Matthias Kegel
Oberstaatsanwalt
Generalstaatsanwaltschaft
des Landes Brandenburg

Brandenburg a.d.H., den 18.02.2019

- per E-Mail –

An den
Deutschen Bundestag
Ausschuss für Recht
und Verbraucherschutz
Sekretariat PA 6

Öffentliche Anhörung

des Ausschusses für Recht und Verbraucherschutz

des Deutschen Bundestages

zum Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 (BT-Drucksache 19/4671)

am 20.02.2019

Zum vorliegenden Gesetzentwurf nehme ich wie folgt Stellung:

Artikel 1 Nummer 6 a bb: § 100g Absatz 1 Sätze 3 und 4 StPO-E

Die neuen Sätze 3 und 4 in § 100g Absatz 1 StPO-E erlauben die Erhebung der aus betrieblichen Gründen gespeicherten (retrograden) Standortdaten nach § 96 Absatz 1 TKG. Die Regelung ist unbedenklich; sie widerspricht weder der Intention des Gesetzgebers aus 2015, noch werden damit die Befugnisse der Strafverfolgungsbehörden erweitert. Vielmehr wird dadurch eine nicht vorhersehbare planwidrige Vollzugslücke geschlossen.

Standortdaten dürfen in Umsetzung der Entscheidung des Bundesverfassungsgerichts vom 02.03.2010 (NJW 2010, 833) nur noch in den engen Grenzen von § 100g Absatz 2 StPO aus den Vorratsdaten nach § 113b TKG erhoben werden. Bereits im Zeitpunkt des Inkrafttretens des „Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ am 18.12.2015 bestand in Bezug auf die Erhebung von Standortdaten eine Vollzugslücke, weil die Pflicht zur Speicherung dieser Daten nach § 113b Absatz 4 TKG für die Provider nach der Übergangsregelung des § 150 Absatz 13 TKG erst zum 01.07.2017 gegriffen hat und in dieser Zeitspanne die Erhebung von Standortdaten nach § 100g Absatz 2 StPO ins Leere gelaufen wäre. Der Gesetzgeber wollte hingegen einen lückenlosen retrograden Abruf von Standortdaten beim Verdacht auf Begehung einer Katalogstraftat nach § 100g Absatz 2 StPO (BT-Drs. 18/5088, S. 44) ermöglichen. Diese Lücke schloss er mit einer Übergangsregelung in § 12 Absatz 1 EGStPO, wonach die nach § 96 Absatz 1 Satz 1 Nummer 1 TKG gespeicherten Standortdaten bis zum 29.07.2017 auf der Grundlage des § 100g Absatz 1 StPO in der bisherigen Fassung erhoben werden durften.

Faktisch bestand auch nach dem 01.07.2017 ein Vollzugshemmnis fort, was dazu führte, dass die Staatsanwaltschaften Standortdaten nach § 113b Absatz 4 TKG weiterhin nicht erheben konnten. Denn fast alle Provider speichern überhaupt keine Vorratsdaten mehr, nachdem die Bundesnetzagentur am 28.06.2017 unter Hinweis auf die Entscheidung des OVG Münster vom 22.06.2017 (Az. 13 B 238/17, BeckRS 2017, 114873) und das Urteil des EuGH vom 21.12.2016 (NJW 2017, 717) erklärt hat, keine Anordnungen und sonstige Maßnahmen zur Durchsetzung der Speicherverpflichtung gegen Provider zu ergreifen. Damit wird die Aufklärung von schweren Straftaten erschwert, wenn nicht gar verhindert. Die Justizministerinnen und Justiz-

minister haben auf ihrer Herbstkonferenz am 09.11.2017 daher den Gesetzgeber aufgefordert, Sorge zu tragen, dass den Strafverfolgungsbehörden weiterhin der Zugriff auf von den Dienstanbietern gespeicherte Standortdaten ermöglicht wird.

Wie zuvor in 2015 wird der gesetzgeberische Wille nach einer lückenlosen Erhebung der Standortdaten durch die Neuregelung in § 100g Absatz 1 Satz 3 und 4 StPO-E geschlossen, indem die Strafverfolgungsbehörden die nach § 96 Absatz 1 Satz 1 Nummer 1 TKG gespeicherten Standortdaten unter den Voraussetzungen des § 100g Absatz 2 StPO-E erheben dürfen.

Artikel 1 Nummer 35: § 491 StPO-E

Nach der Neuregung von § 491 StPO-E entfallen nach Antrag durch die betroffenen Personen die Sperrfristen für die Auskunft zu laufenden Verfahren und der pauschale Hinweis bei einer Negativauskunft auf diese Sperrfristen nach § 491 Absatz 1 Satz 2 bis 6 StPO. Damit wird (zum Leidwesen insbesondere der staatsanwaltschaftlichen Praxis wegen des damit verbundenen Mehraufwandes) konsequent Artikel 14 der Richtlinie (EU) 2016/680 umgesetzt, der solche Sperrfristen nicht kennt. § 491 StPO-E gilt nur noch subsidiär zum Auskunftsanspruch der betroffenen Personen nach § 57 BDSG.

Das BMJV hat in der Abstimmung zu den Referentenentwürfen die Einwände aus der staatsanwaltschaftlichen Praxis in § 491 Absatz 2 Satz 2 StPO-E aufgegriffen, um der Gefahr einer Ausforschung des staatsanwaltschaftlichen Fachverfahrens zu begegnen, indem der Bescheid an die antragstellende Person keinen Rückschluss zulassen soll, ob noch geheim zu haltende Ermittlungsverfahren vorliegen oder nicht, um den Ermittlungserfolg nicht zu gefährden. Dadurch wird die bisherige Auskunftserteilung – bis auf die Sperrfristen – beibehalten.

Artikel 1 Nummer 41: § 500 StPO-E

Dass Teil 3 des Bundesdatenschutzgesetzes auf das gesamte Strafverfahren für alle öffentlichen Stellen der Länder anzuwenden ist, wird ausdrücklich begrüßt. Damit wird ein einheitlicher Datenschutzstandard bei Gerichten, Strafverfolgungsbehörden, Vollstreckungsbehörden, Bewährungshilfe, Aufsichtsstellen bei Führungsaufsicht und Gerichtshilfe gewährleistet, eine länderspezifische Zersplitterung vermieden und alle betroffenen Personen datenschutzrechtlich gleich behandelt.

Würden hingegen die jeweiligen Landesdatenschutzgesetze für Staatsanwaltschaften, Gerichte und Polizei zur Anwendung gelangen, wäre das mit nicht unerheblichen Nachteilen verbunden, weil die Länder bereits im Gesetzgebungsverfahren begonnen hatten, die Richtlinie (EU) 2016/680 für Justiz und Polizei in den Landesdatenschutzgesetzen mit differenzierenden Regelungen von Bundesland zu Bundesland zu integrieren.

a) Eine länderspezifische Zersplitterung würde in den länderübergreifenden Fachverfahren zu schwierigen länderspezifischen Anpassungsprogrammierungen führen. Neben dem zusätzlichen personellen und finanziellen Aufwand wäre die Weiterentwicklung der Fachverfahren kaum mehr zu beherrschen.

b) Die länderübergreifende Kommunikation und der länderübergreifende Datenaustausch in Strafsachen bei elektronischer Aktenführung wären durch eine unterschiedliche datenschutzrechtliche Ausgestaltung in den einzelnen Bundesländern erschwert. Die Kommunikationsszenarien müssten diese Unterschiede berücksichtigen. Das würde dem Bestreben aus dem Koalitionsvertrag zuwiderlaufen, den Datenaustausch im Bereich der Strafverfolgung zwischen Polizei und Justiz verbessern zu wollen (S. 123, Zeile 5767 f.).

Der Verbleib der Zuständigkeit der Datenschutzaufsicht bei den Landesbeauftragten gewährleistet im Übrigen eine einheitliche Aufsicht der Staatsanwaltschaften und der übrigen öffentlichen Stellen in den jeweiligen Bundesländern.

Artikel 2: § 17 EGStPO-E

Die IT-Anwendungen der Staatsanwaltschaften und Gerichte sind nicht in der Lage, die datenschutzrechtlichen Anforderungen kurzfristig umzusetzen. Die entsprechenden Hinweise der Landesjustizverwaltungen sind in § 17 Absatz 3 EGStPO aufgegriffen worden, wonach für die IT-Anwendungen der Staatsanwaltschaften und Gerichte längere Umsetzungsfristen nach Artikel 63 Absatz 2 und 3 der Richtlinie (EU) 2016/680 gelten sollen, um hinreichend Zeit für die Umsetzung der neuen Protokollierungsvorgaben und die hierfür erforderlichen technischen Anpassungen einzuräumen.

gez.
Matthias Kegel
Oberstaatsanwalt