Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Bürgerrechte

-

unter besonderer Berücksichtigung
der ermittlungstaktischen und beweisrechtlichen Bedeutung
von Verkehrsdaten in der Ermittlungs- und Verfahrenspraxis
der Strafverfolgungsbehörden und Gerichte[1]

vorgelegt von
Richter am Oberlandesgericht Marc Wenske[2]

Der Entwurf eines Gesetzes zur Stärkung der Bürgerrechte sieht eine Streichung der durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I, S. 2218; im Folgenden: Vorratsdatenspeicherungsgesetz) eingeführten Vorratsspeicherung von Telekommunikations-Verkehrsdaten zu Zwecken der öffentlichen Sicherheit vor.[3] Er stellt damit den vorläufigen Schlusspunkt der rechtspolitischen Diskussion über das in Rede stehende Ermittlungsinstrument dar.

Zur Vorbereitung der rechtspraktischen Bewertung der geltenden Rechtslage sollen die maßgeblichen Regelungen zunächst einleitend zusammenfassend dargestellt werden (**I. u. II.**); sodann soll auf die dem Gesetzesentwurf zugrunde liegenden Bewertungen im Einzelnen näher eingegangen werden, wobei hier der Schwerpunkt auf einer rechtspraktischen Betrachtung des Ermittlungsinstruments gespeicherter Verkehrsdaten liegen wird (**III.**). Abschließend sollen die absehbaren Konsequenzen des Gesetzesvorhabens in den Blick genommen werden (**IV.**).

---

[1] Anhörung des Ausschusses für Recht und Verbraucherschutz vom 13. Juni 2018.
[2] Der Verf. ist Mitglied des mit Revisions- und Beschwerdeverfahren sowie Auslieferungssachen befassten 1. Strafsenats des Hanseatischen Oberlandesgerichts in Hamburg und zugleich Ermittlungsrichter I in Staatsschutzsachen desselben Gerichts; zuvor war er tätig in Großen Strafkammern des Landgerichts Hamburg, am Amtsgericht, dort auch als Ermittlungsrichter, und war abgeordnet als wissenschaftlicher Mitarbeiter an den 5. Strafsenat des Bundesgerichtshofs.
[3] Art. 1, 2, 3 und 6 des Gesetzesentwurfs, BT-Drucks. 19/204.

I. Gesetzessystematischer Hintergrund

Die mit dem Vorratsdatenspeicherungsgesetz eingeführte Speicherpflicht und eingeführte Höchstspeicherfrist für Verkehrsdaten dient nach der Gesetzesbegründung der Vereinheitlichung der Speicherpraxis der Erbringer öffentlich zugänglicher Telekommunikationsdienste. Es soll Unzulänglichkeiten in der Strafverfolgungsvorsorge und der Gefahrenabwehr durch abgestimmte Regelungen in der Strafprozessordnung und im Telekommunikationsgesetz beseitigen.[4]

1. Die erste Tür: Schutzmaßgaben des Telekommunikationsgesetzes

Der durch das Vorratsdatenspeicherungsgesetz neugefasste § 113a Abs. 1 TKG bestimmt mit den Anbietern öffentlich zugänglicher Telekommunikationsdienste für Endnutzer den Verpflichteten der Vorratsdatenspeicherung. Er verpflichtet nunmehr diese – allein – privaten Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, bestimmte und näher spezifizierte Verkehrs- und Standortdaten unabhängig von einem besonderen Anlass für einen bestimmten Zeitraum zu speichern und für die Nutzung durch die Sicherheitsbehörden bereitzuhalten. Verkehrsdaten im Sinne des § 113b Abs. 2 und 3 TKG, etwa Rufnummern, Datum und Uhrzeit von Beginn und Ende der Verbindung, Internetprotokoll-Adressen, müssen gemäß § 113b Abs. 1 Nr. 1 TKG für zehn Wochen gespeichert werden; die Speicherpflicht für Standortdaten nach § 113b Abs. 4 TKG, etwa die Bezeichnungen der Funkzellen bei der Nutzung mobiler Telefondienste, beträgt demgegenüber vier Wochen (vgl. § 113b Abs. 1 Nr. 2 TKG). Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen aufgrund dieser Vorschrift nicht gespeichert werden (vgl. § 113b Abs. 5 TKG). Dieses Speicherverbot gilt gleichermaßen für Daten, die den in § 99 Abs. 2 TKG genannten Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen (§113b Abs. 6 Satz 1 TKG).

Die Speicherung der Daten hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können (vgl. § 113b Abs. 7 TKG). Nach

[4] Vgl. BT-Drucks. 18/5088, S. 21 f.

§ 113b Abs. 8 TKG hat der nach § 113a Abs. 1 TKG Verpflichtete die gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach § 113b Abs. 1 TKG, irreversibel zu löschen oder die irreversible Löschung sicherzustellen. In § 113c TKG werden abschließend (vgl. § 113c Abs. 2 TKG) die zulässigen Verwendungszwecke der nach § 113b TKG gespeicherten Daten normiert. So dürfen etwa gespeicherte Daten an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b TKG genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt. Die Daten sind dabei so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 113b TKG gespeichert waren (vgl. § 113c Abs. 3 Satz 2 TKG).

Weiter wird hier gesetzlich ausdrücklich bestimmt, für welche Zwecke die Daten verwendet werden dürfen und, dass private Telekommunikationsunternehmen von ihrer im Übrigen geltenden Geheimhaltungspflicht insoweit befreit werden. Auch sieht § 113d TKG näher bestimmte Anforderungen an die Gewährleistung der Datensicherheit vor. Der nach § 113a Abs. 1 TKG verpflichtete private Telekommunikationsunternehmer hat gemäß § 113e TKG sicherzustellen, dass für Zwecke der Datenschutzkontrolle jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren der gespeicherten Daten protokolliert wird und etwa die Protokolldaten – Zeitpunkt des Zugriffs, zugreifende Personen, Zweck und Art des Zugriffs – nach einem Jahr gelöscht werden.

2. Die zweite Tür: Staatlicher Abruf allein auf richterliche Anordnung

Ob die Daten an die staatlichen Stellen weitergegeben werden dürfen, also nach der Erhebung durch die privaten Telekommunikationsanbieter auch den Weg durch eine zweite Tür, zu den Ermittlungs- oder Gefahrenabwehrbehörden finden, ist nicht Regelungsgegenstand des Telekommunikationsgesetzes. Die entsprechenden Verfahrenssicherungen für diese zweite Tür und für eine berechtigte Datenübermittlung an staatliche Stellen bestimmt sich für das Strafverfahren nach § 100g StPO.[5] Während in § 100g Abs. 1 die Erhebung von Verkehrsdaten geregelt wird, die aus geschäftlichen

[5] Vgl. BT-Drucks. 18/5088, S. 36, 40.

Gründen bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste gespeichert werden (§ 96 TKG), legt § 100g Abs. 2 StPO fest, unter welchen Voraussetzungen die gespeicherten retrograden Daten erhoben werden dürfen: Gesetzlich zwingend erforderlich sind hier ein durch bestimmte Tatsachen begründeter Verdacht betreffend eine der in § 100g Abs. 2 Satz 2 StPO enumerativ und abschließend aufgeführten besonders schweren Straftaten,[6] die auch im Einzelfall besonders schwer wiegen. Darüber hinaus muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. § 100g Abs. 4 StPO schließt zum Schutz von Berufsgeheimnisträgern im Sinne des § 53 Abs. 1 Satz 1 Nr. 1 bis 5 StPO die Erhebung von Verkehrsdaten nach § 100g Abs. 2 StPO aus.

In formeller Hinsicht wird die Anordnung gesetzlich allein dem Richter überantwortet. Die Überprüfung sämtlicher Anordnungsvoraussetzungen, gerade auch des Tatverdachts und der Tatschwere, unterliegt damit ausschließlich unabhängiger gerichtlicher Kontrolle (Art. 97 Abs. 1 GG; §§ 101a, § 100b Abs. 1 StPO). Schließlich ist nach § 101 a Abs. 6 StPO eine Benachrichtigung der Beteiligten der betroffenen Telekommunikation nach Maßgabe des § 101 Abs. 4 Satz 2 bis 5 und Abs. 5 bis 7 StPO gesetzlich vorgesehen.

II. Rechtsentwicklung nach Inkrafttreten der Neuregelung

Unmittelbar nach Inkrafttreten der vorgenannten Neuregelungen wurden hiergegen Eilanträge beim *Bundesverfassungsgericht (BVerfG)* mit dem Ziel eingereicht, die maßgebenden Bestimmungen des Telekommunikationsgesetzes und der Strafprozessordnung außer Kraft zu setzen; das Bundesverfassungsgerichts hat sämtliche Eilanträge abgewiesen und hierzu in seinen Beschlussgründen namentlich ausgeführt:

> „a) Ein besonders schwerwiegender und irreparabler Nachteil, der es rechtfertigen könnte, den Vollzug der Norm ausnahmsweise im Wege einer einstweiligen Anordnung auszusetzen, liegt in der Datenspeicherung allein nicht.

[6] Vgl. BT-Drucks. 18/5088, S. 31.

Zwar kann die gegenüber den Verpflichteten nach § 113a TKG in § 113b TKG angeordnete umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann für staatliche Zwecke, die sich zum Zeitpunkt der Speicherung der Daten nicht im Einzelnen absehen lassen, einen erheblichen Einschüchterungseffekt bewirken, weil das Gefühl entsteht, ständig überwacht zu werden. Dieser Effekt ließe sich für die Zeit zwischen dem Inkrafttreten der Norm und der Entscheidung des Bundesverfassungsgerichts selbst dann nicht rückgängig machen, wenn die Verfassungsbeschwerde in der Hauptsache Erfolg haben sollte.

Der in der Speicherung für Einzelne liegende Nachteil für ihre Freiheit und Privatheit verdichtet und konkretisiert sich jedoch erst durch einen Abruf der Daten zu einer möglicherweise irreparablen Beeinträchtigung. Die Datenbevorratung ermöglicht zwar den Abruf, doch führt erst dieser zu konkreten Belastungen. Das Gewicht eines denkbaren Einschüchterungseffekts hängt dann davon ab, unter welchen Voraussetzungen die bevorrateten Daten abgerufen und verwertet werden können. Je weiter die Befugnisse staatlicher Stellen insoweit reichen, desto eher müssen die Bürgerinnen und Bürger befürchten, dass diese Stellen ihr Kommunikationsverhalten überwachen (vgl. BVerfGE 121, 1, 20). So ist mit der Speicherung allein jedoch noch kein derart schwerwiegender Nachteil verbunden, dass er die Außerkraftsetzung eines Gesetzes erforderte. Dies gilt auch für die Speicherung der Daten von Berufsgeheimnisträgern.

…

b) Eine Aussetzung des Vollzugs ist auch nicht hinsichtlich der §§ 100g, 101a und 101b StPO geboten.

aa) Allerdings liegt in dem Verkehrsdatenabruf nach § 100g Abs. 1 und 2 StPO ein schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG. Ein solcher Datenabruf ermöglicht es, weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte der Betroffenen zu erlangen, ggf. sogar begrenzte Rückschlüsse auf die Gesprächsinhalte zu ziehen. Zudem weist ein Verkehrsdatenabruf eine erhebliche Streubreite auf, da er neben der Zielperson des Auskunftsersuchens notwendigerweise deren Kommunikationspartner erfasst, also vielfach Personen, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff in ihr Grundrecht aus Art. 10 Abs. 1 GG durch ihr Verhalten nicht veranlasst haben (vgl. BVerfGE 107, 299, 318 ff.; 121, 1, 22).

Doch hat der Gesetzgeber mit § 100g Abs. 2 StPO den Abruf von Telekommunikations-Verkehrsdaten im Sinne des § 113b TKG von qualifizierten Voraussetzungen abhängig gemacht, **die das Gewicht der dem Einzelnen und der Allgemeinheit durch den Vollzug der Vorschrift drohenden Nachteile für die Übergangszeit bis zur Entscheidung über die Hauptsache hinnehmbar und im Vergleich mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen lassen.**“[7]

(Hervorhebungen durch *Verf.*)

Mit Urteil vom 21. Dezember 2016 entschied der *Gerichtshof der Europäischen Union (EuGH)* in den verbundenen Verfahren C-203/15 und C-698/15 über die Vereinbarkeit von Regelungen des Königreiches Schweden und des Vereinigten Königreiches

[7] BVerfG, Beschl. v. 8. Juni 2016 – 1 BvR 229/16, EuGRZ 2016, 501; ebenso Beschl. v. 8. Juni 2016 – 1 BvQ 42/15, NVwZ 2016, 1240.

Großbritanniens und Nordirland mit den Maßgaben der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rats vom 12. Juli 2012 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Er stellte insoweit klar, dass eine allgemeine und unterschiedslose Vorratsdatenspeicherung unionsrechtlich unzulässig sei.[8]

Auch im Lichte dieser allein das Königreich Schweden und das Vereinigte Königreich Großbritannien und Nordirland betreffenden Entscheidung aus dem Dezember 2016 hat das *BVerfG* keinen Anlass gesehen, nunmehr den bei ihm anhängigen Eilrechtsschutzbegehren gegen die Regelungen im deutschen Recht stattzugeben. Auch die unionsrechtlichen Fragen werden damit dem bislang noch nicht vom *BVerfG* entschiedenen Hauptsacheverfahren über die anhängigen Verfassungsbeschwerden überlassen.[9]

Ungeachtet dessen hob das *OVG Nordrhein-Westfalen* in einem von einem Internetprovider betriebenen verwaltungsgerichtlichen Eilrechtsschutzverfahren im Juni 2017 dessen gesetzliche Pflicht zur Speicherung von Verkehrsdaten bis zur Entscheidung über die Hauptsache wegen einer von ihm erkannten Unvereinbarkeit des deutschen Rechts mit unionsrechtlichen Maßgaben auf.[10] Zur Begründung führte es an, dass sich die Regelungen wegen des mit der Speicherpflicht verbundenen technischen und finanziellen Aufwands als rechtswidriger Eingriff in die unternehmerische Freiheit des dort antragstellenden Internetproviders erweisen würden.

Die Bundesnetzagentur hat diese Eilrechtsentscheidung zum Anlass genommen, keine Anordnungen oder sonstige Maßnahmen zur zwangsweisen Durchsetzung der Speicherverpflichtung gegen sämtliche Erbringer von Telekommunikationsdienstleistungen in den Fällen verletzter gesetzlicher Speicherpflichten zu ergreifen (vgl. § 149 TKG). Sämtliche Erbringer von Telekommunikationsleistungen sehen derzeit mit Blick auf diese Verwaltungspraxis der Bundesnetzagentur und mit Blick auf die Entscheidung des Oberverwaltungsgerichts von einer ihrer gesetzlichen Verpflichtung entsprechenden Speicherung ab. Dies auch, obgleich das *BVerfG* zeitlich nachfolgend eine

[8] Vgl. EuGH, Urt. v. 21. Dezember 2016 – C-203/15 u. C-698/15, NJW 2017, 717.
[9] BVerfG, Beschl. v. 26. März 2017 – 1 BvR 141/16, ZD 2017, 300.
[10] OVG Müster, Beschl. v- 22. Juni 2017 – 13 B 238/17, NVwZ-RR 2018, 43.

(weitere) Verfassungsbeschwerde gegen § 113b Abs. 1 TKG mit folgender Begründung nicht zur Entscheidung angenommen hat:

> „Es handelt sich um eine Berufsausübungsregelung, die – gestützt auf die Erwägung, dass die Daten in Blick auf die Anwendbarkeit der deutschen Regelungen und die Zuständigkeit deutscher Aufsichtsinstanzen im Inland gespeichert werden sollen – ungeachtet der unionsrechtlichen Harmonisierung des Datenschutzes einen legitimen Gemeinwohlzweck verfolgt und im Übrigen verhältnismäßig ist.“[11]

Auch auf eine richterliche Anordnung hin stehen den Strafverfolgungs- und Gefahrenabwehrbehörden mangels Erfüllung der gesetzlichen Speicherpflichten durch die Anbieter öffentlich zugänglicher Telekommunikationsdienste seitdem keine Verkehrsdaten über zurückliegende Telekommunikationsvorgänge als Erkenntnismittel zur Aufklärung von Straftaten oder zur – etwa polizeilichen – Gefahrenabwehr zur Verfügung.

III. Ausgangspunkte des Gesetzesentwurfs

Der Gesetzesentwurf knüpft den Vorschlag, die Neuregelung über die Verkehrsdatenspeicherung aufzuheben (Art. 1, 2, 3 und 6 des Gesetzesentwurfs), an einen doppelten Befund:

Zunächst habe der Gesetzgeber nach Ansicht des Entwurfs bei dem auch ihm obliegenden „Schutz der Bürger vor den Bedrohungen durch Kriminalität und Terrorismus“, die „Grenzen, die das Grundgesetz staatlichem Handeln zieht … mehrfach überschritten“, sodass die „verfassungs- und europarechtswidrige Vorratsdatenspeicherung“ abzuschaffen sei. Überdies sei es – die Vereinbarkeit der Vorratsdatenspeicherung mit dem Grundgesetz unterstellt – „verfassungspolitisch nicht klug“, die äußersten Grenzen des Verfassungsrechts… ohne überzeugende Gründe auszureizen.“[12]

IV. Stellungnahme zu beiden Ausgangspunkten

1. Vom Überschreiten verfassungsrechtlicher Grenzen

An dieser Stelle soll – aus strafrechtspraktischer Sicht – zur Frage der Verfassungswidrigkeit der geltenden Rechtslage nur auf folgende Umstände hingewiesen werden:

[11] BVerfG, Beschl. v. 28. September 2017 – 1 BvR 1560/17, BeckRS 2017, 129759.
[12] BT-Drucks. 19/204 S. 1.

a) Eine Entscheidung des *BVerfG* über die Vereinbarkeit der deutschen Neuregelungen aus dem Jahre 2015 mit dem Grundgesetz, aber auch mit europarechtlichen Maßgaben ist bisher nicht ergangen. Der Ausgang der anhängigen Verfassungsbeschwerdeverfahren ist derzeit nicht absehbar; sämtliche – freilich nur eine äußerst begrenzte verfassungsgerichtliche Prüfpflicht auslösende – Eilanträge blieben erfolglos. Auch kann der fachgerichtlichen Entscheidung eines Oberverwaltungsgerichts kein Fingerzeig auf den Ausgang der Verfassungsbeschwerdeverfahren entnommen werden. Dies gilt schon deshalb, weil sich die verwaltungsgerichtliche Fachentscheidung allein auf eine – vom *BVerfG* aber bereits in seinem Urteil vom 2. März 2010 (1 BvR 256/08) unter dem Aspekt der Berufsausübungsfreiheit (Art. 12 Abs. 1 GG) ohne durchgreifende verfassungsrechtliche Bedenken in den Blick genommene[13] – Beeinträchtigung der auch unionsrechtlich geschützten unternehmerischen Freiheit stützt und damit gerade nicht die erkennbar im Verfassungsbeschwerdeverfahren absehbar besonders bedeutsamen Fragen der Telekommunikationsfreiheit tragend berücksichtigt hat. Im Übrigen sei auf die allein dem Bundesverfassungsgericht als Verfassungsorgan zustehende Kompetenz zur Nichtigerkärung von Gesetzen hingewiesen (vgl. § 95 Abs. 3 BVerfGG).

b) Selbst wenn aber Teile der Neuregelung einer verfassungsgerichtlichen Überprüfung nicht standhalten sollten, so ist mit Blick auf die mit Augenmaß und streng orientiert an den Maßgaben der Entscheidung des *BVerfG* aus dem Jahre 2010 gefassten gesetzlichen Neuregelungen nicht abermals eine vollständige Nichtigerklärung der angegriffenen Vorschriften zu erwarten. Bereits im Jahre 2010 war diese Frage im 1. Senat nicht unumstritten.[14] Der Gesetzgeber würde in diesem Fall deshalb absehbar die Gelegenheit zu partiellen Nachbesserungen haben und wird auch weiterhin nicht pauschal von diesem Ermittlungsinstrument absehen müssen.

c) An der deshalb derzeit offenen verfassungsgerichtlichen Beurteilung ändert auch die zwischenzeitlich ergangene und vorstehend dargelegte Entscheidung des *EuGH* nichts. Zunächst wirkt sie nur inter partes; Regelungen deutschen Rechts waren nicht

[13] NJW 2010, 833, 850.
[14] Vgl. die abweichenden Voten der Richter *Schluckebier* und *Eichberger*, a.a.O., S. 855 f.

Gegenstand der entschiedenen Verfahren. Überdies unterscheiden sich die deutschen Regelungen über die Verkehrsdatenspeicherung von denen, die der Beurteilung durch den *EuGH* unterstellt waren. Hier sei insbesondere auf die verfahrensrechtlichen Absicherungen der „doppelten Tür", auf den uneingeschränkten Richtervorbehalt (vgl. § 101a Abs. 1 Satz 1 StPO), auf die Benachrichtigungspflichten sowie auf die spezifischen gerichtlichen Tenorierungspflichten hingewiesen. Aber auch in materieller Hinsicht unterscheidet sich die deutsche Rechtslage; so liegt nach geltendem Recht eine den schwedischen und britischen Regelungen vergleichbare flächendeckende und undifferenzierte Erhebung von Verkehrsdaten nicht vor. Nach geltendem Recht werden nämlich insbesondere Daten über den E-Mail-Verkehr der Nutzer nicht erhoben; weiterhin ist auf § 113b Abs. 6 TKG hinzuweisen, nach dem Anschlüsse von Personen, Behörden und Organisationen aus dem kirchlichen und sozialen Bereich ausgenommen sind.

2. „Ohne überzeugende Gründe"

Der zweite Begründungsansatz des Gesetzesentwurfs knüpft daran an, dass es an überzeugenden Gründen für das Ermittlungs- und Gefahrenabwehrinstrument der Verkehrsdatenspeicherung fehle. Abgehoben wird damit erkennbar auf die in der langen rechtspolitischen Diskussion regelmäßig vorgetragene Behauptung, dass die Verkehrsdatenspeicherung keinen oder jedenfalls keinen hinreichenden Nutzen habe, der ihren Aufwand gerade auch gemessen am Grundsatz der Verhältnismäßigkeit rechtfertigen könne. Dementsprechend war und ist immer wieder zu lesen, dass retrograd zu erhebenden Verkehrsdaten in der Praxis der Strafverfolgungsorgane keine oder allenfalls geringe praktische Bedeutung zukomme. Auch seien schwerste Straftaten durch dieses Instrument nicht zu verhindern.[15] Hierzu wird als Referenz immer wieder auch ein Gutachten des Max-Planck-Instituts aus dem Jahre 2011 herangezogen.[16]

---

[15] Vgl. nur etwa https://www.t-online.de/digital/sicherheit/id_74154630/vorratsdatenspeicherung-in-deutschland-das-sollten-sie-wissen.html Beitrag vom 18. Oktober 2015.

[16] Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg, 2. Aufl. 2011; vgl. zur berechtigten Kritik an Aussagekraft und Methodik des Gutachtens die Stellungnahme des Sachverständige Herrn Richter am Bundesgerichtshof Dr. Nikolaus *Berger* für die Anhörung im Ausschuss für Recht und Verbraucherschutz am Bundesgerichtshof Dr. Nikolaus *Berger* am 21. September 2015; abrufbar unter Bundestag.de.

Aus rechtspraktischer Sicht ist dieser Vermutung indes zu widersprechen. Die Verkehrsdaten sind als Ermittlungswerkzeug aus moderner und effektiver Kriminaltechnik und damit aus einer effektiven Verbrechensaufklärung nicht wegzudenken. Die nachstehende Darstellung soll daher zunächst beschreiben, welche Verkehrsdaten nach geltendem Recht durch die (privaten) Provider gespeichert und durch die Ermittlungsbehörden – allein auf richterliche Anordnung hin – von diesen abgefragt werden können (**a**). Sodann wird anhand von Beispielsfällen aus der Berufspraxis des *Verf.* die ermittlungstaktische Bedeutung der Verkehrsdaten für die Tataufklärung durch die Strafverfolgungsbehörden und für die Beweisführung der Strafgerichte beispielhaft dargestellt werden (**b**). Hierzu sollen die Sachverhalte und Tatvorwürfe mit groben Strichen skizziert und der Einsatz der Verkehrsdaten und seine Folgen für den Verfahrensausgang dargelegt werden. Die Darstellung erhebt freilich nicht den Anspruch einer umfassenden empirischen Untersuchung. Sie soll vielmehr anhand von konkreten Fällen aus der Praxis der Strafjustiz die Bedeutung von Verkehrsdaten für die Aufklärung schwerer Straftaten veranschaulichen.

a) Verkehrsdaten – Welche Informationen sind hiervon umfasst?

Klarstellend sei zunächst nochmals erwähnt, dass durch die Speicherung von Verkehrsdaten keine inhaltliche Aufzeichnung der Telekommunikation erfasst wird. Dies bringt nicht zuletzt § 113b Abs. 5 TKG zum Ausdruck. Eine inhaltliche Überwachung der Telekommunikation wird abschließend in §§ 100a, 100b StPO geregelt und ist nicht Gegenstand der Verkehrsdaten. Die Verkehrsdaten werden danach unterschieden, ob sie die Kennung, den Standort oder den Zeitpunkt der genutzten Geräte betreffen und ob hierbei das angerufene und anrufende Gerät von Relevanz sind.

aa) Kennung

In Hinblick auf die Kennung kann zwischen Festnetz- und Mobilfunkanschlüssen sowie der Nutzung des Internets unterschieden werden. Bei Festnetzanschlüssen wird die Rufnummer gespeichert. Bei Nutzung von Mobilfunkgeräten sind die internationale Kennung oder eine andere Kennung (IMSI – International Mobile Subscriber Identity) und die internationale Gerätekennung erfasst (IMEI – International Mobile Station Equipment Identity). Dies gilt auch für die Übermittlung von Kurznachrichten (SMS –

Short Message Service) und Multimedianachrichten (MMS – Multimedia Messaging Service). Für das Internet werden die Internetprotokoll-Adresse (IP-Adresse) sowie die jeweils zugewiesene Benutzerkennung erfasst.

bb) Standort

Die Standortdaten sind nur bei Mobilfunkgeräten (einschließlich Internet) und öffentlich zugänglichen Internetzugangsdiensten von Relevanz. Dabei sind die Funkzelle und die Funkantenne (Sendemast) erfasst. Eine Funkzelle ist der Bereich, in dem das von einer Sendeeinrichtung eines Mobilfunknetzes gesendete Signal empfangen und fehlerfrei decodiert werden kann (Cell-ID). Über die Abfrage der Funkzelle kann damit eine geographische Zuordnung des genutzten Gerätes erfolgen. Die Funkzellen sind unterschiedlich groß und werden auf Grundlage der von den Netzbetreibern zur Verfügung gestellten Daten durch die Ermittlungsbehörden vermessen. Für eine genauere Zuordnung ist die Auswertung des jeweiligen Funkmasts erforderlich.

cc) Zeitpunkt

Ferner sollen das Datum und die Uhrzeit der jeweiligen Zeitzone sowie Beginn und Ende der Verbindungen erhoben werden.

b) Einblick in die Ermittlungspraxis deutscher Strafverfolgungsbehörden

aa) Verfahrensbeispiele

Nachstehend werden Strafverfahren aus verschiedenen Deliktsbereichen und die jeweilige Bedeutung der Verkehrsdaten als Ermittlungsansatz und/oder als Beweistatsache für die Beweiswürdigung dargestellt. Es handelt sich nicht um systematisch erhobene oder ganz außergewöhnliche Fälle, sondern um alltägliche Strafverfahren, mit denen die Staatsanwaltschaften der Länder und die Landgerichte regelmäßig befasst sind. Zur Vermeidung von Wiederholungen nimmt der *Verf*. hier ergänzend Bezug auf die Stellungnahme des durch den Ausschuss für Recht und Verbraucherschutz im Zuge des Gesetzgebungsverfahrens zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten angehörten Sachverständigen Richter am Bundesgerichtshof Dr. Nikolaus *Berger* vom 21. September 2015.[17] Der Sachverständige

[17] Abrufbar unter Bundestag.de.

hat aus seiner Praxis am Bundesgerichtshof eine beeindruckende Vielzahl an Verfahren zusammengestellt, in denen Verkehrsdaten als Ermittlungsansatz oder aber als Beweismittel eine zentrale Rolle bei der Verbrechensaufklärung gespielt haben und/oder die deshalb ihre Bedeutung in besonderer Weise erhellen. Der *Verf*. war an der damals durchgeführten Erhebung auf Landesebene beteiligt.

Ergänzend hierzu an dieser Stelle nur beispielhaft Folgendes:

(1) Staatsschutzstrafrecht

Verfahrensgegenstand: Der Beschuldigte soll sich ab März 2014 dem sogenannten „Islamischen Staat“ angeschlossen haben. In der Folgezeit soll er durch ihn ausgebildet worden sein und an Kampfhandlungen der Vereinigung – auch etwa bewaffnet mit AK 47 oder Panzerfäusten – teilgenommen haben. Nach seiner Einreise in das Bundesgebiet und während des laufenden Asylverfahrens lebt er in Norddeutschland.

Beweisrechtliche Bedeutung von Verkehrsdaten: Nachdem sich gegen den Beschuldigten Anhaltspunkte im Sinne eines Anfangsverdachts (§ 152 StPO) für die Mitgliedschaft des Beschuldigten in einer ausländischen terroristischen Vereinigung (§ 129b StGB) ergeben hatten, ist – neben weiteren Abklärungen – für die Strafverfolgungsbehörden in diesem aktuell noch laufenden Ermittlungsverfahren von Bedeutung, zu wem der Beschuldigte gerade auch in der zurückliegenden Zeit über den auf ihn registrierten Anschluss Kontakte unterhält. Hieraus können sich Anhaltspunkte für die Aufklärung des Schuldgehalts ergeben, namentlich durch den Abgleich mit weiteren bereits vorliegenden Erkenntnissen zu möglichen Mitgliedern der Vereinigung sowie – etwa mit Blick auf einen naheliegenden Austausch von Bildmaterial untereinander – Anknüpfungspunkte für weitere Erkenntnisse über die Beteiligung an kämpferischen Aktivitäten der Vereinigung.

(2) Bandenkriminalität

Verfahrensgegenstand: Die Angeklagten sind rechtskräftig unter anderem wegen schweren Bandendiebstahls in mehreren Fällen (§ 244 Abs. 1 StGB) sowie wegen vorsätzlichen unerlaubten Ausübens der tatsächlichen Gewalt über eine Kriegswaffe zu mehrjährigen Gesamtfreiheitsstrafen verurteilt worden. Sie hatten sich zusammengeschlossen, um gewerbsmäßig und gemeinschaftlich 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.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die Überwachungskameras des geschädigten Betriebes zeichneten zwar das Tatgeschehen auf. Eine Täteridentifikation war anhand dessen aber wegen Maskierung der Täter nicht möglich. Erkennbar war auf dem Videofilm indes, 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 im Zusammenhang mit der 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 dieserart überführten Angeklagten gestanden in der Hauptverhandlung die Taten überwiegend. Einer Darstellung des Beweisergebnisses der Verkehrsdaten bedurfte es in den schriftlichen Urteilsgründen mit Blick auf diese Geständnisse nicht.

(3) Betäubungsmittelhandel

Verfahrensgegenstand: Die Angeklagten sind rechtskräftig u.a. wegen unerlaubten Handeltreibens mit Betäubungsmitteln in nicht geringer Menge in mehreren Fällen zu mehrjährigen Freiheitsstrafen verurteilt worden (§ 29a BtMG).[18] Sie erwarben gemeinschaftlich insgesamt etwa 150 kg Marihuana in den Niederlanden und verbrachten das Rauschmittel sodann zum Zwecke des gewinnbringenden Verkaufs nach Hamburg und verkauften es dort weiter. Dabei gingen sie arbeitsteilig vor: Drei Täter waren an den Beschaffungsfahrten in den Niederlanden beteiligt, während ein weiterer Täter

[18] Az. 6004 Js 232/10.

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 von Überwachungsmaßnahmen nach § 100a StPO einem konkreten Beschuldigten zugeordnet werden konnte, mit Hilfe von in den Niederlanden im 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 zugeschriebenen Mobilfunkanschlüsse ein Rückschluss auf ihre Abwesenheit vom Bundesgebiet möglich. Denn während der Zeiträume der vorgeworfenen Beschaffungsfahrten ließen sich keine Daten im deutschen Mobilfunknetz feststellen. Dies korrespondierte mit einer Abrede, die im Zuge der Gesprächsüberwachung – nach § 100a StPO – mitgeschnitten worden war. Hiernach war zwischen ihnen vereinbart worden, ihre Mobiltelefone während der Beschaffungsfahrten auszuschalten und in Hamburg zu belassen. Für frühere Zeiträume und dort naheliegend durchgeführte Beschaffungsfahrten konnte auf Verkehrsdaten der von den Angeklagten in Deutschland verwendeten Mobiltelefone nicht mehr zurückgegriffen werden. Der Nachweis der Fahrten erfolgte für zwei Beschuldigte insoweit anhand der Daten über die Anmietung von Kraftfahrzeugen. Einem weiteren Angeklagten, der in den anderen Fällen an der Beschaffung in den Niederlanden beteiligt gewesen war, konnte indes eine Fahrtbeteiligung nicht nachgewiesen werden. Eine Fahrzeuganmietung durch ihn erfolgte in diesem Fall nicht. Deutsche Verkehrsdaten, die eine Nutzung der diesem Beschuldigten durch Telekommunikationsüberwachung zugeordneten Mobilfunknummern und Rufnummern ermöglichen könnten, waren für diesen nicht mehr zu erlangen.

(4) Besonders schwerer Raub

Verfahrensgegenstand: Angeklagt war ein besonders schwerer Raub (§ 249 Abs. 1, § 250 Abs. 2 Nr. 1, § 25 Abs. 2 StGB).[19] Die Angeklagten sollen den Geschädigten aufgefordert haben, sein Mobiltelefon herauszugeben, und – als dieser sich weigerte – diesem sodann mit einer Flasche derart auf den Kopf geschlagen haben, dass der Geschädigte bewusstlos zu Boden stürzte. Anschließend sollen die Angeklagten ihm das Mobiltelefon entwendet und es noch am selben Tage veräußert haben.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die Angeklagten schwiegen im Ermittlungsverfahren. Der hinreichende Tatverdacht wurde gestützt auf die Aussage einer Zeugin, die das Mobiltelefon wenige Stunden später von den Angeklagten zum Kauf angeboten bekommen und es nach Erwerb noch in derselben Nacht verschenkt haben soll. Bei diesem beschenkten Zeugen konnte die Tatbeute schließlich im Rahmen einer Durchsuchung aufgefunden werden. Diese Zeugenaussage wurde bestätigt durch die Verkehrsdaten. Mit Hilfe der Gerätenummer (IMEI-Nummer) des gestohlenen Mobiltelefons konnte ermittelt werden, dass der beschenkte Zeuge das dem Geschädigten entwendete Mobiltelefon mit seiner eigenen SIM-Karte betrieben hatte.

(5) Besonders schwere räuberische Erpressung - „mobile.de“

Verfahrensgegenstand: Dem Angeklagten lag eine schwere räuberische Erpressung zur Last (§§ 253, 255, 250 Abs. 2 Nr. 1 StGB). Er soll ein Scheinangebot über den Verkauf eines Kraftfahrzeugs auf einer Internetplattform zum Preis von 40.000 Euro eingestellt, sich telefonisch mit einem Interessenten über den Verkauf geeinigt und sich mit diesem und dessen Lebensgefährtin verabredet haben. Am abgelegenen Treffpunkt soll der Angeklagte dem Käufer einen Revolver an den Kopf gehalten, Bargeld in Höhe von 40.000 Euro verlangt und für den Fall einer Weigerung mit dem Erschießen des Geschädigten sowie dessen Lebensgefährtin gedroht haben. Der Geschädigte soll sodann das Bargeld übergeben haben.

Beweisrechtliche Bedeutung von Verbindungsdaten: Noch am Tatabend eingeleitete Fahndungsmaßnahmen blieben erfolglos. Eine Identifizierung des Angeklagten

[19] Az. 3411 Js 497/14.

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 erhobenen Verkehrsdaten bestätigt. Denn anhand der Verkehrsdaten zu der vom Täter gegenüber dem Geschädigten angegebenen Rufnummer konnte ermittelt werden, wo sich der Nutzer vor der Tat aufgehalten hatte. Dies war überwiegend ein Bereich im Osten Hamburgs in der Nähe zur Wohnanschrift des Angeklagten, auf den die Zeugenhinweise abzielten.

(6) Schwerer Raub bei Widerstandsunfähiger

Verfahrensgegenstand: Die Anklage legte den Angeklagten einen gemeinschaftlich begangenen schweren Raub zur Last (§ 249 Abs. 1, § 250 Abs. 1 Nr. 1 b, § 25 Abs. 2, §§ 27, 52 StGB). Sie sollen auf Grundlage eines gemeinsamen Tatplans an der Tür der bettlägerigen älteren Zeugin geklingelt haben. Sodann soll einer der Täter nach Öffnen der Tür durch die Angestellte eines Pflegedienstes dieser eine Hand auf den Mund gedrückt haben, um diese am Schreien zu hindern, sie sodann in das Innere der Wohnung gedrängt und sie nach Bargeld befragt haben. Dann soll die Zeugin gefesselt und mit einem Handtuch geknebelt worden sein. Die Täter sollen mit Bargeld geflüchtet sein und die Geschädigte in gefesseltem Zustand zurückgelassen haben.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die schweigenden Angeklagten – die persönliche Kontakte zum Pflegedienst unterhielten – wurden erheblich belastet durch die Ergebnisse der Verkehrsdatenauswertung ihrer Mobiltelefone. Hiernach sollen zwischen ihnen insbesondere zur Tatzeit und unmittelbar danach mehrere Telefonate geführt worden sein. Überdies zeigte die Geovisualisierung der Verbindungsdaten – eine graphische Aufbereitung der verschiedenen Standorte von Funkzellen, in denen die Mobilfunkanschlüsse eingeloggt waren –, dass sich ein Angeklagter zur Tatzeit in unmittelbarer Nähe des Tatorts aufgehalten hat.

(7) Betrug – „Enkeltrick“

Verfahrensgegenstand: Der Angeklagte ist rechtskräftig wegen banden- und gewerbsmäßig begangener Betrugstaten in der Begehungsweise eines „Enkeltricks“ in mehreren Fällen verurteilt (§ 263 Abs. 1, Abs. 3 Nr. 1 und Abs. 5, §§ 25 Abs. 2, 53 StGB). Insgesamt hat die Bande auf diese Weise knapp 70.000 Euro erbeutet. Der

Angeklagte reiste jeweils aus seiner Heimat Litauen in das Bundesgebiet ein, um hier in Umsetzung des Tatplans die Bargelder in den Wohnungen der Geschädigten abzuholen.

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.

(8) Räuberische Erpressung

Verfahrensgegenstand: Der Angeklagte ist rechtskräftig u.a. wegen versuchter räuberischer Erpressung zu einer mehrjährigen Gesamtfreiheitsstrafe verurteilt worden.[20] Zugrunde lagen den Tatvorwürfen per SMS an die Tatopfer übermittelte Drohungen, wie etwa:

> *„Sie haben unsere wahrnung ignorirt.. Ich habe die freundligkeit ihnen mitteilen ich habe Geld bekomen, ihnen Hand und Ohr abschneiden. Sie haben zwei Wochen sich einigen wegen U. mit anwahlt. kein wort an polizei oder klug, sonst sofort kugel in kopf. Deine letzte chance , danach du nie wieder gesund dein geld ausgeben. Allah dich bestrafen, du ungläubiger.“*

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hat zunächst geschwiegen und sich später dahin eingelassen, dass jemand anderes diese Nachrichten versandt haben muss. Die Strafkammer sieht den Angeklagten – sachlichrechtlich durch den Bundesgerichtshof unbeanstandet – auf Grund folgender, maßgeblich auf die Verkehrsdaten gestützter beweiswürdigender Erwägungen als überführt an:

[20] Az. 6003 Js 21/13.

„(...) Der Angeklagte wird insbesondere belastet durch die ... Verbindungsdaten zu der Rufnummer 49176XXX, die mit dem Zeugen K. eingehend in der Hauptverhandlung erörtert wurden. 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 nebst Sicherstellungsverzeichnis und Lichtbild des Mobiltelefons sowie der Angaben des Zeugen K. bei der Durchsuchung des Wohnhauses des Angeklagten in der H.- Straße 15 in G..., am 7. Mai 2013 ... 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 4917XXX 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 N 53.5939, E 10.3903 des Providers O2, einem Funkturm im Bereich der Trittauer Heide östlich der Bundesstraße 404 und nördlich der Ortschaft K. Auch die russisch-sprachige Droh-SMS an den Zeugen Kh. wurde von dieser Funkzelle aus unter der Rufnummer 49176XXX versandt, eine IMEI-Nummer des für diese SMS verwendeten Endgerätes war insoweit zum Zeitpunkt der Verkehrsdatenabfrage nicht mehr gespeichert, da die IMEI vom Anbieter nach den vom Zeugen K. berichteten Ermittlungen (Auskunft der Firma Telefonica) bereits nach sieben Tagen gelöscht wurde. Diese Funkzelle deckt nach der Funkzellenausmessung des Landeskriminalamtes ... auch den Bereich H.Straße 15 in G.... im Übrigen weite Teile von G. und K...ab

Zur Tatzeit ... waren nach der mit dem Zeugen K. erörterten 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 N533706, E 102344, einem Funkturm in Trittau, 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 Trittau eingeloggt, teils in die Funkzelle des Providers Vodafone mit der Zellkennung LAC/Zell-ID 409/15001, einem Funkmast in Witzhave mit den

Koordinaten N53.565833, E10.339722, 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 Witzhave."

(9) Besonders schwerer Raub – Freispruch

Verfahrensgegenstand: Der Angeklagte ist rechtskräftig vom Vorwurf des besonders schweren Raubes freigesprochen worden (§ 249 Abs. 1, § 250 Abs. 2 StGB).[21]

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hat im Ermittlungsverfahren und vor der Strafkammer geschwiegen. Besondere Bedeutung kam in diesem „Indizienprozess" namentlich den erhobenen Verkehrsdaten betreffend den Mobilanschluss zu, von dem aus eine Pizzabestellung aufgegeben und mittels dessen der Lieferant in einen Hinterhalt gelockt worden war. Die Telefonnummer war als 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, den Eltern und Geschwistern, oder aber 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 indes nur dann tragfähig sein, wenn mit der notwendigen Gewissheit auszuschließen war, dass jemand anderes Zugriff auf den Anschluss hatte. Bis zum letzten Hauptverhandlungstag schien sich dies durch das Ergebnis der Beweisaufnahme zu bestätigen. Einem im Rahmen des Schlussvortrags des Verteidigers gestellten Beweisantrag betreffend den Standort des Tathandys drei Tage vor der 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-Harburg. In den Urteilsgründen hat die Strafkammer Folgendes ausgeführt:

[21] Az. 4181 Js 1/12.

„Trotz dieser teilweise gewichtigen Beweiszeichen vermochte die Strafkammer letzte Zweifel an der Täterschaft des Angeklagten nicht zu überwinden. Diese betrafen die Frage, ob der Angeklagte die Mobilfunknummer zur Tatzeit auch selbst genutzt hat.

Zwar lag es mit Blick auf den längeren vorangegangenen Zeitraum, in dem der Angeklagte den Anschluss ersichtlich für sich genutzt hat, nicht etwa nahe, dass er den Anschluss in der Tatnacht Dritten zur Verfügung gestellt hat oder ihn gänzlich aufgegeben haben sollte. Auch deuteten die Verbindungs- und Standortdaten vom Tattage nicht auf einen anderen Nutzer hin. Das bestimmende Gewicht des Beweiszeichens „Nutzung des Tat-Mobiltelefons" wurde aber für die Strafkammer dadurch in Frage gestellt, dass zumindest für den 25. Dezember 2011 und damit drei Tage vor der Tatbegehung ein Dritter den Mobilfunkanschluss verwendet haben muss. Mehrere Zeugen, darunter die S., hatten glaubhaft angegeben, dass der Angeklagte an jenem Abend jedenfalls ab 21 Uhr bei den Eheleuten S. in Hamburg Musik gemacht hätte. Zur selben Zeit war der Mobilfunkanschluss allerdings eingeloggt in einer Funkzelle in Tarp/Schleswig-Holstein. Damit war durch die Strafkammer in der gebotenen Gesamtschau zu berücksichtigen, dass ein Dritter zumindest drei Tage vor der Tat Zugang zu diesem Anschluss hatte.

Dies schwächte das Beweiszeichen in ganz empfindlicher Weise. Denn es konnte nunmehr nicht sicher ausgeschlossen werden, dass ein Dritter möglicherweise auch am Tatabend Zugang zu dem Mobilfunkanschluss hatte. Diese Schwäche des Beweiszeichens war ferner zu Lesen vor dem Hintergrund, dass der Anschluss am Abend unmittelbar vor der Tat zumindest auch in Eidelstedt eingeloggt war. Dort wohnte die Freundin des H., die Zeugin P. Überdies war zu bedenken, dass gerade der tatverdächtige H. engen Kontakt zur Familie des Angeklagten hatte und daher zahlreiche Verbindungen des Tathandys auch auf Telefonate durch ihn zurückzuführen sein könnten.

Die Strafkammer vermochte deshalb auch nach umfassender Beweisaufnahme und Gesamtschau der vorliegenden Beweiszeichen letzte bestimmende Zweifel an der Täterschaft des Angeklagten nicht zu überwinden."

b) Zusammenfassende Überlegungen

Die vorstehend dargestellten Verfahrensskizzen zeigen auf, dass die Verkehrsdaten teilweise zum unmittelbaren Tatnachweis dienten. In der überwiegenden Anzahl der Fälle waren sie aber – wie aus Sicht des *Verf.* rechtspraktisch in der überwiegenden Anzahl der Verfahren – ein Hebel für weitere wesentliche Ermittlungsschritte. Sie lieferten auch Hinweise auf weitere Personen, die im unmittelbaren zeitlichen und örtlichen Zusammenhang mit der Tat im Kontakt zum Verdächtigen standen und können dieserart Täterstrukturen aufzuklären helfen. Ferner vermögen sie Schlüsse auf die Anwesenheit von Verdächtigen an bestimmten Orten zu bestimmten Zeiten zu tragen und deren Reisewege – etwa bei unerlaubter Drogeneinfuhr oder Schleuserhandlungen – oder gar Rückschlüsse durch die jeweils von einer Telefonnummer geführten

Gespräche auf den Nutzer eines Anschlusses nachvollziehbar zu belegen; dies alles, ohne dass hierbei auf Gesprächsinhalte zugegriffen wird. Die Verfahrensskizzen belegen ferner, dass den hierdurch gewonnenen Erkenntnissen nicht ausschließlich belastende Wirkung zukommen muss. Gerade bei dem Rückschluss auf den Nutzer eines Tattelefons ist einem Angeklagten möglich durch Verkehrsdaten entlastender Umstände – etwa gar in Form einer Alibibehauptung – vorzubringen.

c) Verfahrensrelevanz aus der Sicht anderer Dienststellen

Über die vorstehend beschriebenen Verfahren aus dem Alltag der Ermittlungsbehörden hinaus gibt es zahlreiche Kriminalitätsbereiche, in denen Verkehrsdaten wegen spezifischer Tatbegehungsweisen eine besondere Bedeutung zukommt („Enkeltrick"; „Autobahnschütze", dessen Standorte jeweils anhand Verbindungsdaten aufgeklärt werden konnten).

Betreffend die besondere ermittlungstaktische Bedeutung von IP-Adressen hat sich erst jüngst der Präsident des Bundeskriminalamtes geäußert: Hiernach hätten im Jahre 2017 trotz 8.400 Hinweisen auf Kinderpornografie die Ermittlungen eingestellt werden müssen, weil eine retrograde Abfrage von IP-Adressen derzeit mangels tatsächlicher Speicherungen durch die Internetdienstleister nicht möglich sei.[22] Die Verkehrsdaten sind nach Einschätzung weiterer Fachdienststellen geeignet, eine Aufklärung etwa auch in der Pyramide der Täter nach oben hin zu ermöglichen. Insbesondere sei 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 möglich. Ferner wird mit Recht darauf hingewiesen, dass Verkehrsdaten gerade auch die Aufklärung von Tatserien erleichtern kann. So können etwa Kreuzvergleiche zwischen verschiedenen Funkzellen und unterschiedlichen Tatorten ergeben, dass jeweils dieselbe Nummer dort eingeloggt war. Gerade bei Serientaten dient deren Aufklärung nicht nur dem Strafverfolgungsinteresse, sondern sie beugt mit der Ermittlung und Verurteilung des Serientäters auch von ihm drohenden Wiederholungstaten vor.

[22] Pressemitteilung des BKA vom 6. Juni 2018.

Schließlich weist das BKA auch mit Recht darauf hin, dass – jenseits gefahrenabwehrrechtlicher Aspekte – die Strafverfolgung gerade auch terroristischer Straftaten, etwa solche von Mitgliedern des sog. „Islamischen Staats“, ohne Verkehrsdatenspeicherung deutlich erschwert oder gar unmöglich sei. Mit Hilfe dieser Daten können die Anrufziele der sich etwa in Syrien aufhaltenden Verdächtigen in Deutschland erhellt und hierdurch Erkenntnisse über die Strukturen und Beteiligtenkreise auch im Bundesgebiet gewonnen und namentlich die Urheber im Internet hochgeladener, verherrlichender Videos ermittelt werden.

V. Abschließende Bewertung

1. Die Verkehrsdatenspeicherung ist heute als Instrument zeitgemäßer strafrechtlicher Ermittlungen nicht wegzudenken und steht in ihrer kriminalistischen Bedeutung den Errungenschaften der Daktyloskopie gleich. Dies belegen neben Einblicken in die Strafrechtspraxis eindrucksvoll schon die seit langem festzustellenden exorbitanten Steigerungsraten hinsichtlich der Zahl der Telefonanschlüsse, vor allem aber auch der im Netz ausgetauschten Sprach- und Datenvolumina.[23] Das Kommunikationsverhalten der Menschen hat sich in den letzten Jahrzehnten grundlegend verändert;[24] damit geht erkennbar einher auch die Verwendung dieser Mittel für die Begehung schwerer und schwerster Straftaten sowie korrespondierend hiermit die Annahme eines erfolgversprechenden ermittlungstaktischen Anknüpfungspunkts für die Tataufklärung.

2. Die derzeit geltende Rechtslage stellt unter Beachtung bisheriger verfassungsgerichtlicher Maßgaben einen mit Augenmaß gestalteten Ausgleich zwischen der rechtsstaatlichen Pflicht auf eine zu gewährleistende effektive Strafverfolgung einerseits und einen streng begrenzten und strikten formellen Anforderungen unterworfenen Eingriff in die Freiheitsrechte der Bürger andererseits dar.

3. Die Verkehrsdaten werden nicht bei staatlichen Behörden gespeichert, sondern unter strengen Sicherheitsbedingungen bei privaten Telekommunikationsprovidern für die gesetzliche Höchstspeicherdauer vorgehalten. Entgegen einer weit verbreiteten

[23] Vgl. nur die Übersicht im Tätigkeitsbericht der Bundesnetzagentur aus dem Jahre 2016, S. 28.
[24] Vgl. bereits BT-Drucks. 16/5846, S. 38, 50 ff., 59.

Sorge ist allein mit der Speicherpflicht für die privaten Anbieter von Telekommunikationsdienstleistungen keine flächendeckende staatliche Überwachung aller Bürger verbunden.

4. Die kurzfristig gespeicherten Verkehrsdaten dürfen von den Strafverfolgungsbehörden nur zur Aufklärung schwerwiegender Straftaten und nur mit richterlicher Genehmigung abgerufen und verwendet werden. Die Hürden dafür sind ebenso hoch wie bei dem – freilich ungleich intensiveren – Eingriff durch eine Wohnraumüberwachung und damit sogar strenger als bei der – ebenfalls eingriffsintensiveren – Überwachung von Telefongesprächen.

5. Die derzeit ergebnisoffene verfassungsgerichtliche Bewertung sollte vor dem Hintergrund der ausdifferenzierten deutschen Regelungen abgewartet werden. Auch ist gerade mit Blick auf die Bedeutung des Ermittlungsinstruments sorgsam zu prüfen, ob und in welchem Umfang die Maßgaben der Rechtsprechung des *EuGH* Anlass zur einer – etwa teilweisen – Korrektur des geltenden Rechts geben. Eine dem vorgreifende – gar übereilte – vollständige Abschaffung des Ermittlungsinstruments wird der Verantwortung für eine effektive und verantwortungsvolle Strafrechtspflege nicht gerecht. Sie hat auch der *EuGH* nicht pauschal gefordert, sondern erkennbar weiterhin gesetzgeberischen Handlungsspielraum gesehen.

6. Eine Alternative zur Speicherung von Verkehrsdaten über einen begrenzten Zeitraum durch private Anbieter ist derzeit nicht ersichtlich. Bei einem Verzicht hierauf – auch unter Einführung eines vom Gesetzesentwurf indes nicht vorgesehenen sog. Quick-Freeze – hinge die erfolgreiche und öffentlich wahrnehmbare Verfolgung schwerster Straftaten von Zufälligkeiten, wie etwa der Sicherung und Auswertung von Tatortspuren, sowie von dem Umstand ab, welche Priorität die Ermittlungsbehörden dem jeweiligen Verfahren zuschreiben. Auch ist es etwa unvorhersehbar,

- wann eine Tat den Ermittlungsbehörden bekannt wird;
- wann eine Tat angezeigt wird;
- ob bei der Tatbegehung auch die Verwendung von Telekommunikationsdiensten bedeutsam war;
- welcher Telefonanschluss (Nummer, IMSI- oder IMEI-Nummer) hier von Bedeutung war.

Wird nach einer Vermisstenmeldung ein Tötungsdelikt zum Nachteil der vermisst gemeldeten Person erst Wochen später bekannt, so wäre deshalb bei fehlender Speicherpflicht von Verkehrsdaten dieser wichtige Ermittlungsansatz – namentlich die Feststellung anwesender Personen in der betreffenden Funkzelle – bei einem Kapitalverbrechen verloren.

7. Der Erforderlichkeit einer Verkehrsdatenspeicherung kann auch nicht entgegengehalten werden, dass sie zur Abwehr terroristischer Gewalttaten ungeeignet sei und dies durch bereits erfolgte Terroranschläge auch in Deutschland belegt werde. Freilich: Die strafprozessuale Abrufbefugnis von Verkehrsdaten kann einen Anschlag zwar nicht verhindern; dies schaffen andere repressive und eben nicht gefahrenabwehrrechtliche Ermittlungsinstrumente, wie etwa Wohnraumdurchsuchungen, jedoch ebenfalls nicht. Ermöglicht werden aber eine Aufhellung des Täterumfelds und der Täterbewegungen, ihrer Kontaktpersonen und Unterstützer sowie in diesem Umfang auch die Verhinderung von Wiederholungstaten. Indem Unterstützer ermittelt und strafrechtlich verfolgt werden, wird nicht nur generalpräventiv auch terroristischen Straftaten vorgebeugt, sondern effektiv gerade auch islamistischer Terrorismus durch das Strafrecht bekämpft.