DEUTSCHER BUNDESTAG

AUSSCHUSS FÜR RECHT UND VERBRAUCHERSCHUTZ

ÖFFENTLICHE ANHÖRUNG

ZUM

ENTWURF EINES GESETZES ZUR EINFÜHRUNG EINER SPEICHERPFLICHT UND EINER HÖCHSTSPEICHERFRIST FÜR VERKEHRSDATEN

STELLUNGNAHME

FRANK THIEDE

KRIMINALDIREKTOR

LEITER DER BERATUNGSSTELLE FÜR POLIZEIPRAKTISCHE RECHTSFRAGEN UND RECHTSPOLITIK, BUNDESKRIMINALAMT WIESBADEN

ORT:	BERLIN PAUL-LÖBE-HAUS RAUM 4.900
ZEIT:	21.09. 2015 16:00 UHR

1. Grundsätzliches zum polizeifachlichen Bedarf der anlassbezogenen Verwendung und Bedeutung von Verkehrsdaten

Bei der 2008 in Kraft getretenen (und 2010 vom BVerfG für nichtig erklärten) Regelung der sog. Vorratsdatenspeicherung in §§ 113a ff. TKG und der Befugnis ihrer Abfrage nach § 100g StPO und (2009 in Kraft getretenen Regelung des) § 20m BKAG i.V.m. § 4a BKAG ist dem Fachbereich KI 15 des Bundeskriminalamtes, in dem die Rechtstatsachensammel- und Auswertestelle (RETASAST) zur Bündelung des polizeifachlichen gesetzlichen Änderungsbedarfs geführt wird - von Polizeien des Bundes und der Länder der erkannte gesetzgeberische Regelungsbedarf berichtet worden. Während der polizeifachliche Bedarf der Auskunft über Telekommunikationsverkehrsdaten für eine effektive Ermittlungsarbeit im Bereich der Gefahrenabwehr wie Strafverfolgung unstreitig sein dürfte, war ein zunehmender Verlust von Verkehrsdaten bei zugleich heterogener Speicherpraxis der Betreiber festzustellen, da bei einer Vielzahl unterschiedlichster Geschäftsmodelle eine Speicherung der Daten durch den Betreiber „zu Abrechungszwecken“ nicht erforderlich und damit ggf. auch nicht zulässig wurde. Ohne eine einheitliche Verpflichtung der Betreiber war festzustellen, dass die Daten entweder nicht mehr vorhanden waren oder es vom Zufall abhing, bei welchem Anbieter die Zielperson ihren Vertrag mit welchem Geschäftsmodell geschlossen hat.

Besonders eklatant zeigte sich schon frühzeitig das Defizit bei Auskunftsersuchen zu einer dynamischen IP-Adresse, um anhand der IP mit Zeitstempel den konkreten Nutzer/Anschlussinhaber beim Betreiber zu ermitteln: Auskunftsersuchen nach §§ 161, 163 StPO i.V.m. § 113 TKG, später 2013 aufgrund der Gesetzesänderung nach dem dann einschlägigen § 100j StPO i.V.m. § 113 TKG, gingen und gehen wieder ohne Vorratsdatenspeicherung in den meisten Fällen ins Leere, da der Betreiber intern eine Zuordnung zu einem Anschluss zu einem bestimmten Zeitpunkt gar nicht (mehr) vornehmen konnte und kann, da die Verbindungsdaten – etwa mangels Abrechnungsinteresse – nicht mehr gespeichert waren/sind. Gerade bei IP-Adressen zeigt sich heute wie damals, dass ohne Zuordnung zu einem Anschluss oftmals schon der erste und meist einzige Ermittlungsansatz fehlt.

Dieser defizitäre Zustand vor 2008 wurde mit der Einführung der o.g. Regelungen zunächst geheilt, fiel dann aber mit der Entscheidung des BVerfG 2010 auf den alten Zustand zurück

und verschärfte sich dabei zusätzlich, da etwa Flatrate-Angebote mittlerweile fast „Standard“ geworden waren.

Umso wichtiger war es für die deutsche Polizei, den Gesetzgeber im Interesse einer möglichst zeitnahen wie verfassungskonformen Regelung der Vorratsdatenspeicherung zu beraten und ihm Rechtstatsachen zur Verfügung zu stellen. Das hat das Bundeskriminalamt gemeinsam mit den Polizeien von Bund und Ländern umgehend nach der Entscheidung des BVerfG 2010 zu einer bislang einzigartigen wie umfangreichen Erhebung veranlasst. Die 2011/2012 abgeschlossene Erhebung der Rechtstatsachensammel- und Auswertestelle (RETASAST) des BKA in Sachen Mindestspeicherfristen enthält die Darstellung der Ermittlungsdefizite ohne Mindestspeicherfristen nach dem BVerfG-Urteil vom 02.03.2010. Auf den auf der Homepage des BKA (FAQ zum Stichwort „Mindestspeicherfristen“ mit weiteren Erläuterungen) eingestellten Abschlussbericht und Falldarstellungen wird hingewiesen.

Kernaussagen:

- Im Rahmen der BKA Erhebung vom 02.03.2010 bis 26.04.2011 wurden insgesamt Auskunftsersuchen zu 5.082 Anschlüssen gestellt, wovon 84% nicht beauskunftet wurden.
- 83% der nicht beauskunfteten „Negativ“-Fälle erfolgten zur Strafverfolgung in den Bereichen (Computer- und Subventions-) Betrug (45%) und Kinderpornographie (39%).
- 90% der Auskunftsersuchen lediglich zu einer jeweils bereits vorliegenden IP-Adresse (also gerichtet auf die Auskunft über die hinter der IP mit Zeitstempel stehenden Kunden-/Bestandsdaten) wurden in den Bereichen KiPo und Betrug gestellt.
- In 9% der Fälle wurden retrograd Verkehrsdaten angefragt, v.a. Fälle schwerster Kriminalität. Im Bereich der Strafverfolgung konnte in den Fällen einer Nicht-Auskunft die zu Grunde liegende Straftat in 83% der Fälle nicht aufgeklärt werden.
- Die IP ist in fast allen Fällen immer der erste und einzige Ermittlungsansatz.

Das Bundeskriminalamt sieht seine Rolle im Rahmen der Expertenanhörung des Ausschusses primär in der Darlegung des polizeifachlichen Bedarfs der Regelungen. Die dringende Notwendigkeit, die Beauskunftung von retrograd gespeicherten Verkehrsdaten zu

ermöglichen, wird zudem durch die bei den Ländern, der Bundespolizei und im BKA erhobenen und im anliegenden Fallarchiv zusammengetragenen Rechtstatsachen belegt.

2. Anmerkungen zum vorliegenden Gesetzentwurf:

Ohne an dieser Stelle auf alle Vorschriften des Gesetzentwurfs einzugehen, können aus Sicht des Bundeskriminalamtes zusammenfassen zuvörderst folgende Bewertungen aus polizeifachlicher Sicht vorgenommen werden:

Feststellung Inhaber IP-Adresse

IP-Adresse ist im Bereich Cybercrime häufig der erste und erfolgversprechendste Ermittlungsansatz, um den hinter der vorliegenden IP mit Zeitstempel den Anschlussinhaber zu ermitteln, dem die IP im angegebenen Zeitfenster vom Provider zugewiesen worden. Um diese Zuordnung vornehmen zu können, muss der Provider denknotwendig auf die gespeicherten Verkehrsdaten intern zurückgreifen. Ist das mangels Speicherpflicht nicht möglich, scheitern in der Regel jegliche weiteren Ermittlungen.

Beispiel 1: ***Amok-Drohung***

Wegen eines anonymen Hinweises auf einen möglichen Amoklauf in Hessen wurde in einem Internet-Forum tatsächlich die Ankündigung eines Amoklaufs an einer bestimmten Schule festgestellt. Über die IP zum Eintrag konnte der Provider festgestellt werden. Erste Ermittlungen zur Person des Absenders verliefen jedoch negativ, da der Provider keine retrograden Verbindungsdaten mehr speichert.

Die Person des Absenders/Täters konnte später nur zufällig durch Recherchen über seinen Nickname festgestellt werden, da der Täter in einem anderen Forum mit demselben Nickname angemeldet war und dabei Bruchstücke seines Namens und der Adresse angegeben hatte. Der Täter wurde festgenommen, war geständig und wurde in eine psychiatrische Klinik eingewiesen.

Beim Täter wurde ein hohes Maß an tatsächlicher Amok-Bereitschaft festgestellt. Ort und Datum des Amok-Laufs waren bereits festgelegt. Der Täter hatte bereits erfolglos versucht, sich eine "scharfe" Schusswaffe zu verschaffen. Wegen der fehlenden Verkehrsdaten konnte die Gefahr erst zu einem späteren Zeitpunkt beseitigt und die Tat nur wesentlich erschwert aufgeklärt werden.

Beispiel 2: ***Ermittlungen im Darknet zu Kinderpornographie***

Im Juli 2013 wurde in einer konzertierten Aktion eine der zentralen Plattformen zur Verbreitung von Kinderpornographie abgeschaltet. Auf der Plattform waren insgesamt 2 Millionen kinderpornographische Bilder. Mit Abschalten der Plattform wurden die Online-Aktivitäten von ca. 25.000 Pädophilen unterbrochen, die Szene konnte deutlich verunsichert werden.

Insgesamt wurden 60 europäische IP-Adressen identifiziert, darunter 15 Nutzer mit deutschen IP-Adressen. Zu 13 Adressen konnten Bestandsdaten erhoben und die Nutzer identifiziert werden, in den beiden anderen Fällen waren trotz sofortiger Anfrage bei den entsprechenden Providern aufgrund fehlender Mindestspeicherfristen keine Daten mehr verfügbar.

Das bedeutet im Ergebnis: Trotz aufwendiger Sondervereinbarungen mit unseren internationalen Partnern FBI und Europol, die deutsche IP-Adressen sofort übermittelt haben – alle anderen an der Operation beteiligten Länder erhielten die IP-Adressen ihrer Länder am Ende der Operation gesammelt – und trotz der sofortigen Bearbeitung der Daten (in 24/7 Schichtdiensten), konnte in diesen beiden Fällen die IP-Adresse keinem Nutzer, keiner real existierenden Person zugeordnet werden.

Über die Sichtung der verschiedenen Boards der Plattform nach deren Abschaltung (retrograd) konnten ca. 200 weitere mutmaßlich deutsche Nutzer festgestellt werden. Zu diesen Usern liegen lediglich Nick-Name und E-Mail-Adressen, keine IP-Adressen vor. Eine Identifizierung ist so nur in wenigen Ausnahmefällen möglich.

- Die im Gesetzentwurf vorgesehene Speicherpflicht – wenn auch nur für 10 Wochen – vermeidet immerhin, dass die Ermittlungen, wie der Bericht des BKA belegt, in vielen Fällen andernfalls scheitern würden.

Funkzellenauswertung

Die Erhebung eingeloggter Mobiltelefone in bestimmter Funkzelle zu bestimmten Zeitpunkt (Ort-Zeit-Datum) ist für die Polizeiarbeit von zentraler Bedeutung, um etwa bei Tatserien Kreuztreffer zu ermitteln und so Ermittlungsansätze erst zu generieren oder bereits identifizierten Tätern/Tatverdächtigen die Tat nachzuweisen.

Beispiel 3: ***Autobahnschütze***

Über 760-mal schoss der Täter deutschlandweit aus seinem Lkw auf Transporter, Pkws und Gebäude. Eine Pkw-Fahrerin wurde schwer verletzt; Lkw-Fahrer hatten schlicht Glück, wenn das Geschoss das Seitenfenster durchschlug und um Haaresbreite den Kopf verfehlte. Tatorte waren überwiegend Autobahnen deutschlandweit.

Die Mobilfunkdaten des Verdächtigen haben wir mit den Funkzellen mutmaßlicher Tatörtlichkeiten und Tatzeiten auf Hunderten von Kilometern deutscher Autobahnen abgeglichen. Dadurch verdichtete sich der Verdacht zum Beweis. Wir konnten weitestgehend Übereinstimmungen mit den relevanten Tatstrecken und Tatzeiten feststellen. Dieser Abgleich mit Verkehrsdaten aus Funkzellen war besonders wichtig, weil wir außerhalb von Autobahnen keine Kennzeichenlesegeräte aufstellen konnten. Insbesondere bei den außerhalb von Autobahnen abgegebenen Schüssen konnten nun örtliche Bezüge auch zu diesen Tatorten hergestellt werden.

Beispiel 4: ***Enkeltrick***

Zunehmend geraten auch ältere Menschen in das Visier von Kriminellen. Ein Beispiel ist der sog. Enkeltrick, bei dem die Täter vorher ausfindig gemachte ältere Menschen anrufen und ihnen vorgaukeln, in einem verwandtschaftlichen Verhältnis zu stehen und dringend Geld zu benötigen. Diese Form des gewerbsmäßigen Betrugs hat häufig schwerwiegende finanzielle, seelische und gesundheitliche Folgen für die Opfer. Um die Täter ermitteln zu können, ist es nötig zu wissen, wer das Opfer von wo aus angerufen hat, wer vom Täter zur Geldabholung

beauftragt wurde und wer das Geld wo abgeholt hat. Hierzu sind Verkehrsdaten als Ermittlungsansatz zwingend erforderlich.

- Explizite Regelungen der Erhebung von Funkzellendaten im Gesetzentwurf der Bundesregierung zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten finden sich in §§ 100g Abs. 3, 101a Abs. 1 S. 2 StPO-E.

  § 100g StPO-E differenziert in Abs. 1 und Abs. 2 grundsätzlich zwischen dem Zugriff auf Daten gem. § 96 TKG (Daten, welche die TK-Unternehmen zu geschäftlichen Zwecken zu speichern befugt sind) und dem Zugriff auf die sogenannten Vorratsdaten, die nach § 113b TKG-E verpflichtend zu speichern sind. Für letztere finden sich in § 100g Abs. 2 StPO-E weitaus strengere Voraussetzungen der Datenerhebung, insbesondere muss ein Anfangsverdacht bezüglich einer besonders schweren Straftat aus dem angeführten Straftatenkatalog vorliegen.

  Auch § 100g Abs. 3 StPO-E, der explizite Regelungen zur Funkzellenabfrage enthält, knüpft an diese Differenzierung an. Je nachdem ob Daten gem. § 96 TKG oder solche nach § 113b TKG-E erhoben werden sollen, gelten unterschiedliche Voraussetzungen:

- Die Frist von vier Wochen zur retrograden Erhebung von auf Vorrat gespeicherten Daten liegt deutlich unter den Erwartungen des Bundeskriminalamts. Ob und ggf. wie schwer sich das Defizit für die polizeiliche Praxis auswirkt, wird sich in Zukunft erweisen.

  Ferner kommt künftig eine Anfrage – ungeachtet der kurzen Frist – bei einigen Straftatbeständen, bei denen ein Rückgriff auf Standort- oder (ohne Abrechnungszweck gespeicherte) Funkzellendaten wesentlich ist, schon in Ermangelung der Qualifikation gem. § 100g Abs.2 StPO nicht in Betracht, etwa bei (noch nicht) qualifizierten Fällen des Wohnungs-Einbruchsdiebstahls oder des Computerbetrugs. Sollten sich in der Praxis die befürchteten Defizite zeigen, werden wir berichten.

Retrograde Telekommunikationsdaten

Der Rückgriff auf Verkehrsdaten ist im Zuständigkeitsbereich des BKA etwa zur Erhellung von Netzwerkstrukturen im Bereich Terrorismus und Organisierte Kriminalität elementar. Die Verbindungen von Personen zu kennen, ist auch wichtig, um effektive Gefahrenabwehr zur Verhütung von Straftaten des internationalen Terrorismus (§ 4a BKAG) zu betreiben.

Beispiel 5: ***NSU***

Wegen fehlender Verbindungsdaten bis heute nicht klar, ob alle Kontakte und Verbindungen des Trios bekannt sind, wie der NSU die begangenen Verbrechen logistisch organisierte und ob es weitere Unterstützer oder weitere Zellen gab und gibt, die Anschläge planen.

In 1 658 Fällen wurden Verkehrsdaten bei Providern angefragt. Nur in 113 Fällen (7%) waren bei den Providern noch Daten vorhanden und konnten übermittelt werden.

- Auffällig ist im Gesetzentwurf, dass bei anschlussbezogenen Standortdaten ein Rückgriff auf diese Daten – ungeachtet ihres „Status“ als Abrechnungs- oder Vorratsdaten – nur in einem Zeitraum von vier Wochen und zugleich bei Vorliegen der Voraussetzungen einer Katalogtat nach § 100g Abs.2 StPO-E zulässig ist. Das Bundeskriminalamt wird aufmerksam beobachten, ob und ggf. wie sich Defizite in der polizeilichen Praxis auswirken.

  Dabei weist das Bundeskriminalamt vorsorglich noch einmal darauf hin, dass die von den Polizeien von Bund und Ländern in der o.g. Erhebung für notwendig erachtete gesetzliche Speicherfrist von sechs Monaten (auch für Standortdaten) nicht etwa übermäßig war, sondern vielmehr folgendem Umstand Rechnung trägt: Die polizeiliche Reaktionszeit (vom Eingang der Information bis zur Antragstellung beim Provider) hat nur einen geringen Einfluss auf die erforderliche Mindestspeicherfrist, denn nicht die polizeiliche Reaktionszeit, sondern das „Alter“ der Verkehrsdaten bestimmt den Speicherzeitraum (Beispiel: Spätes Bekanntwerden der Straftat oder lange Dauer der Datenträgerauswertung). Polizei und StA haben meist keinen Einfluss

darauf, wie schnell sie durch Anzeige oder von anderen (ausländischen) Stellen von einem Sachverhalt erfahren und somit Verkehrsdaten anfragen können. D.h. an der polizeilichen Reaktionszeit liegt es nicht: Zwischen dem Zeitpunkt der Kenntniserlangung des BKA über das Vorliegen ermittlungsrelevanter Verkehrsdaten und dem Moment der Stellung des Auskunftsersuchens lagen ausweislich der statistischen Erhebung des BKA in 86% der der Fälle, in denen keine Auskunft erteilt werden konnte, höchstens sieben Tage.

Annex: Einführung eines neuen Straftatbestands der „Datenhehlerei“ im Gesetzentwurf

Die geltende Rechtslage gem. StGB enthält keine Rechtsvorschrift, in der explizit die Strafbarkeit des Weiterverkaufs unerlaubt erlangter Daten unter Strafe gestellt wird. Die Justizministerkonferenz hatte am 13./14.06.2012 die Initiative der Einführung des Straftatbestandes der Datenhehlerei beschlossen. Der bereits seit 2013 vorliegende Gesetzentwurf des Landes Hessen, der sich inhaltlich mit den Forderungen des BKA im Wesentlichen deckt, wurde mit Bundesratsbeschluss vom 14.30.2014 erneut in den Bundestag eingebracht. Inhaltlich sieht dieser Entwurf

- neben der Einführung des Straftatbestands der Datenhehlerei (§ 202d StGB-E)
- auch eine Erhöhung des Strafrahmens des Ausspähens und Abfangens von Daten (§§ 202a, 202b StGB-E)
- Qualifikationstatbestände für Fälle des gewerbs- oder bandenmäßigen Handelns
- eine Versuchsstrafbarkeit

vor.

Für Fälle der gewerbs- oder bandenmäßigen Begehung sollte aus Sicht des BKA zudem das Recht der Telekommunikationsüberwachung in der StPO angepasst werden.