Bund Deutscher Kriminalbeamter

Der Bundesvorsitzende

BDK Der Bundesvorsitzende | Poststraße 4 - 5 | D-10178 Berlin

Deutscher Bundestag
An die Vorsitzende des
Ausschusses für Recht und
Verbraucherschutz
Renate KÜNAST
11011 Berlin

Ihr/e Zeichen/Nachricht vom

Ihr/e Ansprechpartner/in
André Schulz
E-Mail
andre.schulz@bdk.de
Telefon
+49 (0) 30 24 630 45 - 0
Telefax
+49 (0) 30 24 630 45 29

Berlin, 08. Juni 2015

Stellungnahme des Bundes Deutscher Kriminalbeamter zur Öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Sehr geehrte Frau Vorsitzende,

nachfolgend nehmen wir zum o.a. Gesetzesentwurf Stellung.

Das Fazit vorab: Der BDK begrüßt den überfälligen Gesetzesentwurf, da die Erhebung von Telekommunikationsdaten einen ganz wesentlichen Baustein bei der Kriminalitätsbekämpfung und der Abwehr schwerster Straftaten darstellt. Wir haben Verständnis für die Sorgen und Ängste der Kritiker dieses Gesetzes. Gemessen an den tatsächlichen Erfordernissen einer effektiven Strafverfolgung greift der Gesetzesentwurf jedoch zu kurz. Er hat erhebliche Schwachstellen, bleibt in wesentlichen Teilen sogar noch hinter der heutigen Rechtslage zurück, geht zum Teil an der Praxis vorbei und bedarf aus unserer Sicht zwingend der Nachbesserung!

Wesentliche Datenerhebungen schließt das Gesetz ganz aus. Gerade der Katalog möglicher Straftaten, die eine entsprechende Datenerhebung rechtfertigen, greift viel zu kurz. Die Einführung des Straftatenkatalogs des § 100g Abs. 2 StPO-NEU steht im Widerspruch zu der Rechtsprechung des BVerfG, welches wiederholt das verfassungsrechtliche Gebot einer effektiven Strafverfolgung hervorgehoben, das Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesent-

lichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet hat (BVerfGE 129, 208 <260> m.w.N.). Im vorliegenden Gesetzentwurf ist jedoch zum Beispiel der sexuelle Missbrauch von Kindern und Vergewaltigung zum Beispiel explizit ausgenommen. Das bedeutet für die Praxis meiner Kolleginnen und Kollegen, dass wir die Täter eventuell anhand von Telekommunikationsspuren ermitteln könnten, die hierfür erforderlichen Daten aber nicht erheben dürfen. Das kann man gerade bei Sexualdelikten weder den Opfern, noch einem rechtschaffenen Mitbürger schlüssig erklären. Es ist gar nicht erforderlich eine abstrakte Terrorgefahr zu beschwören. Die Digitalisierung unseres Alltages hat längst dazu geführt, dass Telekommunikationsdaten heute auch bei sogenannter Alltagskriminalität wie dem Wohnungseinbruch oder bei Kfz-Diebstählen und bei Betrugstaten benötigt werden, in etlichen Fällen stellen sie sogar den einzigen Ermittlungsansatz dar.

Die Bundesregierung möchte mit dem neuen Gesetz explizit ein Erstellen von Bewegungs- und Persönlichkeitsprofilen auf Grundlage der erhobenen Daten verhindern. Kennzeichen der Bandenkriminalität, der Korruption und der Organisierten Kriminalität sind jedoch oftmals weit auseinanderliegende Tatorte und Tatzeiten sowie wechselnde Aufenthaltsorte im In- und Ausland. Dies erschwert das Erkennen von Tat-/Tat- und Tat-/Täterzusammenhängen. Oftmals werden derartige Straftaten als Einzeltaten betrachtet und Strukturen nicht erkannt. Gerade das Erstellen von Bewegungsbildern mit Hilfe von Telefondaten, ermöglicht eine solche Erkennbarkeit und ist somit Grundlage einer effektiven Verbrechensbekämpfung.

Berufsgeheimnisträger und zeugnisverweigerungsberechtigte Personen unterliegen - zu Recht - einem besonderen Schutz. Dieser Schutz wird aber bereits heute durch § 160 a StPO gewährleistet und würde auch durch eine Erhebung von Telekommunikationsdaten nicht gefährdet.

Der Gesetzentwurf orientiert sich an den gesetzlichen Grundlagen der akustischen Wohnraumüberwachung. Die Maßnahme der Vorratsdatenspeicherung ist jedoch bei Weitem nicht mit der Eingriffsintensität des „Großen Lauschangriffs" vergleichbar. Das Abhören des gesprochenen Wortes inklusive Übermittlung aller wie bei der Vorratsdatenspeicherung angelieferter (Geo-)Daten der Kommunikationsteilnehmer ist an geringere Voraussetzungen gebunden als zukünftig das Erheben noch nicht personifizierter Daten im Rahmen der Vorratsdatenspeicherung. Die Polizei darf also nach dem Willen der Bundesregierung künftig bei zahlreichen Delikten Gesprächsinhalte aufzeichnen, aber nicht wissen, wer vor vier Wochen mit wem telefoniert hat. Das ist eine Pervertierung des Grundrechtsschutzes.

Sowohl das Bundesverfassungsgericht als auch der Europäische Gerichtshof erklärten in ihren Urteilen richtigerweise, dass die Vorratsdatenspeicherung dem

Gemeinwohl diene und für die Bekämpfung schwerster Kriminalität und zur Gefahrenabwehr benötigt wird. Beide Gerichte zeigten zudem die Rahmenbedingungen für die verfassungsgemäße Einführung auf. Aber auch hier ist die grundsätzliche Diskussion noch nicht zu Ende geführt worden: Bei der Speicherung von Telekommunikationsverkehrsdaten muss speziell die Eingriffsqualität betrachtet werden. Hier sind deutliche Zweifel an der Qualifizierung der Speicherung als „besonders schwerer" Eingriff gegeben. Diese Zweifel begründen sich hauptsächlich darin, dass es der Auswertung der Daten in weiten Bereichen bereits – wie es auch aus der Rechtsprechung des Bundesverfassungsgerichts zur automatischen Auswertung großer Datenmengen deutlich wird – am über die bloße Speicherung hinausgehenden Eingriffscharakter fehlt.
Zudem muss man sich in der heutigen Lebenswirklichkeit fragen, ob beispielsweise die Rückführung von IP-Adressen zum Anschlussinhaber überhaupt den von den Speichergegnern heraufbeschworenen Eingriffscharakter hat. Die überwältigende Mehrheit der deutschen Internetnutzer geht über einen Router ins Internet, der von mindestens den Mitgliedern der Familie oder WG, wahrscheinlich auch in einem bestimmtem Rahmen von Freunden oder Bekannten mitgenutzt wird. Der Fall, dass eine IP-Adresse tatsächlich auf eine Person zurückzuführen ist, ist gerade im Bereich von IPv4 (das uns sicher noch 20 – 30 Jahre lang begleiten wird) die absolute Ausnahme. Eine IP-Adresse ist in der heute gelebten Praxis vielmehr mit einem Autokennzeichen oder einer Telefonnummer vergleichbar. Man kann zwar mit deren Hilfe den Vertragspartner ermitteln, das bedeutet aber ausdrücklich nicht, dass dieser auch gleichzeitig zum Tatverdächtigen wird. Die Anzahl der Geräte, mit denen eine einzelne IP-Adresse heute genutzt wird, dürfte im Schnitt im unteren zweistelligen Bereich liegen. Diese Zahl wird in Zukunft im Rahmen der „Smart Homes" noch deutlich steigen. Die Ermittlung der elektronischen Daten bildet somit nur das – zwingend notwendige – Grundgerüst für die Aufklärung von Straftaten und den Einstieg in weitere Ermittlungen.

Gerade anhand der sehr stark kritisierten Speicherung von IP-Adressen wird von den Gegnern gerne behauptet, dass die Gefahr der Erstellung von Bewegungsprofilen besteht. Bei nüchterner Betrachtung ist dies unter Einbeziehung des vorstehenden Gesetzentwurfes gerade **nicht** möglich. Die Erstellung von Profilen im Internet ist eine sehr wohl bestehende Gefahr, wenn man mehr Daten zur Verfügung hat als diejenigen, die gespeichert werden sollen. Es wird ja nachvollziehbar und sinnvoll auf die Erhebung derartiger Daten verzichtet, wie zum Beispiel die aufgerufenen Internetseiten oder die übertragenen Inhalte. Die Gefahr einer Profilerstellung ist mit den begrenzten aber deutlich spezifischeren Informationen, die ein Webseiten- oder Suchmaschinenbetreiber automatisch übertragen bekommt, wesentlich höher als mit den Daten, die im Rahmen der Verkehrsdatenspeicherung

konserviert werden. Dieser Aspekt soll ausdrücklich nicht kritisiert werden sondern dabei helfen, die Bewertung der tatsächlichen Eingriffstiefe der geplanten Speicherung zu objektivieren.

Jeder Kriminalist weiß, dass die Speicherung der Telekommunikationsdaten kein Allheilmittel ist, sondern nur einen Baustein in der Kriminalitätsbekämpfung darstellt. In Frankreich, wie in fast allen anderen europäischen Ländern, gibt es diese Speicherung. Die französische Polizei wertet derzeit immer noch die vorhandenen Telekommunikationsdaten nach den Anschlägen in Paris aus. Die Daten haben bereits jetzt dabei geholfen, die Tat- und die Täterstrukturen aufzuhellen und werden vermutlich weitere Mitwisser bzw. Tathelfer aufdecken. Die Daten helfen dabei, zukünftige Anschläge nach Möglichkeit verhindern zu können. Die Kriminalpolizei in Deutschland wäre nach einem Anschlag nicht in der Lage, festzustellen, mit wem der oder die Täter zwei Wochen vor der Tat kommuniziert hätten. Verbindungen und Netzwerke könnten deshalb nur schwer oder gar nicht erkannt und aufgedeckt werden.

Der BDK respektiert ausdrücklich die Kritik und Sorgen, die sich für einige aus der Vorratsdatenspeicherung ergeben. Was Kriminalpolizei und Staatsanwaltschaft keinesfalls wollen, ist das Ausspähen privater Daten nach Lust und Laune. Genau das will die Exekutive sogar verhindern. Das Vorliegen einer Straftat mit einem Verdacht im konkreten Einzelfall, die staatsanwaltschaftliche Überprüfung sowie der Richtervorbehalt, sind die Grundvoraussetzungen zur Nutzung der Telekommunikationsdaten zur Strafverfolgung.

Den Befürwortern der für die Strafverfolgung erforderlichen Speicherung von Verkehrsdaten geht es nicht darum, alle Bürgerinnen und Bürger unter Generalverdacht zu stellen. Es geht vielmehr darum, "flüchtige digitale Spuren" im Rahmen gezielter Strafverfolgung (bei konkreter Verdachtslage gegen eine oder mehrere Personen) zur Verfügung zu haben, ohne die Beschuldigte nicht beweiskräftig überführt werden können.

Nachfolgend beispielhaft einige Deliktsbereiche, in denen Verkehrsdaten zwingend erforderlich sind, um Tatverdächtige zu ermitteln und zu überführen sowie Strukturen der (Organisierten) Kriminalität überhaupt nachweisen zu können:

- **Phishing** - Ausspähen von Daten beim Onlinebanking
- **Skimming** - Ausspähen von Daten an Bankautomaten mit entsprechenden Vermögensschäden. Hier findet die weitere Tatausführung fast ausschließlich mittels Telekommunikation im weitesten Sinne statt.

- **Wohnungseinbruch** - Auch hier nutzen organisierte Banden Telekommunikationseinrichtungen zur Begehung von Einbrüchen sowie zur Verwertung der Beute
- **Verbreitung von Kinderpornografie**
- **Androhung von AMOK-Lagen und Bombendrohungen**
- **Enkeltrick und Schockanrufe** - Diese Betrugstaten zum Nachteil alter Menschen finden fast ausschließlich über Telekommunikation statt. Ohne Verkehrsdaten sind nur Einzelfälle (meist als Versuch) zwar nachweis- jedoch nicht gerichtsfest aufklärbar. Der Nachweis dieses als Organisierte Kriminalität definierten Bereichs von Straftaten ist ohne die Verkehrsdaten (Personenbezüge) nicht möglich.
- **Stalking** - Dieses Delikt lässt sich in den meisten Fällen überhaupt nur als solches qualifizieren, wenn der Zugriff auf rückwirkende Verkehrsdaten möglich ist.
- **Betrug/Warenkreditbetrug** unter Nutzung der Netze und Packstationen der Transportunternehmen
- **Wirtschaftskriminalität/Wirtschaftsspionage**
- **Korruption**
- **Hackerangriffe**
- **Internetkriminalität** wie z.B. Ausspähen von Daten und dessen Vorbereitung
- **Terrorismus**

Einige Beispiele aus der Praxis:

- Im Mordprozess von Horkheim (Baden-Württemberg) wurde der Täter vom Landgericht Heilbronn im März 2015 zu einer lebenslänglichen Freiheitsstrafe verurteilt. Der Täter hatte das Opfer mit 26 Messerstichen brutal getötet und dann einen Brand gelegt, um Spuren zu beseitigen. Erhobene Telekommunikationsdaten spielten bei der Tataufklärung eine ganz entscheidende Rolle.

- Der Vorfall stammt noch aus der Zeit, als die Daten zu Abrechnungszwecken gespeichert wurden: Eine verheiratete Frau hatte per Internet Kontakt zu einem ihr Unbekannten bekommen. Es entwickelte sich eine "Freundschaft", es wurde geflirtet und sie übersandte irgendwann Nacktfotos von sich. Der Täter loggte sich anschließend in ihren E-Mail-Account ein und versandte Mails mit den Fotos in ihrem Namen an alle ihre Freunde und die der Familie, darunter auch an etliche Arbeitskollegen ihres Mannes. In diesen Mails strebte sie angeblich eine "Karriere als Fotomodell und mehr" an. Neben der persönlichen Scham und dem Umstand, dass sie den Kontakt zu ihrem Freundeskreis weitgehend abbrach, hatte dies auch für ihren Mann erhebliche dienstliche Konsequenzen, denn er war Aufsichtsbeamter in einer JVA. Mittels Telekommunikationsdaten konnte der Täter ermittelt werden.

- Eine psychisch labile junge Frau erstattete Anzeige, weil sie immer wieder auf "StudiVZ" angegriffen wurde. Es war schnell klar, dass der Täter, oder wie sich dann herausstellte die Täterin, über Insider-Kenntnisse verfügte. Trotz intensivster Vernehmung konnte der Kreis derer, die von diesen intimen Dingen (Krankheitsverlauf, Schübe, familiäre Situation, Art und Weise der bisherigen Suizidversuche) wussten, nicht so weit eingegrenzt werden, dass ein Tatnachweis geführt werden konnte. Es blieb immer ein Kreis von 5 bis 6 Personen über. Die Täterin meldete sich immer wieder bei Studi-VZ unter neuem Namen an, attackierte die Geschädigte und meldete den Account wieder ab. In diesem Moment wurden sämtliche Daten bei StudiVZ wieder gelöscht. Diese Attacken waren sehr massiv, z.B. wurde ihr vorgeworfen, sie könne sich nicht einmal richtig umbringen, in einer anderen Nachricht wurde sie direkt zum Suizid aufgefordert, „das wäre ihre erste nützliche Tat im Leben“. Das Opfer fing daraufhin wieder an sich zu ritzen und war psychisch so angegriffen wie Jahre zuvor, sie musste sich wieder in Behandlung begeben. Die Tataufklärung gelang letztlich über die Website einer Diskothek, wo ein Foto vom Opfer hämisch kommentiert wurde. Anhand von erhobenen IP-Adressen konnte schließlich die Täterin ermittelt werden. Die IP-Adresse gehörte zu einer Universität. Da die Täterin Bewohnerin eines Studenten-Wohnheims war, war die IP ermittelbar. Die Täterin fühlte sich sicher und drohte der Polizei Strafanzeigen und Beschwerden an, da sie der Ansicht war, dass die Polizei nach dem Ende der VDS solche Daten gar nicht mehr zu Ermittlungszwecken erlangen könnte. Die überführte Täterin war die Freundin des Ex-Freundes des Opfers.

- 2013 wurde ein Umfangsverfahren gegen eine nigerianische Tätergruppe geführt. Modus operandi war das sogenannte "Voice-Phishing". Die Täter

spähten dabei per Mail die Zugangsdaten aus, generierten eine Überweisung und ließen eine rhetorisch geschulte muttersprachliche Deutsche bei den Opfern anrufen. Unter der Legende, der TAN-Generator müsste auf SEPA umgestellt werden, gab sie die "Umstell-Codes" durch und brachten die Opfer dazu, einen Betrag und die Zielkontonummer einzugeben und eine TAN zu übermitteln. Im Rahmen der Ermittlungen konnte die Gruppierung in Essen lokalisiert werden. Über ein Gespräch, das im Rahmen der Telefonüberwachung auflief, konnte ein Geschädigter vorgewarnt werden. Die betroffene Sparkasse stellte für den Zugriffstag eine Mitarbeiterin ab, die das Konto beobachtete. Der Polizei gelang es, eine IP-Adresse in dem Moment zu erheben, als die Täter sich ins Konto einloggten. Da es sich um eine laufende Session handelte, konnte der Provider den Inhaber herausgeben. Nach Session-Beendigung wäre dies nicht mehr möglich gewesen.

- Die StA Deggendorf (Az. 4 VRs 4720/97) lässt aktuell nach einem flüchtigen Sexualstraftäter, der seit 17.04.2015 aus einer Psychiatrischen Klinik abgängig ist, mit internationalem Haftbefehl suchen. Die Fahndung führte auch nach BW. Hier konnte am 15.05.2015 in Erfahrung gebracht werden, dass der Flüchtige sich telefonisch bei seiner Mutter auf dem Festnetztelefon am 10.05.2015 (Muttertag) gemeldet hatte. Sofortige Ermittlungen ergaben, dass keine Daten vorhanden sind, da diese nur 3 Tage gespeichert werden.

- Vermutlich aus dem polnischen Posen (Zentrum der Enkeltrickbetrügerbanden) heraus wurden in Braunschweig mehrere Hunderte ältere Menschen angerufen und bei ihnen versucht den Eindruck zu erwecken, dass ein Angehöriger in Not am Telefon sei. In einem Fall aus dem März 2015 wurde ein über 80jähriger Mann von den Tätern überredet, zur Bank zu gehen und dort 15.000 € abzuheben, um sie seinem vermeintlichen Angehörigen zu übergeben. Hier passte allerdings die Hausbank des alten Herrn auf und unterrichtete die Angehörigen, die sich dann nach einigen Tagen an die Kripo Braunschweig wendete. Im Rahmen des Ermittlungsverfahrens wurde versucht, die bei dem Opfer eingehenden Telefonate nachzuvollziehen, was aber aufgrund der nicht vorhandenen Verbindungsdaten scheiterte. In einem weiteren Fall im April 2014 wurden tatsächlich an die unbekannten Täter 8000 € übergeben. Spätere Versuche, über die Telefonverbindung an die Tätergruppe zu gelangen, verliefen negativ, da keine Daten mehr vorhanden waren.

- Bei den Ermittlungen des Arbeitsbereich Internetrecherche (AIR) beim LKA Baden-Württemberg im Jahr 2013 konnten bei 64 der 297 in Deutschland initiierten Fälle (22 %) die Ermittlungen gegen deutsche Tatverdächtige nicht weitergeführt werden, da Bestandsdatenanfragen an die Provider negativ beauskunftet wurden. Das bedeutet, dass keine Daten gespeichert waren, selbst in den Fällen, in denen der Täter zum Moment der Bestandsdatenabfrage noch im Internet online war. In einzelnen Operationen in den vergangenen Jahren lag der Anteil der Fälle, die aufgrund fehlender Datenspeicherung nicht mehr verfolgt werden konnten, bei jeweils über 50 %. Im Ergebnis bleibt festzustellen, dass die Verbreitung kinderpornografischer Dateien im Bereich der Netzwerke und damit auch die Beendigung von laufenden Missbrauchshandlungen ohne Vorratsdatenspeicherung derzeit nur unzureichend verfolgt werden kann (vergleiche auch: www.polizei-bw.de/Dienststellen/LKA/Documents/2013_Cybercrime_Digitale_Spuren.pdf).

- Verfahren aus der Zeit der Vorratsdatenspeicherung: Nur durch die bei den einzelnen Taten ermittelten Verbindungsdaten ergaben sich bei einer bundesweiten Serie von Betrugstaten durch aus dem Ausland agierende Anruferin Tatzusammenhänge und die vollständige Beweislage. Die in Einzelverfahren bei 44 verschiedenen Staatsanwaltschaften geführten Ermittlungsverfahren konnten mit den jeweils erhobenen Daten bei der StA Köln zusammengeführt werden (StA Köln 107 Js 19/09). Aus dem Gesamtbild der erhobenen Daten konnten die Aktivitäten der Haupttäterin für ca. 1,5 Jahre nachvollzogen werden, 34 vollendete Taten und mehrere Hundert Versuche geklärt und ein europäischer Haftbefehl erwirkt werden. Gesamtbeute nachweislich 231.000,- Euro, tatsächliche Beute geschätzt ca. 1 Millionen Euro. Telefonüberwachungsmaßnahmen waren zur Tatklärung nicht erforderlich, sondern wurden nur durchgeführt, um den Aufenthaltsort der Täterin zu ermitteln, die dann in den Niederlanden festgenommen und ausgeliefert wurde. Aufgrund der erdrückenden Beweislage der Telekommunikationsdaten legte die Täterin ein umfassendes Geständnis ab. Das gesamte Täternetzwerk konnte so nachvollzogen werden.

In zahlreichen Mordfällen, bandenmäßig begangenen Wohnungseinbrüchen, bewaffneten Raubüberfällen und Sexualdelikten, die auch mediale Aufmerksamkeit erfuhren, führte die Auswertung retrograder Telekommunikationsdaten zur Aufklärung und Überführung des Täters. Einige davon nachfolgend auszugsweise zum Nachlesen:

- http://www.spiegel.de/panorama/justiz/chefermittler-ingo-thiel-handy-daten-fuehrten-zu-mircos-moerder-a-866189.html
- http://www.suedkurier.de/region/hochrhein/bonndorf/Richtige-Spur-per-Handy;art372589,5578379
- http://www.nordbayern.de/region/nuernberg/lotto-mord-handy-daten-fuhrten-zu-den-angeklagten-1.2582472
- http://www.merkur-online.de/lokales/muenchen/stadt-muenchen/mordfall-poschinger-handy-zeigt-taeters-996878.html
- http://www.derdetmolder.de/?p=82761
- http://www.westfalen-blatt.de/OWL/Lokales/Kreis-Lippe/Leopoldshoehe/1881630-Mordkommission-sucht-weiterhin-Zeugen-Toedliche-Schuesse-Mann-aus-Lage-festgenommen

Die Aufzählung ist natürlich bei weitem nicht abschließend und könnte aus kriminalpolizeilichen und justiziellen Kreisen seitenlang (auch mit konkreten Aktenzeichen) fortgeführt werden.

Die praktische Arbeit hat gezeigt, dass die vorgesehenen Fristen für IP-Adressen und Verbindungsdaten zu Telefongesprächen erheblich zu kurz sein werden. Eine Speicherfrist von 3 bis 6 Monaten ist hier mindestens erforderlich (Vergleiche auch: www.bka.de/nn_234028/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/120130StatistischeDatenerhebungMindestspeicherungsfristenAbschlussbericht.html).

Weitere Defizite des Gesetzesentwurfes und Problemfelder:

Fehlen des Ortes der Internetnutzung
Gerade im Zusammenhang mit Festnetzanschlüssen ist es für die weiteren Ermittlungen zwingend erforderlich, den Ort der Nutzung zu kennen. Bei vielen Internetprovidern (außer bei Kabelanbietern) können die dem Kunden zugewiesenen Zugangsdaten bundesweit im gesamten Netzwerk des Providers genutzt werden. Ein Täter kann sich also mit seinen oder erbeuteten Zugangsdaten sowohl in München, als auch in Hamburg oder Berlin in das Netz einwählen und das Internet von dort aus nutzen. Unter anderem für die Planung und Durchführung von Folgemaßnahmen ist die Kenntnis des genauen Orts der Internetnutzung zwingend erforderlich.

Im Ergebnis sollte noch ein zusätzlicher Punkt in den neu zu definierenden § 113 b TKG aufgenommen werden, der die Zugangsprovider zum Speichern des Einwahlorts verpflichtet. Der Einwahlort ist dem Provider grundsätzlich bekannt, so dass sich der Aufwand darauf beschränken würde, ein zusätzliches Datum zu sichern.

Fehlen des § 176 StGB

In der Liste der Straftaten, die eine Abfrage der nach dem geplanten § 113 b TKG gespeicherten Daten ermöglichen, fehlt der § 176 StGB („Sexueller Missbrauch von Kindern"). Damit wird es in einem Fall, in dem ein Erwachsener ein Kind per Online-Chat dazu bringt, sich vor laufender Webcam auszuziehen und an seinen Geschlechtsteilen zu manipulieren **nicht** möglich sein, auf die gespeicherten Daten zurückzugreifen, um den Täter zu identifizieren, obwohl unter § 176 Abs. 4 Nr. 4 eigens die Begehung derartiger Straftaten unter Nutzung von Telekommunikationsmitteln definiert wurde. Einerseits wird diese Begehungsart explizit und gezielt unter Strafe gestellt, auf der anderen Seite fehlt dann aber die konsequenterweise notwendige Ermittlungskompetenz. Das gleiche gilt für den Fall, wenn ein Erwachsener sein Kind vor laufender Webcam „anbietet" und seinerseits an dessen Geschlechtsteilen herummanipuliert. Erst mit vollendeter Penetration (o.ä.) tritt hier der vom Gesetzentwurf geforderte schwere Fall ein, der die Ermittlung des Inhabers einer IP-Adresse legitimiert.
Es ist einem rechtschaffen denkenden und gesetzestreuen Bürger kaum zu vermitteln, dass es erst eines besonders schweren Falls des sexuellen Missbrauchs eines Kinds bedarf um beispielsweise den Nutzer einer IP-Adresse ermitteln zu dürfen und dass gerade die Taten unter Nutzung von Kommunikationsmitteln nicht unter die Befugnis fallen sollen. Deshalb muss der Straftatenkatalog auf den § 176 StGB, der den „einfachen" sexuellen Missbrauch von Kindern unter Strafe stellt, erweitert werden.

Beschränkung auf § 177 Abs. 2 Satz 2 Nr. 2 StGB

Gleichermaßen unverständlich erscheint die Tatsache, dass im Bereich der Vergewaltigungshandlungen ausschließlich die Vergewaltigung durch Gruppentäter - die in Deutschland zum Glück in der polizeilichen Praxis keine allzu große Rolle spielt - die Möglichkeit eröffnen soll, auf die im Rahmen der Höchstspeicherfrist konservierten Daten zuzugreifen. Eine Vergewaltigung durch einen Einzeltäter in einem weitläufigen Park soll demzufolge den Datenzugriff **nicht** ermöglichen, wobei in derartigen Fällen beispielsweise durch Auswertung der Funkzellendaten die Aufklärung der Straftat unter Umständen erst ermöglicht oder zumindest erheblich erleichtert werden könnte. Dies gilt insbesondere dann, wenn aufgrund der geografischen und netztopologischen Gegebenheiten zu erwarten ist, dass zu dem Zeit-

punkt eine eher überschaubare Anzahl an Nutzern in die konkrete Funkzelle eingebucht sein dürfte. Es ist somit erforderlich, den gesamten § 177 StGB im Straftatenkatalog aufzunehmen.

Fehlen des Erpressungstatbestandes
Erpressung begegnet den mit Internetdelikten befassten Ermittlern heute in vielfältiger Hinsicht. Drei Beispiele seien hier exemplarisch erwähnt:

1. Ransomware-Trojaner: der Computer wird nach angeblichem Fund von „Kinderpornografie" von der „Polizei" gesperrt und der Besitzer soll erst wieder Zugriff auf seine Daten bekommen, wenn er dem oder den Tätern Geldzahlungen zukommen lässt. Teilweise werden die persönlichen Daten verschlüsselt und so dem Zugriff des rechtmäßigen Nutzers entzogen.

2. Drohung mit dDoS-Angriffen: der oder die Täter drohen dem Inhaber eines Onlineshops damit, seine Server durch einen gezielten Überlastungsangriff zu stören und so zu verhindern, dass seine Kunden bei ihm einkaufen können. Es handelt sich dabei um die neue Variante der klassischen Schutzgelderpressung.

3. Sex-Chat-Erpressung: vorwiegend männliche Chater werden durch eine Chatpartnerin geschickt dazu gebracht, sich vor der Webcam zu entblößen und sich selbst zu befriedigen. Nach Vollendung eröffnet die angebliche Chatpartnerin dem Geschädigten, dass sie den Ablauf per Webcam mitgefilmt hat und droht damit, das Video an die Facebook-Freunde des Geschädigten zu verteilen, wenn dieser nicht einen Geldbetrag zahlt.

Alle drei Varianten sind heute keine Ausnahmen mehr sondern polizeilicher Alltag. In keinem der genannten Fälle wäre ein Zugriff auf die gespeicherten Daten möglich, da „einfache" Fälle der Erpressung nicht im Straftatenkatalog erfasst sind. Entsprechend muss der Katalog auf Erpressungstatbestände, mindestens aber auf solche, die unter Nutzung von Telekommunikationsmitteln begangen wurden, erweitert werden.

Beschränkung auf „besonders schwere" und „Bandendelikte"
Die polizeilichen Ermittlungen bringen es mit sich, dass man am Beginn eines Ermittlungsverfahrens in der Regel noch keinerlei zuverlässige Aussage zu den Tätern oder deren Hintergründen machen kann. Diese Informationen ergeben sich zwangsläufig erst im Rahmen der eigentlichen Ermittlungen, wenn sich die gewonnenen Erkenntnisse mit der Zeit zu einem Gesamtbild zusammenfügen. Insofern ist die Beschränkung des Datenzugriffs - und damit die Begrenzung der Ermittlungsmöglichkeiten auf „besonders schwere Fälle" und Bandendelikte - nicht

zielführend, da man in sehr vielen Fällen aufgrund fehlender Befugnisse gar nicht bis zu der Stelle kommen wird, an der man erkennt, ob es sich überhaupt um ein Bandendelikt handelt. Die Ermittlungen würden in vielen Fällen vielmehr vor dem Ausschöpfen der vorhandenen Möglichkeiten an eine Grenze stoßen und beendet werden müssen.

Keine Erfassung anderer relevanter Delikte

Im geplanten Katalog des neu gefassten § 100g Abs. 2 StPO ist kein einziger Korruptions- oder Betrugstatbestand enthalten (Betrug und Computerbetrug). Die polizeiliche Praxis zeigt, dass die Hemmschwelle potentieller Täter sinkt, wenn gleichzeitig die Gefahr, erwischt zu werden, erkennbar verringert ist. Dies zeigt sich unter anderem darin, dass immer mehr Betrugshandlungen unter Nutzung von Telekommunikationseinrichtungen (Internet/Telefon) begangen werden. Gerade in diesen Zusammenhängen sind bei derartigen Delikten in sehr vielen Fällen IP-Adressen und andere rein virtuelle Spuren die einzigen halbwegs verlässlichen Daten (Versand der Ware erfolgt beispielsweise an Packstationen oder Fakeadressen, so dass darauf kaum Ermittlungen aufgebaut werden können). Die Attraktivität derartiger Betrugshandlungen wird dadurch noch gesteigert, dass der Täter sich unter den geplanten Voraussetzungen keinerlei Gedanken bezüglich der Anonymisierung seiner Internetnutzung machen muss, da diese bereits durch die fehlenden Ermittlungsmöglichkeiten quasi „staatlich garantiert" ist.

Die Entwicklung hin zur Telekommunikation als Tatmittel zeigt sich auch in anderen Deliktsbereichen, wie beispielsweise beim Stalking („Nachstellung" gem. § 238 StGB). Die Tathandlungen bei der Nachstellung greifen wie kaum ein anderes Delikt in die private Lebensgestaltung ein, Opfer derartiger Taten werden nicht selten hochgradig traumatisiert. In Extremfällen kann dies bis zum Suizid des Opfers führen, das keinen anderen Ausweg mehr sieht. Die nähere Vergangenheit zeigt, dass Internet und Telekommunikationsmittel bei diesen Delikten fast ausschließlich als Tatmittel verwendet werden. Leider garantiert hier gerade die Nutzung von Mobilfunktechnik ein für den Täter höchst erfreuliches Maß an Anonymität.

Unverständlich erscheint deshalb, warum gerade bei den Delikten, die unter Nutzung von Telekommunikationsmitteln begangen werden oder die gegen Datenverarbeitungsanlagen gerichtet sind, nicht mit Hilfe des Zugriffs auf die gespeicherten Daten ermittelt werden darf. Speziell diese Taten sind in der Regel dadurch gekennzeichnet, dass meist ausschließlich technische Spuren in Form von IP-Adressen o.a. gesichert werden können. Andere Spuren sind bei derartigen Delikten selten bzw. oftmals überhaupt nicht verfügbar oder vorhanden. Nach dem

derzeitigen Entwurf dürften die tatrelevanten IP-Adressen jedoch nicht mittels der gespeicherten Daten ausermittelt werden.

Deshalb muss zwingend der Straftatenkatalog auf solche Delikte ausgeweitet werden, die unter Nutzung von Internet oder Telekommunikationsmitteln begangen wurden. Es erscheint nicht nur fair sondern geradezu rechtsstaatlich erforderlich, zwischen Strafverfolgung und Täter mehr oder weniger eine Art von Waffengleichheit herzustellen. Ein Täter, der seine Tat unter Ausnutzung der scheinbaren Anonymität im virtuellen Raum begeht, soll wissen, dass die Strafverfolgung adäquate Möglichkeiten hat, in diesem Bereich zu ermitteln.

Ständige Zunahme der Nutzung von verfälschten Telefonnummern

Die Anzahl der Delikte, die telefonisch unter Nutzung gefälschter Rufnummern begangen werden, steigt ständig. Hierbei werden beliebige Rufnummern - bevorzugt solche von Behörden - beim Angerufenen angezeigt. Hintergrund ist die außerordentlich einfache Möglichkeit, beliebige Rufnummern als angebliche Anrufernummer zu verwenden. Diese in der eigenen Telefonanlage, auf der Webseite des Telefonproviders oder einfach in einer Smartphone-App eingetragene Rufnummer wird anschließend ohne weitere Prüfung von den am Telefongespräch beteiligten Providern bis zum Angerufenen weitergereicht. In Unkenntnis der einfachen Fälschbarkeit wird die angezeigte Rufnummer von den meisten Bürgern als Fakt hingenommen und nicht hinterfragt. Gängige Praxis sind betrügerische Anrufe von „Amtsgerichten", „Staatsanwaltschaften" oder der „Polizei", wobei die angezeigten (falschen) Rufnummern mit der Betrüger-Legende korrespondieren. In einem hier dokumentierten Fall wurde bei einem Opfer gar die Rufnummer „110" bei einem Gespräch mit einem angeblichen Polizisten angezeigt.
Eine Lösung des Problems wäre hier sehr schnell und ohne großen Aufwand möglich: Sollte es sich um ein Gespräch handeln, das von einem nicht verifizierten Ursprung ausgeht (z.B. VoIP-Provider oder außerdeutscher Provider), so könnte man diesen Umstand durch Hinzufügen eines entsprechenden Hinweises im Display kommunizieren, indem man beispielsweise seitens des Providers des Angerufenen ein oder mehrere Fragezeichen vor der eigentlichen Rufnummer einfügt.
Die Anzeige von

??? 0931 457 0

würde in diesem Beispiel signalisieren, dass es sich um eine nicht überprüfte Anrufernummer handelt, der mit entsprechender Vorsicht zu begegnen ist. Diese Neuerung ließe sich auch in der Bevölkerung recht einfach ohne großen Aufwand kommunizieren.

Fehlen von E-Mail-Metadaten
Bei der Bewertung des vorliegenden Entwurfs stellt man fest, dass auf die Speicherung von E-Mail-Metadaten komplett verzichtet werden soll. Es wäre aber erforderlich, dass E-Mailprovider zumindest dazu verpflichtet werden, die Identifizierung eines Mailabsenders aufgrund von Message-ID und Zeitstempel zu ermöglichen.

Fazit
Es besteht noch erheblicher Nachbesserungsbedarf am Gesetzesentwurf! Seitens der Politik müssen die Sicherheitsbehörden hinsichtlich der rechtlichen Möglichkeiten sowie der personellen und materiellen Ressourcen in die Lage versetzt werden, alles Menschenmögliche für die Sicherheit der Bürgerinnen und Bürger in Deutschland unternehmen zu können. Opfer und Geschädigte haben ein Grundrecht auf Sicherheit, Schutz und Aufklärung von Straftaten. Es gibt derzeit zur Vorratsdatenspeicherung keine Alternativen, die einen geringschwelligeren Grundrechtseingriff darstellen würden. Zur kriminalistischen Beweisführung sowie zum Nachweis und zur Aufhellung von Tat- und Täterstrukturen und damit auch zur Abwehr von terroristischer Bedrohung führt derzeit kein Weg an der Vorratsdatenspeicherung vorbei. Wir müssen in Deutschland endlich die teilweise hysterisch geführte Diskussion beenden, im 21. Jahrhundert ankommen und dürfen uns nicht hinter Ideologien und kolportierten Halbwahrheiten sogenannter Netzaktivisten verstecken. Hier ermutige ich Sie zu einer breiteren Debatte, an der sich der Bund Deutscher Kriminalbeamter gern beteiligt. Wir brauchen endlich eine gesamtgesellschaftliche Diskussion über den Datenschutz in Deutschland, der sich an der Praxis einer digitalisierten Gesellschaft orientiert.

Der BDK steht Ihnen für weitere Ausführungen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

André Schulz
Bundesvorsitzender