen.“

dem Zeitpunkt eines Ermittlungsbeginns und von der unterschiedlichen Praxis der Telekommunikationsunternehmen hinsichtlich Umfang und Dauer von Speicherungen abhängen; diese Praxis ist nach Maßgabe ihrer eigenen geschäftlichen Bedürfnisse willkürlich und – wie die weite Verbreitung von Flatrates und ein damit einhergehendes Entfallen von Verbindungs-Einzelabrechnungen zeigt – einem rasanten Wandel unterworfen. Zufallsbedingte Verfahrensergebnisse sind mit den – auch verfassungsrechtlichen – Anforderungen an eine gleichmäßige funktionstüchtige Strafrechtspflege unvereinbar.

3. Die mit dem Gesetzentwurf beabsichtigte Speicherung von Verkehrsdaten bei privaten Telekommunikationsprovidern unterscheidet sich in der praktischen Ausgestaltung nicht von der geschäftsmäßigen Speicherung von Verkehrsdaten durch diese Unternehmen aufgrund der vertraglichen Beziehungen mit ihren Kunden. Eine staatliche „Überwachung“ aller Nutzer mobiler Telekommunikation ist mit dem geplanten Gesetz nicht verbunden.

4. Der Gesetzentwurf will sicherstellen, dass kurzfristig gespeicherte Verkehrsdaten von den Strafverfolgungsbehörden nur zur Aufklärung schwerwiegender Straftaten und nur mit richterlicher Genehmigung abgerufen und verwendet werden dürfen. Dass die Hürden für diese Maßnahme mit dem Straftatenkatalog nach § 100g Abs. 2 StPO (RegE) allerdings ebenso hoch sein sollen wie bei der – freilich ungleich tiefer in die Grundrechte eingreifenden – Anordnung einer Wohnraumüberwachung nach § 100c StPO und damit sogar strenger als bei einer Überwachung von Inhalten einer Telekommunikation nach § 100a StPO, ist schwerlich nachzuvollziehen. Der Gesetzentwurf lässt eine Begründung für diese Beschränkung einer Erhebungsbefugnis nach § 100g StPO (RegE) vermissen, die dem Gesetzeszweck effektiver Verfolgung schwerer Straftaten zuwider läuft, innerhalb des Gefüges telekommunikationsbezogener Ermittlungsmaßnahmen systemwidrig erscheint und die auch nicht durch eine vom BVerfG vorgegebene Anforderung an ein verfassungsgemäßes

Gesetz geboten ist. In spezifischen Deliktsbereichen sind nach der geplanten Regelung Schutzlücken zu erwarten. So kommt Verkehrsdaten gerade bei der Aufklärung von nicht im Katalog enthaltenen Raubstraftaten (§ 249 Abs. 1 StGB) eine hohe Bedeutung zu (vgl. beispielhaft oben Fall I. 1 a) [1]). Deshalb erscheint hier und etwa auch hinsichtlich des Qualifikationstatbestands eines Verbrechens des bandenmäßigen und gewerbsmäßigen Betrugs (§ 263 Abs. 5 StGB) eine Anlehnung an den für die Überwachung von Telekommunikationsinhalten geltenden (weitergehenden) Straftatenkatalog nach § 100a Abs. 2 StPO sinnvoller.

5. Die sehr knapp bemessenen Speicherfristen insbesondere von nur vier Wochen für Standortdaten (§ 113b Abs. 1 Ziff.2 TKG RegE) dürften sich in der Rechtsanwendungspraxis als zu kurz erweisen, um dem Gesetzeszweck noch gerecht zu werden.

6. Zur Verbesserung des Schutzes der Persönlichkeitsrechte von Beschuldigten wäre es im Übrigen zu begrüßen, wenn das Gesetz bei der richterlichen Anordnung der Herausgabe von Verkehrsdaten – ebenso wie auch bei sämtlichen weiteren an die Provider gerichteten Anordnungen – die Übersendung von Kurzausfertigungen der richterlichen Beschlüsse für eine wirksame Abfrage der gespeicherten Verkehrsdaten ausreichen ließe. Hierdurch würden in der Rechtspraxis immer wieder – in Anmaßung eines scheinbaren Prüfungsrechts – artikulierte Zweifel der Provider an der Wirksamkeit einer richterlichen Anordnung einerseits vermieden[42] und andererseits – nicht zuletzt mit Blick auf die Unschuldsvermutung – dem Provider keine Kenntnis von der Art und Schwere der gegen den Beschuldigten erhobenen Tatvorwürfe gegeben.

[42] Vgl. MPI, aaO, S. 154.