Vorratsdatenspeicherung – Endlich?!

von Dr. Jakob Dalby[*]

Abstract
Dieser Beitrag befasst sich mit der strafprozessrechtlichen Regelung zur Vorratsdatenspeicherung in § 100g StPO sowie der korrespondierenden Regelung zur Datenspeicherung in § 113b TKG. Insbesondere der Umfang der durch die Telekommunikationsunternehmen zu speichernden Daten sowie die konkrete Ausgestaltung der „Erhebung", also des Abrufs, durch die Strafverfolgungsbehörden sind von Interesse. Einzelne kritische Punkte werden hierbei herausgegriffen und bewertet. Der Beitrag versucht jedoch keine abschließende Prüfung der Verfassungsmäßigkeit dieser besonders umfangreichen Regelung, sondern beurteilt nur besondere Problemfelder auf deren verfassungsgemäße Umsetzung.

This Essay deals with the provisions on criminal proceedings with regard to data retention under Sec. 100g StPO and the corresponding provision in Sec. 113b TKG. Especially the extent of data that has to be stored by the relevant telecommunication companies as well as the specific structuring of the data „collection" – the retrieval of data – by the law enforcement authorities are of interest. The essay focuses on some of the crucial issues within the aforementioned sections. A final assessment of the particularly complex provision regarding data retention therefore is not given but the assessment of the specific problems (extent & retrieval) and their constitutional solution.

I. Einführung

Die Vorratsdatenspeicherung ist mittlerweile vermutlich das Steckenpferd vieler Autoren geworden. Vorerst ist die Diskussion im luftleeren Raum jetzt beendet. Der Gesetzgeber hat Fakten geschaffen. Man möchte sagen: Endlich! Zu prüfen ist jedoch, ob nicht ein fragender Unterton angebracht ist. Zumindest hat der Gesetzgeber sich im Nebenbei der Flüchtlingskrise dieser Regelungsthematik angenommen und es so geschafft, das wohl „heißeste Eisen" der jüngeren strafverfolgungsrechtlichen Grundsatzdiskussion lautlos zu schmieden. Dieser Beitrag erläutert die Systematik der Regelung und bewertet die Konzeption der §§ 113b TKG und § 100g Abs. 2 StPO.[1] Der Fokus liegt auf dem Anwendungsbereich der Norm (Datenumfang) und den Verwendungs- und Abrufbestimmungen für die Strafverfolgungsbehörden.

II. Der rechtliche Rahmen

Den rechtlichen Rahmen der neuen Vorratsdatenspeicherung bilden Art. 1 und Art. 2 des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10.12.2015.[2] Hiermit führte der deutsche Gesetzgeber die §§ 113a - g TKG neu ein und änderte den § 100g StPO. Dies ist die gesetzgeberische Antwort auf die Frage „wieviel" Vorratsdatenspeicherung eingedenk der verfassungs- und europarechtlichen Rechtsprechung noch möglich ist.[3] Die Regelungen sollen die Vorratsdatenspeicherung grundrechtskonform im Hinblick auf das Telekommunikationsgeheimnis aus Art. 10 GG sowie die datenbezogenen Grundrechte aus Art. 7 und Art. 8 der Grundrechtecharta ausgestalten.[4]

III. Systematik: Doppeltürmodell

Die Systematik der Vorratsdatenspeicherung mit der Begründung der Speicherpflicht und der Bestimmung der Verantwortlichen und sonstiger Parameter (Art und Dauer) im TKG und der korrespondierenden Zugriffsnorm für den Abruf durch die Strafverfolgungsbehörden in der StPO, folgt dem bekannten Schema des Auskunftsverfahrens über Bestandsdaten (vgl. §§ 113 TKG i.V.m. § 100j StPO).[5] Diese Auseinanderziehung der konkreten Verantwortlichkeiten und Voraussetzungen in zwei verschiedene Gesetze in einem Zweischritt, nennt sich „Doppeltürmodell". Hierdurch werden die Vorschriften, die zum Umgang mit personenbezogenen Daten ermächtigen, in verschiedene, aufeinander aufbauende Eingriffe verschachtelt: Erhebung, Speicherung und Übermittlung (1. Tür) sowie Datenabruf und -übermittlung (2.Tür). Dies ist eine maßgebliche Anforderung an die Verfassungsmäßigkeit der Maßnahme.[6] Die Speicherpflicht und Übermittlungsberechtigung des TKG wird durch die Zugriffsregelung (Erhebungsermächtigung) in der StPO zu einer Übermittlungspflicht konkretisiert.

1. Die erste Tür: Speicherverpflichtung im TKG

a) Verpflichtete, Umfang der Speicherpflicht und Übermittlungsberechtigung

Die Verpflichtungen zur Speicherung von Verkehrsdaten und die sonstigen Regelungsgegenstände (u.a. Datensicherheit) der §§ 113b bis 113g TKG beziehen sich auf Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer gem. § 113a Abs. 1 S. 1 TKG. Dies

---

* Der Verfasser ist Legal Counsel (Legal and External Affairs), British American Tobacco GmbH, Hamburg.

1 Fragen zur Datensicherheit etc., wie sie das *BVerfG* verändert sehen wollte im Vergleich zum § 100g a.F. sind nicht Gegenstand des Beitrags.

2 BGBl. I 2015, S. 2218, in Kraft seit dem 18.12.2015.

3 *BVerfG,* NJW 2010, 833 und *EuGH*, NJW 2014, 2169.

4 BT-Drs. 18/5088, S. 21-23.

5 S. zur manuellen Bestandsdatenauskunft *Dalby*, CR 2013, 361.

6 „Jeder dieser Eingriffe bedarf jeweils einer eigenen Rechtsgrundlage, wobei eine Zusammenfassung mehrerer Rechtsgrundlagen in einer Norm nicht ausgeschlossen ist", *BVerfG*, Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn. 123.

sind Telekommunikationsdiensteunternehmen i.S. von § 3 Nr. 6 lit. a) TKG, also nicht bloß bei der Übermittlung von Daten mitwirkende Unternehmen.[7] Anbieter, die ihren Kunden nur eine kurzzeitige Nutzung des Telekommunikationsanschlusses ermöglichen (Hot Spots in Hotels, Restaurants und Cafés) sind nicht erfasst.[8] Der Umfang der zu speichernden Daten ergibt sich aus § 113b TKG als fachgesetzliche Kernregelung der Vorratsdatenspeicherung im Sinne der ersten Tür. Sie bestimmt die Adressaten sowie die Grundvoraussetzungen der Speicherpflichten und legt die zu speichernden Datenkategorien fest und macht Vorgaben, wie die Speicherung der Daten und deren Löschung zu erfolgen haben.[9]

§ 113b Abs. 1 TKG enthält die Verpflichtung zur Datenspeicherung, differenziert nach Verbindungsdaten (klassische Verkehrsdaten wie Rufnummer, Datum, Uhrzeit, dynamische IP-Adresse, vgl. § 113b Abs. 2 und Abs. 3 TKG) und nach Standortdaten. Die Verbindungsdaten dürfen höchstens zehn Wochen gespeichert werden; Standortdaten (§ 113b Abs. 4 TKG) dürfen hingegen nur für vier Wochen gespeichert werden.

§ 113b Abs. 2 S. 1 TKG regelt die einzelnen Speicherpflichten für Erbringer öffentlich zugänglicher Telefondienste und umfasst Ausprägungen wie Festnetz, Mobilfunk und Internettelefonie. Bei der Übermittlung von SMS, MMS und ähnlichen Nachrichten beziehen sich die Zeitpunkte der Telekommunikation auf Versendung und Empfang der Nachricht (§ 113b Abs. 2 S. 2 Nr. 1 TKG). § 113b Abs. 2 S. 2 Nr. 2 TKG erstreckt die Speicherpflicht auf nicht entgegengenommene oder erfolglose Anrufe. Dies war bereits im Rahmen des § 113a Abs. 5 TKG a. F. mit einem anderen Wortlaut der Fall. § 113b Abs. 2 Nr. 4 TKG regelt die Speicherung von IMSI (lit. a) und IMEI (lit. b) als die internationalen Kennungen von Anschluss und Endgerät. Lit. c erfasst Prepaidkarten und ordnet die Speicherung des Zeitpunkts der ersten Aktivierung des Dienstes an.[10] § 113 Abs. 2 Nr. 5 TKG erfasst IP-Adressen bei der Internettelefonie.[11]

Als wichtigste Regelung muss der folgende § 113b Abs. 3 Nr. 1 TKG bezeichnet werden. Er regelt insbesondere die Pflicht zur Speicherung der dynamischen IP-Adresse für Erbringer öffentlich zugänglicher Internetzugänge. Ferner ist neben der dynamischen IP-Adresse auch die „eindeutige Kennung des Anschlusses“ sowie die „zugewiesene Benutzerkennung“ zu speichern, um die „Rückverfolgung und Identifizierung der Quelle des Kommunikationsvorgangs besser zu ermöglichen“ (§ 113b Abs. 3 Nr. 2 TKG).[12] Die Gesetzesbegründung schweigt sich dazu aus, was diese Begrifflichkeiten meinen. In Betracht kommen verschiedene Kennungen, wie etwa NAT[13] oder die MAC-Adresse[14]. Diesen ist gemein, dass hierdurch nicht konkret ein Nutzer mit Klarnamen identifizierbar ist, sondern es sich um eine zuordnenbare Kennung (etwa eine Nummernfolge) handelt. Kategorisch kann es sich sowohl um Bestandsdaten, wie auch Verkehrsdaten handeln. Weder die Begrifflichkeit „eindeutig“, noch „zugewiesen“, sagt etwas darüber aus, ob es sich um eine permanente Zuordnung handelt, wie es etwa bei der statischen IP-Adresse der Fall ist, oder um eine pro Sitzung vergebene Kennung. Jedenfalls bleibt unklar, welche Daten der Gesetzgeber hiervon erfasst sieht. Gem. § 113 Abs. 4 TKG sind die Standortdaten des anrufenden und des angerufenen Anschlusses bei Beginn der Verbindung, also die konkreten Bezeichnungen der Funkzellen, für vier Wochen zu speichern.

§ 113c TKG konkretisiert nun die Übermittlungsberechtigung im Falle der Anfrage von Strafverfolgungsbehörden

---

7 Erbringer zeichnen sich dadurch aus, dass den Kunden regelmäßig ein eigener, in der Regel auf unbestimmte Dauer angelegter, Telekommunikationsanschluss zur selbstständigen Verwendung überlassen wird, vgl. BT-Drs. 18/5088, S. 37.

8 Interessant ist insofern, dass die Erhebungs-, Verwendungs- und Speicherberechtigung der §§ 96 ff. TKG enger ist, als die Zugriffsregelung des § 100g StPO (implizit auch nicht öffentliche Telekommunikationsdienste und nicht geschäftsmäßig erbrachte). Dies erklärt sich damit, dass die Strafverfolgungsbehörden selbst auch Verkehrsdaten in Echtzeit erheben dürfen (vgl. § 100g Abs. 1 S. 3 StPO) und hierzu nicht mehr nur auf die (berechtigt) gespeicherten Daten des Telekommunikationsdiensteanbieters angewiesen sind; dies bezieht sich auf Standortdaten, aber auch darüber hinaus können Echtzeit-Abfragen erfolgen, vgl. *Hegmann,* Beck OK-StPO, § 100g Rn. 7 mit Verweis auf die Umsetzung des Art. 20 der Cybercrime Convention). Dies ergibt sich aber auch bereits aus einem Umkehrschluss aus § 100g Abs. 5 StPO, wonach sich eine Verkehrsdatenabfrage, die nicht beim Anbieter stattfindet, erst nach Abschluss des Telekommunikationsvorgangs nach den allgemeinen Regeln richtet (§§ 94 ff. StPO). D.h. der Gesetzgeber geht davon aus, dass eine Erhebung – und zwar nicht nur von Standortdaten in Echtzeit ohne Einbindung des Telekommunikationsdiensteanbieters – möglich sein, diese mithin auch Bibliotheken, Unis, Hotspots etc. betreffen kann.

9 Anders als nach § 113a TKG a. F. sind die Daten ausschließlich im Inland zu speichern; eine Verlagerung durch Speicherung in einem anderen Mitgliedstaat der EU ist nicht möglich. Dies sollte die in §§ 113c ff. TKG enthaltenen Anforderungen an die Verwendung und die Sicherheit der Daten gewährleisten.

10 Nicht alle Prepaid-Anschlüsse werden hiervon erfasst. So ist auch eine Aktivierung ohne das Erzeugen von Verkehrsdaten möglich, soweit die Aktivierung des Dienstes auf eine Weise erfolgt, bei der Verkehrsdaten weder erzeugt noch verarbeitet werden, wie dies etwa der Fall sein kann, wenn die Freischaltung durch eine sofortige Onlineanmeldung bei Vertragsschluss erfolgt. Dieser Fall wird auch nicht von § 113 TKG erfasst.

11 Dies ist notwendig, da die Speicherung einer dynamischen IP-Adresse noch keinen Aufschluss über den Adressaten des Internettelefonats gibt.

12 BT-Drs. 18/5088, S. 39.

13 Netzwerkadressübersetzung (englisch Network Address Translation, kurz NAT) ist in Rechnernetzen der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden, vgl. https://netzpolitik.org/2015/vorratsdatenspeicherung-kann-noch-mehr-jetzt-auch-mit-vollprotokollierung-von-portnummern/ (zuletzt abgerufen am 28.7.2016).

14 Die Media Access Control ist die Hardware-Adresse des einzelnen Netzwerkadapters und somit ein eindeutiger Identifikator des Geräts, vglb. der Gerätenummer eines Smartphones (IMEI). Sie ist manuell änderbar, sodass hier wohl kaum die MAC gemeint sein kann. http://www.itwissen.info/definition/lexikon/MAC-Adresse-MAC-address.html (zuletzt abgerufen am 28.7.2016)

nach § 100g Abs. 2 StPO zweckbezogen zu einer Übermittlungsverpflichtung.[15]

b) Bewertung

Die zentrale Forderung des *EuGH* in puncto Speicherpflicht ist die Beschränkung der Datenspeicherung „auf das absolut Notwendige".[16] Demnach ist eine ausnahmslose Speicherung sämtlicher Verkehrsdaten aller Kommunikationsmittel in Bezug auf alle Personen, die zugleich anlasslos, d.h. ohne (auch nur) mittelbare Veranlassung durch die Betroffenen erfolgt und nicht im mittelbaren oder entfernten Bezug zwischen Datenspeicherung und Bekämpfung schwerer Straftaten steht, nicht mit den europäischen und mithin mit den verfassungsmäßigen Grundrechten vereinbar.[17]

aa) Anlasslose Speicherung ist verfassungsgemäß

Gleichwohl werden im Rahmen der Vorratsdatenspeicherung Daten anlasslos gespeichert. In diesem Punkt driftet die Einschätzung des deutschen Gesetzgebers mit einer kritischen Lesweise des *EuGH*-Urteils auseinander. Der deutsche Gesetzgeber erkennt in der obigen Zusammenfassung der *EuGH*-Rechtsprechung nur eine Aufzählung der Gründe, die die Richtlinie zur Vorratsdatenspeicherung und eine entsprechende nationalstaatliche Umsetzung grundrechtswidrig machen würden – und zwar „in Summe".[18] Diese Auffassung fußt darauf, dass der *EuGH* nicht explizit Stellung zur Frage bezieht, ob die eine oder andere Spielart der Vorratsdatenspeicherung schlechthin unzulässig ist.[19] Folglich hält der deutsche Gesetzgeber weiterhin an der Anlasslosigkeit der Speicherung fest, wobei er gleichzeitig verschiedenste Forderungen umsetzt. So werden nicht alle verfügbaren Daten gespeichert (etwa URL nicht). Zudem darf eine Zweckverwendung nach § 113c TKG nur bei Verdacht besonders schwerer Straftaten erfolgen.

In der Tat ist dies jedoch nur ein „marginales Nachgeben" gegenüber der europäischen Rechtsprechung.[20] Diese ist aber nicht frei von Tadel – ganz unabhängig davon, wie man die Grundsätze der Entscheidung lesen möchte. Ein Verzicht auf die anlasslose Speicherung von Verkehrsdaten würde die Vorratsdatenspeicherung nämlich ihres Wesenskerns berauben. Schließlich zeichnet sich eine sinnvolle Speicherung dadurch aus, dass sie auch bisher nicht auffällige Personen einbezieht. Etwa Phänomene wie die „Lonely Wolves"[21] verdeutlichen dieses Dilemma. Diese Täter achten eben gerade peinlich genau darauf, keine Datenspuren zu hinterlassen, die eine mittelbare oder auch nur entfernte Verbindung zu bestimmten Verdachtspersonen schaffen. Ihnen nachzuspüren, auch wenn es nur zur Rekonstruktion des Täterverhaltens vor der Tat ist, wäre schwierig, wenn Datensätze vollständig fehlen.

Freilich gehen die Einschätzung des Nutzens der Vorratsdatenspeicherung bei Befürwortern und Gegnern komplett auseinander.[22] Um diesem Problem gerecht zu werden, wurde jedoch die Evaluationsklausel eingeführt – wenngleich auch erst auf Nachruf des Ausschusses für Recht und Verbraucherschutz – sodass der Nutzen sich noch in einer Endbewertung zeigen muss.[23] Dies stellt einen weiteren notwendigen Schritt dar, um die Geeignetheit der Vorratsdatenspeicherung und mithin die Erforderlichkeit zu beurteilen. Die Evaluationsklausel soll dem Ziel der Beschränkung der Datenspeicherung auf das absolut Notwendigste auf lange Sicht garantieren.[24]

---

15 Natürlich sind die gespeicherten Daten auch präventiv für die Polizeien nutzbar gem. § 113c Abs. 1 Nr. 2 TKG Eine solche Übermittlung ist zulässig, wenn eine Gefahrenabwehrbehörde unter Berufung auf eine gesetzliche Befugnis die Übermittlung verlangt zum Zwecke der Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand des Bundes oder eines Landes. Die Auskunft zur Verfolgung oder Verhinderung von Ordnungswidrigkeiten ist nicht von der Zweckverwendung erfasst.

16 *EuGH*, NJW 2014, 2169 (2172).

17 *EuGH*, NJW 2014, 2169. Unverhältnismäßiger Eingriff in Art. 7 (Recht auf Privatheit) und Art. 8 (Schutz personenbezogener Daten) der EU-Grundrechtecharta, ferner auch ein Eingriff in Art. 10 GG respektive das informationelle Selbstbestimmungsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

18 Der Gesetzgeber spricht insoweit von einer „Vielzahl von Kritikpunkten, die in ihrer Gesamtbetrachtung die Unverhältnismäßigkeit bedeuteten" und einer „Kombination" von langer Speicherdauer ohne Differenzierung nach Datenart, vgl. BT-Drs. 18/5088, S. 23.

19 Vgl. *EuGH*, Urt. v. 8.4.2014 – C 293/12, C 594/12, Rn. 69: „Aus der Gesamtheit der vorstehenden Erwägungen ist zu schließen, dass der Unionsgesetzgeber beim Erlass der RL 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 I der Charta einhalten musste."

20 *Nachbaur*, ZRP 2015, 215 (216). Zur Frage wie sich die europäische Rechtsprechung auf den nationalen Umsetzungsspielraum einer Vorratsdatenspeicherung ausgewirkt, s. *Wollenschläger/Krönke*, NJW 2016, 906; *Boehm/Andrees*, CR 2016, 146.

21 Einzeltäter ohne institutionalisierte Gruppenzugehörigkeit, die terroristische Anschläge verüben.

22 So kommt das Max-Planck-Institut für ausländisches und internationales Strafrecht in einem Gutachten 2011 zu dem Ergebnis, dass keine Schutzlücken entstehen, wenn auf die Vorratsdatenspeicherung verzichtet würde, vgl. http://vds.brauchts.net/MPI_VDS_Studie.pdf (zuletzt abgerufen am 28.7.2016); Richter am *BGH Nikolaus Berger* hingegen begründet den Nutzen der Vorratsdatenspeicherung in seiner Stellungnahme zum Regierungsentwurf 2015 mit praktischen Beispielen, vgl. http://www.bundestag.de/blob/387808/d6991ea70ad90bf15cceaec565c36b3b/berger-data.pdf (zuletzt abgerufen am 28.7.2016);
Münch führt die Anschläge in Paris als Beispiel für eine effektive Rückverknüpfung von Verkehrsdaten zur Rekonstruktion von Personenverbindungen an, *Münch*, ZRP 2015, 130 (131, 132); a.A. *Nachbaur*, ZRP 2015, 215 (216).

23 Nach der Beschlussempfehlung des Ausschusses wurde in Art. 7 des Gesetzes eine Evaluierungsklausel eingefügt, BT-Drs. 18/6391, S.3.

24 Da es keine empirischen Studien im Vergleich zur vorhergehenden gesetzlichen Regelung zur Speicherung von Verkehrsdaten gibt und auch ökonomisch die Kosten, die die Einführung einer Speicherpflicht für die Telekommunikationsunternehmen birgt, in das Ergebnis einzustellen sind, ist die Evaluation zielführendes Mittel. Berücksichtigt soll auch die Einhaltung der datenschutzrechtlichen Regelungen werden. Den Vorgaben der „Konzeption zur Evaluierung neuer Regelungsvorhaben" des Ausschusses der Staatssekretärinnen und Staatssekretäre für Bürokratieabbau in der am 23.1.2013 beschlossenen Fassung wird Rechnung getragen; vgl. BT-Drs. 18/6391, S. 9. Faktenbasis bilden die statistischen Erhebungen unter dem neuen § 101b StPO, wonach über die Maßnahmen nach § 100g StPO eine Übersicht zu erstellen ist. Sinnvoll wäre es, in diese Übersicht sogleich mit aufzunehmen, ob der erfolgreiche Abschluss des Verfahrens gerade aufgrund der Verkehrsdatenabfrage gelungen ist. Dies wäre mühelos zu integrieren gewesen und würde eine Erleichterung der Evaluationsarbeit ermöglichen. Im besten Fall wird das Evaluationsergebnis die Hypothese zur Einführung der Vorratsdatenspeicherung – nämlich diejenigen Lücken zu schließen, die eine rein reaktive und zukunftsgerichtete Abfrage von Verkehrsdaten hinterlässt – tatsächlich praktisch bestätigen.

Die Versteifung der Kritiker der Vorratsdatenspeicherung auf die Anlasslosigkeit berücksichtigt im Übrigen Wirk- und Zweckmechanismus des Doppeltürmodells nicht ausreichend. Die Intensität der anlasslosen Speicherung einer Vielzahl von Daten wird nämlich abgefedert durch sehr strenge Abrufmechanismen.[25] Die Verfassungsmäßigkeit der anlasslosen Speicherung rechtfertigt sich über die enge Zweckbegrenzung des § 113c TKG. Dem Gesetzgeber ist in diesem Punkt beizupflichten. Diese Zweckbindung darf nun aber nicht im Nachhinein aufgeweicht werden, wenngleich eine gewisse Lockerung der Abrufvoraussetzungen noch keine Verfassungswidrigkeit bedeuten würde (hierzu sogleich in der Bewertung des § 100g Abs. 2 StPO).

bb) Speicherpflicht für dynamische IP-Adresse begrüßenswert

Als längst überfällig darf die Aufnahme einer expliziten Speicherpflicht für das wichtigste Verkehrsdatum, die dynamische IP-Adressen, bezeichnet werden.[26] Diese korrespondiert mit der Ergänzung in § 100j Abs. 2 StPO, wonach für Bestandsdatenauskünfte zu dynamischen IP-Adressen auf nach § 113b TKG gespeicherte Verkehrsdaten zurückgegriffen werden darf. Man kann zwar davon ausgehen, dass bereits vorher ein Pool dynamischer IP-Adressen abfrag- und zuordnenbar war, doch die Speicherung dieser dynamischen IP-Adressen auf Grundlage der §§ 96 ff. TKG war hochstreitig. Grund hierfür: Das Diensteunternehmen benötigt diese nicht für Abrechnungszwecke bei der heutigen Verbreitung von Flatrate-Tarifen.[27] Kompliziert wurde die Speicherberechtigung über § 100 TKG konstruiert.[28] Teilweise wehrten sich die Diensteunternehmen auch explizit gegen die Abfrage der dynamischen IP-Adressen unter Verweis auf die ungeklärte Rechtsgrundlage.[29]

Der Gesetzgeber korrigiert mit der Aufnahme nunmehr auch seine eigene Gesetzgebung, führte er doch mit § 113 Abs. 1 S. 2 TKG im Juli 2013 eine Regelung ein, die die Zuordnung dynamischer IP-Adressen voraussetzte, obwohl diese eben nicht hätten gespeichert werden dürfen.[30]

cc) Speicherung der „eindeutigen Anschlusskennung" und „zugewiesene Benutzerkennung" fragwürdig

Bereits über das manuelle Auskunftsverfahren, das explizit den Zweck der Personenidentifizierung verfolgt, ist über die Verknüpfung von dynamischer IP-Adresse mit Bestandsdaten die Identifizierung einer bestimmten Person als Anschlussinhaber möglich. In § 113c Abs. 1 Nr. 3 TKG ist im Rahmen der Zweckverwendung die Möglichkeit der Auskunftserteilung über die dynamische IP-Adresse geregelt für ein anschließendes manuelles Auskunftsverfahren nach § 113 Abs. 1 S. 3 TKG. Dieser Verweis ist vollkommen korrekt, da über die Zuordnung der dynamischen IP-Adresse die dahinterstehende Auskunft über die Bestandsdaten des Anschlussinhaber als Mittel der Personenidentifikation erlangt werden können.

Fraglich ist jedoch, wozu diese Zuordnung überhaupt noch zu erfolgen hat und wie sich die Qualität dieser Auskunft über die hinter einer zu einem bestimmten Zeitpunkt vergebenen dynamischen IP-Adress stehenden Bestandsdaten von der „eindeutigen Anschlusskennung" und der „zugewiesenen Benutzerkennung" i.S.d. § 113 Abs. 3 Nr. 2 TKG unterscheiden. Dies legt die Vermutung nahe, es handelt sich um eine informationstechnische Tautologie. Soweit die Regelung nun aber den genauen Benutzer identifizieren möchte, unterscheidet sich die Regelung vom manuellen Auskunftsverfahren i.V.m. § 100j StPO, welches nur über den Inhaber des „Internetvertrags" aufklärt. Obwohl die Benutzerkennung nicht die Speicherung eines Klarnamens bedeutet, sondern nur etwa einer Nummernfolge, die erst über eine anschließende Bestandsdatenabfrage nach §§ 112, 113 TKG die Zuordnung zu einer Person bzw. einem Geräteinhaber ermöglicht, vermag die Intensität dieser Auskunft höher sein, als die Auskunft über die Gerätekennung eines Smartphones (IMEI) oder besagte Zuordnung dynamischer IP-Adressen. Eine Benutzerkennung eines internetfähigen Gerätes hat schon nach dem Wortlaut einen höheren Aussagewert über die dahinterstehende Person. Ihr liegt eine konkrete Identifizierbarkeit zugrunde, sodass letztendlich personengenau eine Geräte-Zuordnung zu der Person erfolgen könnte, die Initiator der Internetnutzung ist. Dies birgt eine erhöhte Eingriffsintensität, da ohne größeren Aufwand eine Profilerstellung der Internetaktivitäten unter dieser Nutzerkennung möglich erscheint. Dies gilt jedenfalls dann, wenn der Gesetzgeber hiermit systemfremd ein Bestandsdatum in den § 113b TKG aufgenommen hat. Anders als bei der geteilten Nutzung von Internetanschlüssen ist nämlich zu unterstellen, dass mittlerweile die meisten Nutzer über ein eigenes personalisiertes Endgerät das Internet nutzen, dass sich permanent durch eine Benutzerkennung im Internet identifizierbar machen würde. Ähnliche Probleme

---

25 A.A. *Roßnagel*, NJW 2016, 533 (538).

26 In der Praxis sind dynamische IP-Adressen von der größten Wichtigkeit in Zusammenhang mit Cybercrime (90,2 % der Auskunftsersuchen waren Abfragen anhand einer dynamischen IP-Adresse im Jahr 2011, vgl. den Abschlussbericht BKA 2011 – Stand der statistischen Datenerhebung im BKA zu den Auswirkungen des Urteils des *BVerfG* zu „Mindestspeicherfristen", S. 5, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Mindestspeicherfrist/studie.pdf?__blob=publicationFile (zuletzt abgerufen am 28.7.2016).

27 Im Erg. auch *BGH,* NJW 2011, 1509 (1510) in Bezug auf Flatrate-Tarife; vgl. auch *Dittscheid/Rudloff,* in: Beck'scher TKG Kommentar, § 45i TKG Rn. 9 f.

28 V.a. vom *BGH* vertreten *BGH*, NJW 2011, 1509; dagegen *Gercke/Brunst*, Praxishandbuch Internetstrafrecht (2010), Rn. 767 ff. zur Entgeltabrechnung; sehr ausführlich vor allem zur Störungsbeseitigung *Breyer*, MMR 2011, 57; zum für und wider nach der alten Rechtslage ausführlich *Dalby*, Grundlagen der Strafverfolgung im Internet und der Cloud – Möglichkeiten, Herausforderungen und Chancen (2016), S.86 ff.

29 So etwa Vodafone mit dem Hinweis, dass eine Speicherung dynamischer IP-Adressen über die Verbindung hinaus nicht notwendig sei; vgl. http://www.loschelder.de/de/rechtsanwaelte/aktuelles-rechtsfragen/details/artikel/vodafone-wehrt-mit-loschelder-unberechtigte-auskunftsersuchen-von-abmahnern-ab-datenschutz-im-inte.html (zuletzt abgerufen am 28.7.2016).

30 Die Behörde kann über das Abfangen von Telekommunikation und die Überwachung einer Website zwar auch selbst an die dynamischen IP-Adressen kommen, jedoch werden diese zumeist aus den Log-Files des Anbieters stammen, sodass er deren Mitwirkung bedarf.

dürften mit der IPv6 anstehen. Jedenfalls verdient der § 113b Abs. 3 TKG weiter beobachtet zu werden. Eine abschließende Beurteilung kann derzeit nicht erfolgen.

2. Die zweite Tür: Zugriffsregelung in den Fachgesetzen zur Verwendung und Abruf der Daten

a) Voraussetzungen des Abrufs

Die Grobstruktur des § 100g StPO erklärt sich ebenfalls bestens anhand des Doppeltürmodells. Dies wird insbesondere deutlich an der Zweiteilung der Vorschrift nach Art der Daten und zugehörigen Abrufvoraussetzungen. So erfasst § 100g Abs. 1 StPO die Daten, die Telekommunikationsunternehmen ganz unabhängig von der Einführung der Vorratsdatenspeicherung bereits geschäfts- und somit nach §§ 96 ff. TKG rechtmäßig speichern.[31] Ein Abruf dieser Daten durch Strafverfolgungsbehörden ist einfacher möglich als derjenige nach § 100g Abs. 2 StPO. Dieser regelt nämlich die Zugriffsvoraussetzungen auf Daten, deren Speicherverpflichtung durch § 113b TKG neu umrissen wurde.

Der Gesetzgeber nutzt die Heranziehung eines Straftatenkatalogs zur Beschränkung der Zugriffsvoraussetzungen auf „Vorratsdaten". Die Einordnung der „Schwere" der Straftat in das abgestufte Intensitätskonzept der StPO (mittlere, schwere, besonders schwere Kriminalität), die im Einzelfall auch schwer wiegen muss, hat sich bewährt.[32] § 100g Abs. 2 StPO fordert – vergleichbar § 100c StPO – eine besonders schwere Straftat. Dieser Bereich der Kriminalität ist dann betroffen, wenn die Folgen der Tat für betroffene Rechtsgüter besonders schwer sind. Bei bestimmten Straftaten ist die hinreichende Schwere auch im Einzelfall schon durch das verletzte Rechtsgut indiziert (Rechtsgutindikation etwa bei Mord und Totschlag), bei anderen bedarf sie der eigenständigen Feststellung, etwa durch einen Straftatenkatalog.[33] Der Gesetzgeber hat diese auf den § 100c StPO gemünzte Rechtsprechung des *BVerfG* aufgegriffen. Im Kern sind „besonders schwere Straftaten" damit solche, die im Höchstmaß mit Freiheitsstrafe von mehr als fünf Jahren Dauer bedroht sind und solche, bei denen der Qualifikationstatbestand mit einer höheren Strafe als fünf Jahre Freiheitsstrafe droht.[34]

§ 100g Abs. 2 StPO knüpft die Erhebung der Daten, die nach § 113b TKG verpflichtend zu speichern sind,[35] an verschiedene Erfordernisse: (1.) Sie sind nur bei Verdacht einer bestimmten, besonders schweren, im Einzelnen aufgezählten Straftat (Straftatenkatalog) zulässig;[36] (2.) die nach § 113b TKG gespeicherten Verkehrsdaten dürfen nur erhoben werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer einer Katalogtat ist; (3.) eine Erhebung darf nur erfolgen, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht (Subsidiaritätsklausel).

Der Straftatenkatalog weist eine Schnittmenge mit den in § 100a Abs. 2 StPO enthaltenen Straftaten auf, ist diesem gegenüber jedoch noch reduziert. Es handelt sich um Straftaten, die der Bekämpfung des Terrorismus oder dem Schutz höchstpersönlicher Rechtsgüter, insbesondere Leib, Leben, Freiheit und sexuelle Selbstbestimmung, dienen und solcher, bei denen Verkehrsdaten nach kriminalistischer Erfahrung besonders wertvoll sind (etwa Verbreitung kinderpornographischer Schriften).

Herauszuheben ist, dass § 100g Abs. 3 StPO eine Sonderregelung zu Funkzellenabfragen enthält. Durch die Legaldefinition der Funkzellenabfrage wird eine normenklare Ermächtigungsgrundlage geschaffen. Funkzellenabfragen, bei denen auf die nach § 96 Abs. 1 TKG gespeicherten Daten zugegriffen werden soll, erfolgen auf der Grundlage von Absatz 3 Satz 1. Hiermit reagiert der Gesetzgeber auf die Intensität der Abfrage und verengt die Zulässigkeit, um die unverhältnismäßige Beeinträchtigung einer Vielzahl von Betroffenen zu vermindern.[37]

In Ergänzung der in § 99 Abs. 2 S. 2 TKG genannten Ausnahme von der Speicherpflicht des § 113b Abs. 2 TKG verbietet § 100g Abs. 4 TKG die Erhebung von Verkehrsdaten in Bezug auf alle in § 53 Abs. 1 S. 1 StPO genannten

---

31 Das *BVerfG* hatte diesen Teil der Vorschrift des § 100g StPO in seinem Urteil nicht beanstandet, insbesondere auch nicht die Erhebung von Verkehrsdaten, welche die Telekommunikationsunternehmen nach Maßgabe der §§ 96 ff. TKG zu geschäftlichen Zwecken speichern. Herauszuheben in Bezug auf den nicht vorratsdatenbezogenen § 100g Abs. 1 StPO ist, dass die Erhebung von Standortdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit zulässig (§100g Abs. 1 S. 1 Nr. 1) ist. Hierdurch differenziert der Gesetzgeber diese sensiblen Daten, die zur Erstellung von Bewegungsprofilen dienen, nach Verwendung für die Zukunft und Vorratsdaten. Konsequenz ist, dass nicht gespeicherte Standortdaten den Behörden nach wie vor im gleichen Umfang wie vor der Neufassung zur Verfügung stehen; auf gespeicherte Standortdaten ist der Zugriff nur noch unter den Bedingungen des Absatzes 2 möglich.

32 Vgl. §§ 100a Abs. 2, 100c Abs. 2, 112 Abs. 3 StPO.

33 Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm – insbesondere etwa durch deren Strafrahmen – einen objektivierten Ausdruck finden (vgl. BVerfGE 109, 279): „Die besondere Schwere der Tat im Einzelfall kann insbesondere durch die faktische Verzahnung mit anderen Katalogstraftaten oder durch das Zusammenwirken mit anderen Straftätern begründet werden"; vor allem organisierte Kriminalität fällt hierunter; vgl. *BVerfG*, Urt. v. 3.3.2004 - 1 BvR 2378/97, 1 BvR 1084/99, Rn. 335.

34 *BVerfG*, Urt. v. 3.3.2004 - 1 BvR 2378/97, 1 BvR 1084/99, Rn. 238, 241.

35 „Daten" ist hier die korrekte Bezeichnung, da der § 113b TKG, wie erläutert, neben Verkehrsdaten auch Bestandsdaten umfasst bzw. im Rahmen der eindeutigen Benutzerkennung umfassen könnte.

36 *BVerfG* und *EuGH* hatten den Anwendungsbereich der Vorratsdatenspeicherung auf schwere Kriminalität beschränkt, vgl. BVerfGE 125, 260 sowie *EuGH*, Urt. v. 8.4.2014, (Digital Rights) C-294/13 und C-594/12, Rn. 60. Eine Generalklausel oder lediglich die Verweisung auf Straftaten von erheblicher Bedeutung reichen hingegen nicht aus. Auch der Gerichtshof der Europäischen Union hat objektive Kriterien gefordert, die den Eingriff in Artikel 7 und 8 der Charta der Grundrechte auf Straftaten beschränken, die im Hinblick auf die betroffenen Grundrechte als hinreichend schwer angesehen werden können, um den Eingriff zu rechtfertigen *EuGH*, (Digital Rights) C-294/13 und C-594/12, Rn. 60.

37 Lesenswert die Begründung als Beispiel dafür, dass der Gesetzgeber explizit versucht, auf Bedenken einzugehen und Missstände pro-aktiv zu korrigieren: „Bei den anordnenden Stellen soll das Bewusstsein dafür geschärft werden, dass es im Rahmen der Verhältnismäßigkeitsprüfung stets einer besonderen Abwägung insbesondere im Hinblick darauf bedarf, dass durch die Funkzellenabfrage in regelmäßig unvermeidbarer Weise Verkehrsdaten Dritter erhoben werden.", BT-Drs.18/5088, S. 32.

Berufsgruppen. Ein grundsätzliches Speicherverbot ist laut Gesetzgeber nicht möglich, da die Liste der Berufsgeheimnisträger permanent aktualisiert werden müsste und dies zudem nicht möglich wäre, weil dynamische IP-Adressen schließlich ständig neu vergeben würden.[38]

Bekannt und bewährt hat sich die Abfederung des Grundrechtseingriffs durch Benachrichtigungspflicht und Richtervorbehalt. Diese finden sich in § 101a StPO.

b) Bewertung

Um es vorabzuschicken: Die Abrufregelung des § 100g Abs. 2 StPO ist verfassungsgemäß. Man könnte fast schon sagen, der Gesetzgeber ist „zu streng" mit sich selbst. Es ist jedoch ein Fingerzeig für die mittlerweile bestehende Sensibilität des Gesetzgebers bei grundrechtsinvasiven Maßnahmen.

aa) Beschränkung auf Verfolgung besonders schwerer Straftaten (defintiv) ausreichend
Praktisch sinnvoll,[39] rechtlich zulässig und gleichsam erfreulich ist, dass der Gesetzgeber die Zugriffsvoraussetzungen heraufsetzt und an den §§ 100a und 100c StPO orientiert. Hiermit wird den Anforderungen des *BVerfG* an die Knüpfung der schweren Kriminalität ausreichend Rechnung getragen; die Regelung ist zweifelsohne verfassungsgemäß.[40]. Es bestehen zudem weitgehende Übereinstimmungen mit § 100c StPO – wie die fast identische Abbildung der § 100c Abs. 2 Nr. 1 lit. a-l und Nrn. 2-7 StPO.[41]

Im Kern besteht nun zwischen Vorratsdatenspeicherung und einem Eingriff in Art. 10 GG durch die Telekommunikationsüberwachung oder ein sonstiges Abhören von Inhalten kein Wertungsunterschied mehr. Dies ist insofern verwunderlich, als dass § 100g Abs. 2 StPO in seiner Intensität nicht über § 100a StPO hinausgeht. Die Möglichkeit zur Erstellung von Bewegungsprofilen ist zwar weiterhin gegeben, doch müsste hierzu über einen viel längeren Zeitraum auf Verkehrsdaten zurückgegriffen werden. 10 Wochen sind wohl kaum ausreichend.[42] Dies kann nun nur noch über eine sukzessive Verknüpfung der nach 10 Wochen zu löschenden Daten erfolgen. Der Aufwand dürfte immens sein. Etwa müssten über verschiedene Richtervorbehalte auch im Rahmen der §§ 113 TKG, 100j StPO immer wieder erneute Anfragen gestellt werden. Eine Zweckentfremdung des Instruments Vorratsdatenspeicherung in einem ungehörigen und mithin verfassungswidrigen Ausmaß durch eine geschickte Abfrage steht nicht zu befürchten.[43]
Umso mehr verwundert vor diesem Hintergrund die Zwecksetzung der Erhebung zur Bekämpfung der „besonders schweren Kriminalität". Hiermit wird neben dem Straftatenkatalog eine Nähe zu § 100c StPO hergestellt, die die praktische Intensität der Vorratsdatenspeicherung nicht herzustellen vermag. Die Beschränkung der Erhebung nach § 100g Abs. 2 StPO auf schwere Straftaten vergleichbar der Regelung des § 100a StPO wäre ebenso verfassungsgemäß. Dies würde auch einen Gleichklang mit den sonstigen (tele)kommunikationsbezogenen Überwachungsmaßnahmen der StPO bedeuten, da die Nähe zu einer Inhaltsüberwachung seinen Widerhall im Wortlaut finden würde. Der Eingriff in Art. 10 GG durch den Zugriff auf Verkehrsdaten wäre als „kleine Schwester" des § 100a StPO richtig verortet.[44]

Im Ergebnis wird nun eine Verkehrsdatenabfrage in den Intensitätskontext einer Inhaltsüberwachung gestellt (Kataloge der §§ 100a und 100c StPO.) und semantisch sogar in den Intensitätskontext des Lauschangriffs (§100c StPO).
bb) Zweifel an der Begründung der „Nichtumsetzbarkeit" eines Speicherverbots für Daten von Berufsgeheimnisträgern
Der Aufwand einer Listenerstellung für ca. 1000 Telekommunikationsanbieter dürfte sich in Grenzen halten, sodass die Begründung des Gesetzgebers mit einem nicht zu vertretenen Aufwand nicht trägt.[45] Richtig ist jedoch, dass eine solche Liste nur bei einer dauerhaften Zuordnung von IP-Adressen sinnvoll ist. Dynamischen IP-Adressen erschweren die Listenerstellung somit immens. Erneut darf man jedoch fragen, ob dieses Argument vor dem Hintergrund der „eindeutigen Benutzerkennung" gem. § 113b Abs. 3 Nr. 2 TKG noch trägt, da hierüber schließlich eine Identifikation erfolgen könnte.

IV. Fazit

Man merkt dem Gesetzgeber das Bemühen an, eine gerichtsfeste Regelung zu schaffen. Dies dürfte mit der strafprozessualen Vorratsdatenspeicherung gelungen sein.[46] Ein fragender Unterton ist im Hinblick auf die Verfassungsmäßigkeit nicht mehr nötig. Endlich!

Der Gesetzgeber versucht sich an der Umsetzung folgender Prämisse: Der Speicherumfang ist unkritisch, soweit

38 Vgl. BT-Drs. 18/5088, S. 33.
39 A.A. *Nachbaur*, ZRP 2016, 215 (216) zum Beispiel des § 89a StGB.
40 Die Verfassungsmäßigkeit des Straftatenkatalogs des § 100a Abs. 2 StPO wurde bestätigt (*BVerfG*, Beschl.v. 12.10.2011, 2 BvR 236/08 = BVerfGE 129, 208). Wobei *Bär* zurecht darauf hinweist, dass der Katalog eher an § 100c StPO angelehnt ist; vgl. Beck-OK StPO, Ed. 24, § 100g StPO, Rn. 31. Dies ist aber unschädlich, da der § 100c StPO noch strengere Voraussetzungen aufweist, als der § 100 StPO. Erst Recht ist § 100g Abs. 2 StPO unter diesen Voraussetzungen verfassungsgemäß.
41 Eingehend hierzu *Bär*, in: Beck OK-StPO, Ed. 24, § 100g StPO, Rn. 32.
42 Der Gesetzgeber erachtet diese Speicherungsdauer als ausreichend, um in der weitaus überwiegenden Anzahl von Ersuchen eine Verfügbarkeit der maßgeblichen Daten sicherzustellen, BT-Drs. 18/5088, S. 37.
43 Gleichzeitig dürfte die Aufdeckung organisierter Kriminalitätsstrukturen oder serieller Tatbegehung hierdurch schwieriger, wenn auch nicht unmöglich werden, durch eine sukzessive Verknüpfung von Erhebungsergebnissen nach § 100g Abs. 2 StPO.
44 So ja auch das *BVerfG,* das ausführte, dass der Eingriff „grundsätzlich nicht geringer wiegt als die inhaltsbezogene Telekommunikationsüberwachung", NJW 2010, 833 (841).
45 *Roßnagel* verweist zu Recht darauf, dass es der BNetzA gem. § 99 II TKG möglich ist eine aktualisierte Liste von Beratungsstellen zu führen und es daher nicht einzusehen ist, warum es bei den anderen Berufsgeheimnisträgern unmöglich sein soll. Bei der Erstellung der Listen könnten die jeweiligen Kammern, Parlamente oder Berufsvereinigungen unterstützen; NJW 2016, 533 (538).
46 S. Beschl. des *BVerfG* zum einstweiligen Rechtschutz, *BVerfG* 1 BvQ 42/15 und *BVerfG* 1 BvR 229/16, ersterer abgedruckt in diesem Heft ab S. 140 ff.

die Abrufvoraussetzungen den Grundrechtsschutz abbilden. Er schießt hierbei jedoch mit dem Willen, eine gerichtsfeste Regelung zu schaffen, über das Ziel hinaus, denn er knüpft die Vorratsdatenspeicherung an Voraussetzungen, die das intensitätsbezogenen Regelungskonzept der StPO in Frage stellen. Der Versuch, ein Ermittlungsinstrument in den Maßnahmenkatalog des 8. Abschnitts der StPO einzuführen, der entsprechend seiner Intensität zwischen der Bestandsdatenauskunft (§ 100j StPO) und der „Inhaltsdatenüberwachung" (§100a StPO) liegt, gelingt systematisch nicht. Nun wird die Vorratsdatenspeicherung konzeptionell bereits auf dem Papier als schwerwiegender Eingriff statuiert, als ein expliziter Zugriff auf Inhalte der Telekommunikation. Der Gesetzgeber beraubt sich hiermit des Gestaltungsspielraums künftiger und dann tatsächlich gravierender Maßnahmen. Die Luft zwischen den jeweiligen Normen in der StPO wird dünner.

Doch selbst dies scheint die Kritiker dieses Instruments nicht zu befriedigen, die sich weiterhin an der Anlasslosigkeit der Speicherung abarbeiten. Getragen wird die Kritik von einer überbordenden Angst und Skepsis gegenüber dem Gesetzgeber. Sie steht unter der Hypothese, dass die Wegmarke zu einem Überwachungsstaat allmählich passiert wird.

Wenngleich die Bastion der Speicherverpflichtung gefallen ist, steht der Schutzwall – die Verankerung einer verfassungsgemäßen Abrufermächtigung – nun robuster denn je möchte man ihnen zurufen.

Dies ist der Ansatzpunkt für eine versöhnliche Erklärung gegenüber den Bedenkenträgern: Die Abrufermächtigung wird nicht gelockert werden. Dies wäre eine schier unlösbare Aufgabe für den Gesetzgeber im Kontext der verfassungsrechtlichen Rahmenbedingungen, die von den Entscheidungen zum Lauschangriff über die Online-Durchsuchung und Vorratsdatenspeicherung ihren Niederschlag in der StPO gefunden haben. Die Eingriffsschwellen über das nun gesetzte Maß abzusenken, wäre der gesetzgeberische Dolchstoß für die Rechtsprechung des *BVerfG*. Die Befürchtungen der Kritiker haben sich insofern einen unmöglichen Entwicklungsschritt von der Realität entfernt.