Stellungnahme zum Bürgerrechtestärkungs-Gesetz – BuStärG unter dem Aspekt der geplanten Abschaffung der Vorratsdatenspeicherung

Für die Anhörungssitzung des Ausschusses für Recht und Verbraucherschutz vom 13. Juni 2018

Die Vorratsdatenspeicherung ist ein heiß umstrittenes Thema. Entsprechend viele Änderungen mit Einfluss auf die Strafverfolgung hat es in den letzten Jahren gegeben.

Die **Richtlinie 2006/24/EG** über die **Vorratsdatenspeicherung** vom 15. März 2006**,** mit der alle EU-Mitgliedstaaten zur Einführung einer Vorratsdatenspeicherung von sechs Monaten bis zwei Jahren verpflichtet wurden, setzte Deutschland mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21.12.2007 um. Die Strafverfolgungsbehörden konnten über §100 g StPO Zugriff auf die Daten nehmen.

Bei der ersten Vorratsdatenspeicherung wurde noch nicht zwischen Daten, die der Diensteanbieter zur Leistungserbringung nach § 96 TKG speichern darf und solchen, die er zum Zwecke der Strafverfolgung nach § 113b TKG (damals: § 113a TKG) speichern muss, unterschieden.

Das **Bundesverfassungsgericht** beschloss im Wege der einstweiligen Anordnung vom **11.3.*2008*** (1 BvR 256/08) bis zur Entscheidung in der Hauptsache die nur eingeschränkte Anwendung, nämlich nur bei besonders schweren Straftaten.

Das B**undesverfassungsgericht** entschied am **2.3.2010** (BVerfGE 125, 260), dass die §§ 113a, 113b TKG in der Fassung vom 21.12.2007 und § 100g StPO, soweit danach Verkehrsdaten erhoben werden dürfen – sechsmonatige anlasslose Speicherung – gegen Art. 10 GG, das Brief-, Post- und Fernmeldegeheimnis, verstoßen. Eine maximal sechsmonatige Speicherung sei aber nicht von vornherein unzulässig. Es seien im Rahmen der Verhältnismäßigkeit die Datensicherheit, der Umfang der Datenverwendung sowie Transparenz und Rechtsschutz zu beachten. Voraussetzung für den Abruf von Daten zu Zwecken der Strafverfolgung sei ein abschließender Kreis der umfassten Tatbestände, dass die Straftat im Einzelfall schwer wiege und die Datenverwendung verhältnismäßig sei.

In seiner Entscheidung vom **8.4.2014**, C-293/12, C-594/12 (EuGH NJW 2014, 2169) hat der **Europäische Gerichtshof** die Ungültigkeit der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung, die eine Speicherungsfrist von 6 Monaten bis 2 Jahren vorsah, festgestellt. Denn es gebe keine Einschränkung auf das zur Erreichung des Zieles (öffentliche Sicherheit und Terrorismusbekämpfung) absolut Notwendige. Der Entscheidung liegt keine grundsätzliche Absage an die Vorratsdatenspeicherung zugrunde.

Daraufhin kam es zum **Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherfrist von Verkehrsdaten vom 10.12.2015**. In § 100g StPO wurden Katalogtaten für Verkehrsdaten nach § 113b TKG, also Vorratsdaten, eingeführt. Verbindungsdaten nach § 113 b Abs. 1 und 2 TKG, z.B. Rufnummer, Datum und Uhrzeit, Internetprotokoll-Adressen und Anschluss- und Benutzerkennungen sollen 10 Wochen und Standortdaten nach § 114b Abs. 4 TKG, sog. Funkzellendaten, vier Wochen gespeichert werden. Der Anbieter kann aber Standortdaten zu Abrechnungszwecken bis zu sechs Monate speichern, § 97 Abs. 3 TKG.

Das **Bundesverfassungsgericht** hat am **8.6.2016** (1 BvQ 42/15 u. 1 BvR 229/16) den Erlass einstweiliger Anordnungen bezüglich des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.10.2015 und §§ 100g, 101a, 100b StPO abgelehnt. Es entstehe kein schwerwiegender und irreparabler Nachteil durch die Datenspeicherung. Das BVerfG dürfe von seiner Befugnis, den Vollzug eines in Kraft getretenen Gesetzes auszusetzen, nur mit größter

Zurückhaltung Gebrauch machen, da der Erlass einer solchen einstweiligen Anordnung stets ein erheblicher Eingriff in die Gestaltungsfreiheit des Gesetzgebers sei.

Der **Europäische Gerichtshof** hat auf die Vorlage von Großbritannien und Schweden mit Urteil vom **21.12.2016** (C-203/15 und C-698/15) entschieden, dass die von der Richtlinie 2002/58/EG vom 12.7.2002 in der geänderten Fassung der Richtlinie 2009/136/EG vom 25.11.2009 vorgesehene anlasslose Vorratsdatenspeicherung nicht mit den Europäischen Grundrechten vereinbar ist. Eine Verwendung von Vorratsdaten sei nur zur Bekämpfung schwerer Straftaten legitim. Das europäische Recht stehe einer nationalen Regelung entgegen, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsehe. Es steht einer nationalen Regelung entgegen, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder einer unabhängigen Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden im Gebiet der Union auf Vorrat zu speichern sind.

Eine Speicherung sei möglich, sofern die dabei erhobenen Daten in Europa verbleiben und zuvor eine richterliche Genehmigung eingeholt werde.

Das **OVG Münster** hat am **22.6.2017** – 13 B 238/17 -beschlossen, dass die Speicherungspflicht nach § 113a Abs. 1 i.V.m. § 113b Abs. 1 und 3 TKG insgesamt mit Unionsrecht nicht vereinbar sei und das IT-Unternehmen jedenfalls in seiner durch Art. 16 der Charta der Grundrecht der Europäischen Union geschützten unternehmerischen Freiheit verletzt und hat festgestellt, dass bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens des VG Köln keine Speicherpflicht bestehe.

Bis zum 29.7.2017 wurden Verkehrsdaten nach § 100g Abs. 1 StPO a.F. i.V.m. § 12 StPOEG und § 96 Abs .1 S. 1 Nr. 1 TKG sowohl für Straftaten von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat (= Katalog für Taten, für welche eine Telefonüberwachung beantragt werden kann), als auch für eine mittels Telekommunikation begangene Straftat eingeholt, wenn sie für die Erforschung oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich waren. Bei einer Maßnahme mittels Telekommunikation musste die Maßnahme zu o.g. Zwecken überdies auf andere Weise aussichtslos sein, und die Erhebung der Daten muss in einem angemessenen Verhältnis zur Bedeutung der Sache stehen.

Ab dem 30.7.2017 erfolgt eine Differenzierung wie folgt:

Nach § 100g Abs. 1 StPO können Verkehrsdaten und Standortdaten für die Zukunft oder in Echtzeit nur bei einer mittels Telekommunikation begangenen Straftat eingeholt werden.

Nach § 100g Abs. 2 StPO ist die Einholung von Verkehrsdaten nach § 113b TKG (= Vorratsdaten) möglich

- bei Standortdaten für die Zukunft oder in Echtzeit bei einer Straftat von auch im Einzelfall erheblicher Bedeutung
- bei allen Standortdaten für die Vergangenheit bei besonders schweren Taten = Katalogtaten.

Weiter müssen die Verkehrsdaten zur Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein. Die

Erhebung der Daten muss in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Die Tat muss im Einzelfall schwer wiegen.

Nach § 100g Abs. 3 StPO können Funkzellendaten nur bei besonders schweren Taten = Katalogtaten abgefragt werden. Überdies muss es sich um eine Straftat von auch im Einzelfall erheblicher Bedeutung handeln. Die Erhebung der Daten muss in angemessenem Verhältnis zur Bedeutung der Sache stehen. Die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten wäre auf andere Weise wesentlich erschwert oder aussichtslos. Hinsichtlich Vorratsdaten nach § 113b TKG gelten dieselben Voraussetzungen wie bei § 100g Abs. 2 StPO.

Nach § 113b Abs. 6 TKG dürfen Daten zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, nicht gespeichert werden. Bei weiteren Berufsgeheimnisträgern wie Rechtsanwalt oder Verteidiger greift das Verbot der Erhebung nach § 100 g Abs. 4 StPO.

Wie kommt es zu der unterschiedlichen Handhabung?

Bis zum 29.7.2017 konnten Staatsanwaltschaft und Gerichte sich auf die **Übergangsnorm des § 12 StPOEG** berufen. Zwar gab es das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10.12.2015, gültig ab dem 18.12.2015. Die Speicherverpflichtung galt nach § 150 Abs. 13 TKG aber erst spätestens ab dem 1.7.2017. Da es mangels Speicherfrist noch keine gespeicherten Daten gab, konnte vorübergehend auf Verkehrsdaten nach § 96 Abs. 1 TKG zurückgegriffen werden.

Seitdem diese Übergangsregelung ausgelaufen ist, gibt es z.B. keine retrograden Verbindungsdaten mehr für

- Geldfälschung, § 146 StGB
- Sexuellen Missbrauch von Kindern ohne Eindringen in den Körper, § 176 StGB
- Vergewaltigung durch Alleintäter, § 177 Abs. 6 S. 2 Nr. 2 StGB
- einfachen oder besonders schweren Diebstahl („Einbruch“), §§ 242, 243 StGB
- Raub, § 249 StGB
- Erpressung, § 253 StGB
- Betrug oder Computerbetrug, § 263 (a) StGB
- Urkundenfälschung, § 267 StGB.

Es kommt zu einem Auseinanderfallen von Katalogtaten nach § 100a StPO (Telefonüberwachung) und § 100g StPO (retrograde Standortdaten). Letztere sollen nämlich die Erstellung eines Bewegungsprofils ermöglichen. Anders als bei der Telefonüberwachung gibt es nach § 101a Abs. 1 StPO auch keine Eilkompetenz der Staatsanwaltschaft mehr bei Gefahr im Verzug.

Es ist beispielsweise eine Telefonüberwachung möglich, nicht aber die Einholung von retrograden Standortdaten bei

- Geldfälschung
- Fälschung von Kredit-/Scheckkarten oder Schecks
- Menschenhandel
- Bandendiebstahl
- gewerbsmäßige Hehlerei, Bandenhehlerei

- einfacher Geldwäsche
- gewerbs- und/oder bandenmäßigem (Computer-)Betrug
- gewerbs- und/oder bandenmäßiger Urkundenfälschung
- einfachem Raub oder Erpressung.

Dabei geht es bei der Telefonüberwachung um Inhaltsdaten, während es bei den Vorratsdaten „nur" um Verkehrsdaten geht, also im Wesentlichen Rufnummern, IMSI-und IMEI-Nummern, IP-Adresse, Anfang und Ende der Kommunikation sowie Standortdaten.

Moderne Formen der Tatbegehung im Bereich der Cyberkriminalität wie Carding, Skimming, Phishing, DDOS-Angriffe und Drohung damit sowie Ransomware-Angriffe (außer bei Gewerbsmäßigkeit und/oder bandenmäßiger Begehung) oder verbreitete professionelle Betrugstaten wie die sog. Enkeltrickmasche werden außer acht gelassen.

Es gab aber auch deswegen keine retrograde Daten aufgrund der Vorratsdatenspeicherung mehr, weil zwar seit dem 30.7.2017 die Speicherung gesetzlich verpflichtend war, aber grundsätzlich nicht mehr gespeichert wurde. Das hat folgenden Hintergrund:

Die **Bundesnetzagentur** hat aufgrund der Entscheidung des OVG Münster am **28.6.2017** erklärt, bis zum rechtkräftigen Abschluss eines Hauptsacheverfahrens von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der in § 113b TKG geregelten Speicherverpflichtungen gegenüber allen verpflichteten Unternehmen abzusehen. Bis dahin werden auch keine Bußgeldverfahren wegen einer nicht erfolgten Umsetzung gegen die verpflichteten Unternehmen eingeleitet.

Als neue Entwicklung wurde jedoch jüngst bekannt, dass am **26. April 2018** eine **Besprechung der Mobilfunkprovider, dreier Ministerien, der Sicherheitsbehörden und der Generalstaatanwaltschaft Stuttgart** stattgefunden hat. Die Provider Telefónica, Vodafone und Telekom haben sich nunmehr dazu bereit erklärt, retrograde Standortdaten über die für diesen Zweck eingerichtete „Elektronische Schnittstelle Behörden" in digitaler Form zu beauskunften. Es kann unter Berufung auf § 100g Abs. 1, Abs. 2 StPO i.V.m. § 96 TKG um Übermittlung der gemäß § 96 Abs. 1 TKG erhobenen Verkehrsdaten einschließlich zurückliegender Standortdaten gebeten werden. Die Deutsche Telekom wiederum erteilt nur bei Androhung eines Ordnungsgeldes Auskunft. Andere Abfragen werden unter Hinweis auf die Nichtverfügbarkeit der gemäß § 113b TKG zu speichernden Daten zurückgewiesen bzw. wird eine Nullauskunft erteilt.

Wie sieht ein Funkzellenbeschluss aus?

Er wird auch, wenn nicht überwiegend, bei noch nicht offen gelegten Verfahren beantragt. Er wird nach § 44 Abs .4 StPO und unter Zurückstellung der Benachrichtigung des Betroffenen für 12 Monate nach § 101a Abs .6, 101 Abs. 4 und 6 StPO für die drei Netzbetreiber Telekom Deutschland GmbH (D1), Vodafone D2 GmbH und die Telefónica Deutschland Holding AG (E2) eingeholt, grundsätzlich bis zuletzt noch nur zu den Verkehrsdaten – ohne Standortdaten -. Nach der Einigung vom 26.4.2018 wird sich die Auskunft in Zukunft auch wieder auf die retrograden Standortdaten beziehen. Der Tatvorwurf wird konkret und unter Auflistung der einschlägigen Paragraphen aufgelistet. Es wird ausgeführt, dass und warum es sich um eine Straftat von auch im Einzelfall erheblicher Bedeutung handelt, warum die Maßnahme geeignet, zweckdienlich, erforderlich, angemessen ist. So benutzen erfahrungsgemäß Teilnehmer arbeitsteilig ausgeführter Taten Mobilfunkendgeräte, um miteinander zu kommunizieren. Es liegt nahe, dass sie zumindest mit einem absichernden Mittäter in Tatortnähe über eine Telekommunikations- oder Datenverbindung in Kontakt stehen oder sich zumindest

Datenverbindungen durch mitgeführte Mobiltelefone im Rahmen automatischer Zugriffe von und auf Apps aufbauen und ein Vergleich zu weiteren Tatorten möglich wird.

Dem Beschluss werden als Anlagen Ausmessungsunterlagen zu den Funkzellen beigefügt. Die Ausmessung stellt sicher, dass wirlich nur der betroffene Bereich Gegenstand einer Anfrage ist.

Die Maßnahme ist im verdeckten Bereich häufig Ansatzpunkt für eine Telefonüberwachung, der baldmöglichst eine Observation zur Seite gestellt wird.

Praxisbezug

Retrograde Standortdaten spiele eine wichtige Rolle z.B. bei Geldautomatensprengungen, Einbrüchen in Banken und Sparkassen, Raubtaten, der Kfz-Verschiebung, im Betäubungsmittelhandel und in Erpressungsfällen.

Nun ist es in der Tat so, dass § 113b TKG eine allgemeine Speicherpflicht begründet, ohne dass nach personellen, zeitlichen oder geografischen Merkmalen eine Begrenzung stattfindet. Andererseits beträgt der Speicherzeitraum nicht mehr 6 bis 24 Monate, sondern nur noch 10 Wochen für Verkehrsdaten und 4 Wochen bei Standortdaten. Diese Zeiten sind relativ kurz bemessen und müssen den Zeitraum abdecken, in dem es zu einer Anzeige kommt und eine Reaktion der Strafverfolgungsbehörde samt richterlicher Entscheidung ohne schuldhaftes Zögern möglich ist. Überdies sind Personenkreise nach § 113b Abs. 6 i.V.m. § 99 Abs. 2 S. 1 TKG von der Speicherfrist ausgenommen.

Daten im Sinne eines Quick-Freeze-Verfahrens erst ab einem bestimmten Anlass zu speichern führt grundsätzlich nicht weiter. Denn wenn man die Täter vorab nicht kennt, ist eine solche Einschränkung außer nach Tatort bei gleichem modus operandi nicht möglich.

Weiter speichern die Provider immer weniger Abrechnungsdaten nach § 96 TKG, auf welche Strafverfolgungsbehörden Zugriff nehmen könnten.

Hält man die derzeitige Vorratsdatenspeicherung für unionswidrig, wäre zu überlegen, welche Möglichkeiten der Einschränkung dieser Speicherung möglich ist, die wenigstens teilweise eine Vorratsdatenspeicherung ermöglicht. So sieht das Polizeirecht die Einteilung als sog. kriminalitätsbelasteten Ort nach § 21 Abs. 2 Nr. 1. a) aa) ASOG vor, bei welchem ohne Weiteres Personenkontrollen stattfinden können. Die örtliche Eingrenzung würde aber auch die Aussagekraft erlangter Daten entwerten, da gerade untypische, kleinere Orte mit geringer Bevölkerungszahl aufschlussreich sein können, etwa bei einer Nummer, die sowohl am Tatort als auch nachts in einem entlegenen Dorf, in dem ein amtliches Kennzeichen entwendet wurde, festgestellt wurde, wenn bekannt ist, dass die Täter grundsätzlich für ihre Fluchtfahrzeuge gestohlene Kennzeichen nutzen.

Sensibilität der abgefragten Daten

Zu berücksichtigen ist bei den abgefragten Daten auch, dass hier Telefonnummern abgefragt werden, zu denen grds. keine Nachforschung zum Anschlussinhaber stattfindet. Die aufgelieferten Verkehrsdaten an sich haben keine Aussagekraft und lassen keinen Rückschlüss auf eine Einzelperson zu. Erst wenn z.B. bei mehrfach auftretenden Nummern bei Serientaten klar wird, dass eine Relevanz

in Betracht kommt, erfolgen solche Nachfragen. Die Sonderbände der Ermittlungsbehörden weisen keine Hinweise auf konkrete Personen auf. Bei übereinstimmenden Nummern zu mehreren Tatorten führt ein Abgleich häufig zur Feststellung von fiktiven Personalien der Anschlussinhaber. Überprüfungen zur Benachrichtigung nach durchgeführter Maßnahme erfolgen nicht, da dies den Eingriff in die betroffenen Rechte vertiefen würde.

Die Speicherfristen sind auf 4 bzw. 10 Wochen verkürzt. Es gibt Benachrichtigungspflichten und Rechtsschutzmöglichkeiten gegen die Maßnahme. Für Funkzellendaten gibt es einen abschließenden Katalog von Straftaten, der enger ist als der für eine Telefonüberwachung.

Die Mitteilungspflichten nach § 101 StPO sind sehr zeitaufwendig für Polizei (vorbereitend) und Staatsanwaltschaft. Es kommt grundsätzlich nicht zu Beschwerden von Drittbetroffenen – mir persönlich ist keine einzige bekannt -, dafür aber zu einer ganzen Reihe von Nachfragen Drittbetroffener, welche die Anschreiben inhaltlich nicht verstehen und sich erkundigen, ob sie verpflichtet seien, rechtliche Schritte zu unternehmen oder einen Anwalt zu beauftragen, was nicht der Fall ist.

Auswirkung der Änderung in der Strafverfolgung

Werden dem Bürgerrechtsstärkungs-Gesetz folgend keine Vorratsdaten mehr gespeichert, gibt es im Regelfall, da immer weniger Verkehrsdaten nach § 96 TKG gespeichert werden, auch keine Daten mehr, auf welche Strafverfolgungsbehörden Zugriff nehmen könnten. Gemäß § 100 g Abs. 2 StPO wird auf retrograde Verkehrsdaten ohnehin nur zugegriffen, wenn die Erforschung des Sachverhalts auf andere Weise nicht möglich oder erheblich erschwert wäre, in anderen Worten, wenn im Prinzip diese Datenabfrage der einzige Ermittlungsansatz ist. Als Folge des Gesetzes werden also schwere Straftaten unverfolgt bleiben. Das muss jedem, der das Gesetz befürwortet, klar sein. Dem gegenüber sind die Eingriffe angesichts der starken gesetzlichen Einschränkungen m.E. hinnehmbar und verhältnismäßig.

Berlin, den 9. Juni 2018

Petra Leister, Oberstaatsanwältin

Staatsanwaltschaft Berlin