KriPoZ Kriminalpolitische Zeitschrift JuP

**„Junges Publizieren“**

Seminararbeit von

*Yara von Baeckmann*

# Die Vorratsdatenspeicherung – eine (un-)endliche Geschichte

Ludwig-Maximilians-Universität München
Juristische Fakultät
Prof. Dr. Mark Zöller
Abgabedatum: 11.3.2021

**Inhaltsverzeichnis**

## I. Einleitung

Vielleicht eine Geschichte ohne Ende, doch jedenfalls eine Geschichte mit einem Anfang: dem 15.3.2006. An diesem Tag setzte das Europäische Parlament mit dem Erlass der Richtlinie 2006/24/EG den Startschuss für die bewegte Diskussion über eines der meistumstrittensten Themen im Spannungsfeld zwischen Sicherheit und Freiheit; der Vorratsdatenspeicherung.[1] Die verpflichtende Speicherung bestimmter Verkehrsdaten durch Telekommunikationsdienstanbieter (TKD) auf Vorrat und zum Zwecke der Gefahrenprävention und Strafverfolgung[2] sollte den Gefahren und Problemen entgegentreten, die eine Digitalisierung sämtlicher Lebensbereiche für Strafverfolgung und -prävention mit sich bringt.[3] Und obwohl auch in Deutschland schon Jahre vorher über die Einführung einer solchen Regelung diskutiert worden war,[4] waren es erst die Anschläge in Madrid und London, die zunächst innerhalb kürzester Zeit zum Erlass der Richtlinie,[5] später zum ersten deutschen Gesetz zur Vorratsdatenspeicherung und damit einhergehend immer lauter werdender Kritik führten.[6] Und nicht nur die Öffentlichkeit reagierte mit Skepsis auf das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vom 21.12.2007, auch das *BVerfG* entschied 2010, dass die fraglichen Normen gegen die Verfassung verstießen und insoweit nichtig waren.[7] Noch bevor jedoch der Gesetzgeber ein neues verfassungskonformes Gesetz schaffen konnte, erledigte sich das Problem scheinbar von selbst, erklärte doch der *EuGH* 2014 die EU-Richtlinie diesmal in Bezug auf die Grundrechtecharta der EU ebenfalls für grundrechtswidrig.[8] Nichtsdestotrotz schuf der Bundestag 2015 ein zweites, nicht europarechtlich indiziertes Gesetz zur Vorratsdatenspeicherung.[9] Bereits ein Jahr später setzte der *EuGH* in seinem Urteil zu schwedischen und britischen Bestimmungen einer Vorratsdatenspeicherung neue Schranken,[10] welche das *OVG Münster* zu der Annahme verleitete, das deutsche Gesetz verstoße ebenfalls gegen europäisches Recht.[11] Auch wenn die Bundesnetzagentur daraufhin mitteilte, sie würde keine Durchsetzung der betroffenen Regelungen mehr erstreben, bzw. deren Nichtumsetzung nicht ahnden,[12] trat das Gesetz zum 1.7.2017 in Kraft und verpflichtet bis heute die Provider zur Speicherung.[13] Am 6.10.2020 bekräftigte der *EuGH* seine bisherige Linie grundsätzlich,[14] eine Bewertung der deutschen Rechtslage steht jedoch ebenso aus, wie eine durch das *BVerfG*.[15] Und so bleibt die Frage, wie eine europa- und verfassungsrechtkonforme Regelung in das deutsche Rechtssystem integriert werden könnte, vorerst bestehen. Dieser Frage soll die folgende Arbeit nachgehen, indem auf Basis der aktuellen Rechtslage die meistumstrittensten Problemfelder unter Bezugnahme auf Rechtsprechung von *BVerfG* und *EuGH* näher analysiert, Lösungsansätze sowie Verbesserungsvorschläge herauskristallisiert und insbesondere die Schwierigkeiten einer *EuGH*-konformen Umsetzung behandelt werden.

---

1 *Moser-Knierim,* Vorratsdatenspeicherung. Zwischen Überwachungsstaat und Terrorabwehr, 2013, S. 180; MPI, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten (Gutachten), 2. Fassung (2011), S. 255; *Nelles,* Quo Vadis Vorratsdatensdatenspeicherung, 2014, S. 3.
2 *Moser-Knierim*, S. 139.
3 Vgl. *Münch,* ZRP 2015, 130 (132).
4 *Moser-Knierim*, S. 148, 150.
5 *Moser-Knierim,* S. 150; *Puschke,* ZIS 2019, 308 (310); *Szuba,* Vorratsdatenspeicherung. Der europäische Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, 2011, S. 48.
6 *Bär,* in: KMR-StPO, 97. EL (2020), vor §§ 100a-100g Rn. 6; vgl. *Moser-Knierim*, S. 164.
7 BVerfGE 125, 260 (358).
8 *EuGH*, Urt v. 8.4.2014, C-293/12 und C-594/12, ECLI:EU:C:2014:238-Digital Rights (*EuGH*, Digital Rights), Rn. 25.
9 Gesetz zur Einführung einer Speicherfrist und Höchstspeicherfrist von Verkehrsdaten vom 10.12.2015.
10 *EuGH*, Urt. v. 21.12.2016, C-203/15 und C-698/15, ECLI:EU:C:2016:970 -Tele2 (*EuGH*, Tele2).
11 *OVG Münster*, NVwZ-RR 2018, 43 (48).
12 *Wolter/Greco,* in: SK-StPO, 5. Auflage (2018), § 100g Rn. 19c.
13 *Wolter/Greco,* in: SK-StPO, § 100g Rn. 19c.
14 *EuGH*, Urt. v. 6.10.2020, C-511/18, C-512/18 und C-520/180, ECLI:EU:C:2020:791-La Quadrature du Net (*EuGH*, La Quadrature du Net); *EuGH*, Urt. v. 6.10.2020, C-623/17, ECLI:EU:C:2020:790-Privacy International (*EuGH*, Privacy International).
15 Rechtshängig beim *BVerfG*: 1 BvR 141/16, 1 BvR 229/16, 1 BvR 2023/16, 1 BvR 2683/16, 1 BvR 2821/16; beim *EuGH*: C-793/19.

## II. Vorbemerkungen

### *1. Überblick über die Regelungssystematik des § 100g StPO*

Die Regelung der Datenspeicherung und -erhebung zum Zwecke der Strafverfolgung wird primär durch das Zusammenspiel von § 100g StPO mit Normen des Telekommunikationsgesetzes (TKG) bestimmt. § 100g Abs. 1 StPO regelt hierbei zum einen die Datenerhebung in Echtzeit, zum anderen - unter Ausschluss von Standortdaten - den Zugriff auf Verkehrsdaten, die im Rahmen des § 96 Abs. 1 TKG von TKD zu Abrechnungszwecken oder zur Störungsbeseitigung gespeichert werden dürfen. Diese Art der Datenspeicherung und Abfrage beanstandet das *BVerfG* in seiner Entscheidung nicht.[16] Da jedoch die Speicherdauer im Rahmen des § 96 Abs. 1 TKG meist sehr kurz ist[17] und gerade bei Flatrates eine derartige Speicherung häufig gar nicht erfolgt,[18] sind die gewünschten Daten oftmals nicht verfügbar. Diese Lücke sollte § 113b TKG schließen, indem er die in § 113a TKG genannten TKD zur Aufbewahrung bestimmter Daten auf Vorrat verpflichtet.[19] § 113b TKG bildet somit die Grundlage der Vorratsdatenspeicherung. § 100g Abs. 2 StPO bestimmt, inwieweit auf diese Daten im Rahmen der Strafverfolgung zurückgegriffen werden darf. Voraussetzung für eine Erhebung der gespeicherten Daten ist demnach, dass es sich bei der fraglichen Tat um eine Katalogtat des Absatz 3 handelt, welche auch im Einzelfall besonders schwer wiegt, die Abfrage verhältnismäßig ist und eine Ermittlung des Aufenthaltsortes des Beschuldigten oder die Aufklärung des Sachverhalts ohne Erhebung zumindest wesentlich erschwert wäre. § 100g Abs. 3 StPO normiert die Funkzellenabfrage, bei der alle bei einer Funkzelle innerhalb eines bestimmten Zeitraums angefallenen Daten erhoben werden. Satz 2 regelt dabei die Erhebung von Daten, die nach § 113b TKG auf Vorrat gespeichert wurden. Da § 113b TKG jedoch keine Speicherung von Funkzellendaten vorsieht, kann es nach aktueller Gesetzeslage nicht zu einer Speicherung oder Erhebung gespeicherter Funkzellendaten kommen.[20] Aus diesem Grund soll die Funkzellenabfrage aus den folgenden Überlegungen ausgeklammert werden. Das Hauptaugenmerk liegt somit auf den §§ 113a, 113b TKG und § 100g Abs. 2 StPO.

### *2. Vorbemerkungen zur Rechtsprechung von BVerfG und EuGH*

In seiner Entscheidung vom 2.3.2010 prüfte das *BVerfG* eine Vereinbarkeit der §§ 113a, 113b TKG a.F. und § 100g StPO a.F. mit Art. 10 und 12 GG. Während es einen Verstoß gegen Art. 12 GG recht pauschal ablehnte,[21] widmete es Art. 10 GG – welcher Art. 2 Abs. 2 i.V.m. Art. 1 Abs. 1 verdränge - eine ausführliche Prüfung, in deren Rahmen es zu dem Ergebnis kam, die Normen stellten einen unverhältnismäßigen Eingriff dar.[22] Der *EuGH* wählte als Prüfungsmaßstab für seine Kontrolle der Richtlinie 2006/24/EG und der nationalen Gesetzgebung einzelner Mitgliedsstaaten Art. 7, 8 und 11 GrCh sowie die Richtlinie 2002/58/EG.[23] Sowohl *BVerfG* als auch *EuGH* sahen in der Speicherung von Daten durch die TKD und in der Erhebung durch die Strafverfolgungsbehörden jeweils einen selbstständigen Grundrechtseingriff.[24] Die Speicherung allein könne schon „ein diffus bedrohliches

16 BVerfGE 125, 260 (328).
17 BT-Drs. 17/1482, S. 3; *Wolter/Greco,* in: SK-StPO, § 100g Rn. 8.
18 *Wolter/Greco,* in: SK-StPO, § 100g Rn. 8.
19 BT-Drs. 17/1482, S. 3.
20 *Bär,* in: BeckOK-StPO, 37. Ed. (2020), § 100g Rn. 44.
21 Siehe BVerfGE 125, 260 (358 f.).
22 BVerfGE 125, 260 (358).
23 *EuGH*, Digital Rights, Rn. 25; *EuGH*, Tele2, Rn. 122, 125.
24 *EuGH*, Digital Rights, Rn. 34.

Gefühl des Beobachtetseins“[25] hervorrufen, welches die freie Wahrnehmung der Grundrechte beeinflusse. Beide Gerichte erklärten eine Vorratsdatenspeicherung nicht für per se rechtswidrig, betonten jedoch ihre Eingriffsintensivität sowie die besondere Sensibilität des Themas und stellten mehr oder minder genaue Anforderungen an nationale Regelungen.[26]

## III. Zur Ausgestaltung im Einzelnen

### *1. Datenkategorien*

Zunächst empfiehlt sich ein Blick darauf, welche Arten der Information von der Vorratsdatenspeicherung umfasst werden. Das TKG unterscheidet zwischen Bestands-, Inhalts- und Verkehrsdaten. Bestandsdaten sind Kundendaten, welche TKD im Rahmen des Vertragsverhältnisses erheben,[27] und deren staatliche Verwertung die §§ 112, 113 TKG regeln. Der Begriff „Verkehrsdaten“ bezeichnet die Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.[28] Inhaltsdaten schließlich geben Aufschluss über den Inhalt einer Kommunikation.[29] § 113b TKG beschränkt die Vorratsdatenspeicherung auf Verkehrsdaten. Während *BVerfG* und *EuGH* in der Speicherung von Inhaltsdaten einen nicht zu rechtfertigenden Eingriff in den Wesensgehalt des Art. 10 GG[30] bzw. Art. 7, 8 GrCh sehen,[31] kritisieren sie die Speicherung von Verkehrsdaten grundsätzlich nicht.[32] Der Katalog des § 113b TKG ist somit wohl grundrechtskonform. Nichtsdestotrotz empfiehlt sich in Hinblick auf etwaiges Verbesserungspotential ein näherer Blick auf die zu speichernden Datenkategorien.

#### *a) Internetnutzung*

Die erste Kategorie sind hierbei die Internetnutzungsdaten. Diese umfassen die eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, eine zugewiesene Benutzerkennung und den Zeitraum der Nutzung sowie die verwendete Internetprotokoll-Adresse (IP-Adresse). [33] Aus Effizienzgründen werden IP-Adressen meist nicht fest, sondern zeitlich begrenzt vergeben und stetig ausgetauscht (dynamische IP-Adresse).[34] Unter Zuhilfenahme von Informationen bezüglich Anschluss, Anschlussinhaber und Nutzungszeit kann ihre Kenntnis die Zuordnung ansonsten anonymer Aktivitäten zu einzelnen Anschlussinhabern ermöglichen.[35] Gerade im Bereich der Internetkriminalität können Internetnutzungsdaten so entscheidende Anhaltspunkte zur Aufklärung von Straftaten liefern.[36] Unmöglich bleibt jedoch die Feststellung, wer zu dem konkreten Zeitpunkt den betroffenen Anschluss genutzt hat.[37] Typischerweise erfolgt die Ermittlung im Ausgangspunkt von der Aktivität (bspw. dem Verfassen eines Kommentars) hin zum Nutzer und ermöglicht somit nur punktuelle Einblicke in das Verhalten desselben.[38] Die Erstellung eines umfassenden Persönlichkeitsprofils durch umgekehrte Ermittlung, d.h. das Ansetzen beim

25 BVerfGE 125, 260 (320).
26 BVerfGE 125, 260 (316 f.); *EuGH*, Tele2, Rn. 103 ff.
27 Siehe § 3 Nr. 3 TKG.
28 § 3 Nr. 30 TKG.
29 *Moser-Knierim*, S. 290.
30 BVerfGE 125, 260 (322).
31 *EuGH*, Tele2, Rn. 101.
32 *EuGH*, Tele2, Rn. 108; BVerfGE 125, 260 (316).
33 Art. 13b Abs. 3 Nr. 1-3.
34 *Freude,* Technische Fragen der Vorratsdatenspeicherung. Kurzgutachten für die SPD-Bundestagsfraktion (Gutachten), 2011, S. 8 f.; *Zöller,* GA 2007, 393 (406).
35 *Freude*, S. 20 f.
36 BVerfGE 125, 260 (343).
37 *Alsbih,* DuD 2011, 482.
38 *Freude*, S. 21.

Nutzer und die von dort folgende Abfrage aller je benutzten IP-Adressen und damit verbundener Aktionen ist insbesondere, da besuchte Webseiten von den TKD nicht mit gespeichert werden,[39] aufwendig und wenig erfolgversprechend, nichtsdestotrotz technisch möglich[40] und nicht zu unterschätzen.[41]

*b) Sonderfall Portnummern*

Besondere Probleme ergeben sich dort, wo, wie bei Hotspots oder WLANs, eine IP-Adresse durch mehrere Personen benutzt wird, da hier eine eindeutige Zuordnung von einer Aktion zum Handelnden nicht möglich ist.[42] Mitunter wird vorgeschlagen, nunmehr auch Portnummern, welche bisher von der Speicherpflicht ausgenommen waren,[43] jedoch eine eindeutige Zuordnung ermöglichen würden, in den Katalog des § 113b aufzunehmen.[44] Wenn nämlich der Zweck der Vorratsdatenspeicherung in Bezug auf IP-Adressen häufig gar nicht erfüllt werden kann, ist fraglich, ob hier eine Speicherung derselben überhaupt noch zu rechtfertigen ist. Der Wunsch, Portnummern in den Katalog des § 113b TKG aufzunehmen,[45] ist somit nachvollziehbar. Die Idee findet ihre Grenzen jedoch in der Realität. Auch unter Zuhilfenahme der Portnummer kann der Anschlussinhaber nur bei Kenntnis derselben ermittelt werden. Die Portnummern sind den Ermittlern in der Praxis allerdings meist gerade nicht bekannt, da Webseitenbetreiber sie in der Regel nicht speichern.[46] Die Vorratsdatenspeicherung von Portnummern hieße somit einen tiefgreifenden Eingriff mit hohem technischen Aufwand bei gleichzeitig geringem Nutzen.[47]

*c) Telefonverkehr*

Eine weitere Kategorie von Daten sind Informationen zum Telefonverkehr inklusive SMS und MMS. Details über Kommunikationspartner und -zeiten lassen mitunter Schlüsse auf Inhalte der Kommunikation zu und können Auskunft über Persönlichkeits- und persönliche Merkmale des Nutzers verschaffen.[48] Gleichzeitig unterstützen auch diese Daten eine Aufklärung und waren nach Aussagen von Ermittlern jedenfalls um das Jahr 2010 besonders in Bereichen organisierter Kriminalität nach wie vor wesentlich.[49] Es ist anzunehmen, dass die Bedeutung dieser Kommunikationsarten in den letzten Jahren abgenommen hat und in den kommenden Jahren noch weiter sinken wird.[50] Es ist jedoch auch mehr als wahrscheinlich, dass im Falle einer Ausklammerung aus der Speicherungspflicht, Kriminelle wieder auf diese traditionelle Form der Kommunikation zurückgreifen würden und die restliche Vorratsdatenspeicherung ineffektiv, wenn nicht sogar obsolet, würde.

*d) Standortdaten*

Die letzte Kategorie des § 113b TKG bilden sog. Standortdaten. Sie geben Aufschluss über den Aufenthaltsort

39 § 113b Abs. 5 TKG.
40 *Freude*, S. 21.
41 *Roßnagel et al.*, Interessensausgleich im Rahmen der Vorratsdatenspeicherung. Analyse und Empfehlungen, 2013, S. 133.
42 *Alsbih,* DuD 2011, 482 (483).
43 BNetzA, Häufig gestellte Fragen zur Speicherung und Übermittlung von speicherpflichtigen Verkehrsdaten nach den §§ 113a und 113b TKG, 2017, S. 5.
44 *Rudl*, Portnummern im NetzDG. Sinnlose Datenflut statt gezielter Ermittlungen, Netzpolitik 16.3.2020, abrufbar unter: https://netzpolitik.org/2020/sinnlose-datenflut-statt-gezielte-ermittlungen/ (zuletzt abgerufen am 12.10.20).
45 MPI, S. 160.
46 *Freude*, S. 23.
47 *Freude*, S. 23.
48 BVerfGE 125, 260 (319).
49 MPI, S. 138.
50 MPI, S. 138.

einer bestimmten Person, indem sie den Aufenthalt des Endgeräts eines Endnutzers in einer bestimmten Funkzelle bei Beginn der Verbindung bestätigen.[51] Die höhere Sensibilität dieser Daten begründet sich darin, dass sich mit ihrer Hilfe komplexe Bewegungsprofile erstellen lassen.[52] Auch ermöglichen sie so viele Rückschlüsse auf eine Person, dass bereits vier zufällig gewählte Standorte ausreichen, um 95% der Individuen zu identifizieren.[53] Dieser höheren Sensibilität hat der Gesetzgeber Beachtung geschenkt, indem er die Speicherdauer im Vergleich zu den Informationen zu Internet und Telekommunikation von 10 auf 4 Wochen herabgesetzt hat.

*e) E-Mailverkehr*

Ausgenommen aus der Speicherpflicht sind Daten bezüglich des E-Mailverkehrs. In der Gesetzesbegründung finden sich hierfür keine weiteren Erklärungen bis auf die Beschränkung des § 113b TKG auf das Notwendige.[54] Wieso jedoch die Speicherung von Verkehrsdaten von SMS notwendiger sein sollten als die von E-Mails, ist nicht ersichtlich.[55] Schon seit einigen Jahren haben E-Mails vielmehr größere Bedeutung als SMS,[56] eine Einbeziehung in den Anwendungsbereich des § 113b TKG ist somit durchaus denkbar.[57] Parallel zu den Regelungen bezüglich SMS könnten hierbei Postfach von Sender und Empfänger sowie Datum und Uhrzeit von Versendung und Empfang gespeichert werden.[58]

*f) Over-the-top-Telekommunikationsdienstleistungen*

Es ist umstritten, ob die §§ 113a ff. TKG auch sog. Over-the-top-Telekommunikationsdienste (OTT-TKD), d.h. Telekommunikationsdienste, die wie WhatsApp oder Threema über das Internet erbracht werden,[59] verpflichten.[60] Gerade in den letzten Jahren nahmen diese OTT-TKD im Vergleich zu herkömmlichen Telekommunikationsdiensten maßgeblich an Relevanz zu.[61] In seinem Referentenentwurf zum Telekommunikationsmodernisierungsgesetz (TKMoG)[62], nimmt der Gesetzgeber die OTT-TKD jedoch explizit aus dem Anwendungsbereich des § 175, der dem jetzigen § 113b TKG entspricht, heraus.[63] Dies spräche dafür, dass auch nach jetzigem Stand OTT-TKD nicht einbezogen werden sollten. Ob dies aus Effektivitätsgründen sinnvoll ist, bleibt zweifelhaft, die Eingriffsintensität der Vorratsdatenspeicherung wird hierdurch jedoch deutlich abgemildert.

51 § 3 Nr. 19 TKG.
52 BT-Drs. 18/5088, S. 27; *Hensel,* DuD 2009, 527 (528).
53 *De Montjoye et al.,* Unique in the Crowd. The privacy bounds of human mobility, Scientific Report 2013, abrufbar unter: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3607247/ (zuletzt abgerufen am 12.10.20).
54 BT-Drs. 18/5088, S. 23.
55 *Bär,* in: BeckOK-StPO, § 113b TKG Rn. 18.
56 Vgl. *Bulowski,* Regulierung von Internetkommunikationsdiensten. Zur Anwendbarkeit des Telekommunikationsrechts auf Voice over IP, Instant Messaging und E-Mail-Dienste, 2019, S. 31.
57 Vgl. *Bär,* in: BeckOK-StPO, § 113b TKG Rn. 18.
58 Vgl. § 113a Abs. 3 TKG a.F.
59 BNetzA, Nutzung von OTT-Kommunikationsdiensten in Deutschland. Bericht 2020, S. 5.
60 *Mayen,* in: Scheurle/Mayen, 3. Auflage (2018), § 113a Rn. 3.
61 BNetzA (Fn. 59), S. 5.
62 BMWi/BMVI, Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts, 14.12.20, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/telekommunikationsmodernisierungsgesetz-referentenentwurf-20201612.pdf?__blob=publicationFile&v=8 (zuletzt abgerufen am 10.3.21).
63 A.a.O., § 175 Abs. 1 TKG-E.

*2. Zweck der Speicherung*

*a) Verfolgung von Straftaten*

Nach dem Grundsatz der Datenzweckbindung dürfen Daten in der Regel nur zu vorher festgelegten Zwecken gespeichert werden.[64] Gemäß Art. 15 Abs. 1 S. 1 RL 2002/58/EG darf eine Datenspeicherung nur erfolgen, wenn sie für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen notwendig, angemessen und verhältnismäßig ist. § 100g StPO i.V.m. § 113b regelt gerade die Verfolgung von Straftaten, so dass die Regelung bezüglich der Zwecksetzung ohne Weiteres als europarechtskonform gelten kann. Auch nach Vorgabe des *BVerfG* kann eine Vorratsdatenspeicherung zum Zwecke der Strafverfolgung erfolgen.[65]

*b) Sonderfall § 100j StPO*

Andere Anforderungen stellt das *BVerfG* in Bezug auf die Personenauskunft zu dynamischen IP-Adressen. Hierbei können Ermittler eine Auskunft über Bestandsdaten nach §§ 95, 111 TKG anhand dynamischer IP-Adressen fordern. Die Ermittler erhalten so selbst keinen Zugriff auf Verkehrsdaten, für eine Auskunft müssen jedoch die TKD eben solche Verkehrsdaten auswerten.[66]

*aa) Beurteilung durch das BVerfG*

Das *BVerfG* sieht hierin aus mehreren Gründen einen schwächeren Eingriff in Art. 10 Abs. 1 GG. Zum ersten erhielten die Behörden selbst keinen Zugriff auf die sensiblen Verkehrsdaten.[67] Darüber hinaus bleibe der Erkenntniswert verhältnismäßig gering[68] und der Ausschnitt der Daten, die verwendet werden müssten, sehr klein.[69] Daraus leitet das *BVerfG* ab, dass ein solches Auskunftsersuchen sogar zur Verfolgung von „besonders gewichtigen Ordnungswidrigkeiten“ möglich sei.[70] Der Gesetzgeber hat auf diese Möglichkeit zwar verzichtet, so dass Ordnungswidrigkeiten gemäß § 46 Abs. 2 OWiG gänzlich vom Anwendungsbereich des § 100j Abs. 2 ausgeschlossen sind. Dennoch sind die Anforderungen des § 100j Abs. 1, 2 deutlich geringer als die des § 100g StPO.

*bb) Kritik*

Die Einschätzung durch das *BVerfG* ist keineswegs unproblematisch. Für das Datenmengenargument gilt, dass eine gezielte Abfrage nur einer Verbindungsinformation ebenfalls eine deutlich geringere Menge an Daten verlangt, als die umfassende Vorratsdatenspeicherung bereithält. Doch gerade die Menge an Möglichkeiten dieser für sich genommen wenig datenintensiven Erhebungen ist es, die die Sensibilität der Speicherung und damit hohen Voraussetzungen an die strafprozessuale Verwertung, sei sie im Rahmen von § 100g Abs. 2 oder § 100j Abs. 2 StPO, begründet. Auch das Argument des fehlenden Verkehrsdatenzugriffs durch Behörden überzeugt nur begrenzt. Wenn das *BVerfG* in jeder Verwertung der Daten einen Eingriff[71] sieht und dem Gesetzgeber

64 Art. 6 Abs. 1 lit. c Datenschutzrichtlinie 95/46/EG; BVerfGE 65, 1 (46).
65 Vgl. BVerfGE 125, 260 (328).
66 *Bär,* MMR 2013, 700 (701).
67 BVerfGE 125, 260 (340 f.).
68 BVerfGE 125, 260 (340 f.).
69 BVerfGE 125, 260 (341).
70 BVerfGE 125, 260 (344).
71 BVerfGE 125, 260 (312 f.).

die Speicherung der Daten durch Unternehmen als unmittelbaren Eingriff zurechnet,[72] ist unklar, warum die Verwertung durch dieselben weniger eingriffsintensiv sein sollte als durch die Strafverfolgungsbehörden. Denkbar wäre eine geringere Intensität lediglich deshalb, da die Daten bei den TKD durch die Speicherung sowieso schon vorliegen und durch die Auswertung keine neue Institution Zugriff auf Verkehrsdaten erhält.[73] Zu bezweifeln bleibt auch der geringere Erkenntniswert. Inwieweit der Erkenntniswert, welche Rufnummer es war, die A zu einer bestimmten Zeit angerufen hat, höher sein soll als der, dass Person A es war, die zu einem bestimmten Zeitpunkt eine bestimmte IP-Adresse benutzt hat, bleibt unklar. In beiden Fällen können unter Kenntnis einer weiteren Information (der IP-Adresse zuzuordnende Aktion und Besitzer der Rufnummer) Rückschlüsse auf Aktions- bzw. Telekommunikationsinhalt gezogen werden. Überzeugender ist insoweit das Argument des *EuGH*, der Wert von IP-Adressen für Strafverfahren wäre besonders hoch.[74] Dies ändert jedoch nichts daran, dass die Verwertung von IP-Adressen per se sehr eingriffsintensiv ist, ermöglichen sie doch ebenso tiefe Einblicke in Person und Persönlichkeit wie andere Formen der Telekommunikation.[75] Vor diesem Hintergrund wirken die milden Vorgaben des *BVerfG* und die halbherzige Umsetzung durch den Gesetzgeber unbefriedigend.[76] Zumindest eine geringe Anhebung der Eingriffsvoraussetzungen, bspw. auf die des § 100g Abs. 1 StPO, wäre wünschenswert.

*3. Zweck der Erhebung*

Das *BVerfG* fordert eine klare Begrenzung des Anwendungsbereichs des § 100g Abs. 2 StPO auf Straftaten gegen überragend wichtige Rechtsgüter.[77] Auch wenn sich viele Ermittler eine dem § 100g Abs. 1 StPO vergleichbare Regelung gewünscht hätten,[78] welcher nicht nur leichte Straftaten umfasst, solange sie durch Telekommunikation erfolgen (Nr. 2), sondern auch einen größeren Spielraum bezüglich der zu verfolgenden besonders schweren Tat lässt (Nr. 1), hat das *BVerfG* solche Generalklauseln für § 100g Abs. 2 unmissverständlich untersagt.[79] Das Gesetz von 2015 kommt den Anforderungen des Gerichts nach, indem es den Anwendungsbereich des § 100g Abs. 2 StPO auf einen exklusiven Straftatenkatalog beschränkt.[80]

*4. Datensparsamkeit/ Begrenzung auf das absolut Notwendige*

Um die Schwere der Grundrechtseingriffe auf ein Minimum zu reduzieren,[81] müssen die Speicherung und Verwendung von Daten immer auf das absolut Notwendige begrenzt bleiben.[82] Indem der Gesetzgeber enge Voraussetzungen an die Erforderlichkeit der Erhebung und die Begründung derselben setzt,[83] erfüllt er diesen Grundsatz in Bezug auf die Verwertung. Anders präsentiert sich die Situation jedoch bezüglich der Speicherung von Daten. Fraglich ist bspw., ob eine Einbeziehung reiner Geschäftskundenanbieter in die Speicherpflicht, in Anbetracht ihrer geringen Bedeutung für die Aufklärung von Straftaten nach § 100g Abs. 2 StPO, als erforderlich betrachtet

72 BVerfGE 125, 260 (311).
73 Vgl. *BVerfG*, NJW 2020, 2699 (2713).
74 *EuGH*, La Quadrature du Net, Rn. 152.
75 *EuGH*, La Quadrature du Net, Rn. 153.
76 Vgl. *Greco,* in: SK-StPO, § 100j Rn. 4; *Hauck,* in: LR-StPO, 27. Auflage (2019), § 100j Rn. 15; *Nelles*, S. 223.
77 BVerfGE 125, 260 (328).
78 MPI, S. 160.
79 BVerfGE 125, 260 (329).
80 BT-Drs. 18/5088, S. 24.
81 *Nelles*, S. 35.
82 *EuGH*, Tele2, Rn. 96.
83 Vgl. §§ 100g Abs. 2 S. 1, 101a Abs. 2.

werden kann.[84] Darüber hinaus sollte möglichst keine doppelte Speicherung erfolgen. In Anlehnung an Erwägungsgrund 13 S. 2 der ehemaligen Richtlinie entschied sich der deutsche Gesetzgeber, nur TKD, nicht auch die Netzbetreiber zu verpflichten. Eine Mehrfachspeicherung ergibt sich dennoch in den Fällen, in denen die Kommunikationspartner Kunden unterschiedlicher TKD sind. Hier speichern beide Unternehmen die identischen Daten. Eine Möglichkeit, dies zu vermeiden, wäre die individuelle Verpflichtung nur einzelner TKD durch die Bundesnetzagentur.[85] Dies hätte außerdem den Vorteil, dass bei einer Fokussierung auf die großen Unternehmen höhere Sicherheitsstandards gewährleistet und Kosten gespart werden könnten.[86] Gleichzeitig würde es allerdings zwangsläufig dort zu Lücken führen, wo beide Kommunikationspartner über nichtverpflichtete Unternehmen agieren. Dies wäre nicht nur aus Gleichbehandlungsgesichtspunkten problematisch, sondern würde auch unter Umständen das Notwendige unterschreiten. Um diese Lücken zu vermeiden, müsste in jedem Einzelfall oder für jede Kombination von Dienstanbietern eine Regelung getroffen werden, was in Anbetracht der rund 2500 Anbieter,[87] und damit über 6 Millionen möglicher Kombinationen, eine schier nicht zu bewältigende Aufgabe sein dürfte. Deutlich zweckdienlicher und unkomplizierter scheint es, die Speicherpflicht auf den TKD des Absenders zu beschränken.[88]

*5. Technische Ausgestaltung*

Besonders detaillierte Vorgaben machen *BVerfG* und *EuGH* in Bezug auf die technische Ausgestaltung der Vorratsdatenspeicherung.[89] Dies ist kaum verwunderlich in Anbetracht der Tatsache, dass einer der größten Kritikpunkte die Möglichkeit des Zugangs und Missbrauchs der hochsensiblen Daten durch TKD, den Staat oder Dritte ist.[90] Unter anderem verlangt das *BVerfG*, dass die zutreffenden Sicherheitsvorkehrungen stets an den Stand der Technik angepasst werden und eine Speicherung dezentral bei den Unternehmen erfolgt.[91] Der Gesetzgeber ist dem in seinem Neuentwurf 2015 nachgekommen und hat alle wesentlichen Vorgaben des *BVerfG* eingearbeitet.[92] Lediglich § 101a Abs. 3 StPO, welcher in seinem Anwendungsbereich bisher auf „personenbezogene Daten" beschränkt ist, müsste sprachlich korrigiert werden, um sicherzustellen, dass sich die vom *BVerfG* geforderte Kennzeichnungs- und Löschungspflicht auf alle Verkehrsdaten bezieht.[93] Gerade kleinere Unternehmen dürften Schwierigkeiten haben, die technischen Anforderungen zu erfüllen.[94] Noch vor Verabschiedung des Gesetzes kritisierte der IT-Branchenverband *Eco*, die vorgesehene Speicherung auf vom Internet entkoppelten Rechnern und eine schnelle Übermittlung der geforderten Daten an die Polizei unter Einhaltung der geforderten komplizierten Verschlüsselung seien nicht umsetzbar.[95] Die *BNetzA* stellte jedoch klar, dass die Verschlüsselung nur so komplex sein müsse, dass eine effektive Abfrage noch möglich sei, und schlägt eine transparente Datenbankverschlüsselung

84 *Roßnagel et al.* (Fn. 41), S. 141.
85 *Roßnagel et al.* (Fn. 41), S. 141.
86 *Roßnagel et al.* (Fn. 41), S. 145.
87 *Greis*, Kritik an Gesetzentwurf. Eco hält Vorratsdatenspeicherung für nicht umsetzbar, Golem 20. Mai 2015, abrufbar unter: https://www.golem.de/news/eco-kritik-an-gesetzentwurf-vorratsdatenspeicherung-ist-technisch-nicht-umsetzbar-1505-114166.html (zuletzt abgerufen am 13.10.20).
88 *Roßnagel et al.* (Fn. 41), S. 140.
89 Vgl. BVerfGE 125, 260 (325 ff.).
90 Vgl. BVerfGE 125, 260 (318).
91 BVerfGE 125, 260 (321, 326).
92 Vgl. §§ 113d-g TKG.
93 *Kleen/Riegler,* AL 2017, 59 (63).
94 *Roßnagel et al.* (Fn. 41), S. 144.
95 *Greis* (Fn. 87).

oder eine Container-Verschlüsselung auf Basis des *Advanced Encryption Standards* vor.[96] Eine den aktuellen Gesetzesvorgaben genügende Verschlüsselung scheint somit durchaus möglich zu sein. Darüber hinaus gesteht die *BNetzA* ein, dass eine vollständige Abkopplung vom Internet nicht möglich sei und eine Sicherung gegen Zugriffe durch *Fire-Walls* genüge.[97] Da hier jedoch nicht wirklich von einer „Entkoppelung" gesprochen werden kann, ist der Gesetzestext insoweit anzupassen. Da das *BVerfG* entkoppelte Speicher nur als mögliche, nicht zwingende Maßnahme erachtet,[98] ist dies ohne Weiteres möglich. Kritisiert wird weiterhin, dass nach wie vor keine routinierte, flächendeckende Überprüfung der Umsetzung von Sicherheitskonzepten erfolgt, sondern sich die *BNetzA* auf eine Überprüfung des Sicherheitskonzeptes selbst und einzelne stichprobenartige Überprüfungen beschränkt.[99] Nur wenn regelmäßige, verdachtsunabhängige Kontrollen zur Einhaltung der technischen Anforderungen durchgeführt werden, kann jedoch der Schutz hochsensibler Daten ausreichend sichergestellt werden.[100] Darüber hinaus muss bei Zuwiderhandlung eine effektive Sanktionierung erfolgen.[101] Das *BVerfG* empfiehlt die Festlegung von Sanktionen, um die Sicherheit der Daten zu gewährleisten, betont allerdings zugleich den großen Spielraum des Gesetzgebers diesbezüglich,[102] welcher dementsprechend noch keine Repressalien festgelegt hat. Dies sollte möglichst bald nachgeholt werden. Kaum geregelt ist die Speicherung und Sicherung der Daten bei den Ermittlungsbehörden.[103] Aus datenschutzrechtlichen Erwägungen sollte und darf hier jedoch nichts anderes gelten als für die Speicherung bei den TKD.[104]

*6. Kostentragung*

Nach aktueller Gesetzeslage werden die Kosten der Speicherung von den TKD selbst getragen, solange keine unbilligen Härten entstehen.[105] Nur bei der Datenübermittlung und Auskunftserteilung entstehende Kosten werden gemäß § 23 JVEG ersetzt. Das *BVerfG* beurteilt eine Kostentragung durch die Unternehmen nicht als unverhältnismäßig, beschränkt sich jedoch bei der Analyse möglicher Kostenpunkte auf die Bereitstellung technischer Infrastruktur, über welche die TKD zu großen Teilen schon verfügten.[106] Das Gericht verkennt hierbei jedoch, dass die Sicherheitsanforderungen an die auf Vorrat zu speichernden Daten deutlich höher sind als für die schon früher gemäß §§ 96, 111 TKG gesammelten. So verwundert es kaum, dass die IT-Branchenverbände *Bitkom* und *Eco* mit Mehrkosten in Höhe von 200 bis 600 Millionen Euro rechnen.[107] Besonders kleinere Unternehmen, die mit Kosten von bis zu 80 000 Euro rechnen müssten, drohe deswegen die Insolvenz.[108] Es finden sich folglich viele Befürworter einer zumindest teilweisen Kostentragung.[109] Mitunter wird die Kostentragung durch die TKD sogar als verfassungswidrig erachtet.[110] Eine Kostenübernahme durch den Staat überzeugt vor allem unter dem Gesichtspunkt, dass die Strafverfolgung zu dem Kern staatlicher Aufgaben zählt, so dass, wird die Aufgabe schon nicht

96 BNetzA, Anforderungskatalog nach § 113f TKG. Katalog von technischen Vorkehrungen und sonstigen Maßnahmen zur Umsetzung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, BGBl. I S. 2218, 10.12.2015, S. 15.
97 BNetzA (Fn. 96), S. 17.
98 BVerfGE 125, 260 (325 f.).
99 Siehe §§ 113f Abs. 2 S. 3 iVm 109 Abs. 7 S. 1 TKG; vgl. G*ärtner/Kipker,* DuD 2015, 593 (594).
100 G*ärtner/Kipker,* DuD 2015, 593 (594).
101 *Roßnagel et al.* (Fn. 41), S. 149.
102 BVerfGE 125, 260 (339).
103 G*ärtner/Kipker,* DuD 2015, 593 (596).
104 Vgl. *Roßnagel et al.,* DuD 2009, 536 (538).
105 § 113a TKG.
106 BVerfGE 125, 260 (361 f.).
107 *Greis* (Fn. 87); BT-Drs. 249/15.
108 *Greis* (Fn. 87).
109 *Freiling,* Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, Technischer Bericht TR-2009-005 Universität Mannheim Institut für Informatik, 2009, S. 23; G*ärtner/Kipker,* DuD 2015, 593 (595); *Roßnagel et al.* (Fn. 41), S. 154.
110 *Nelles,* S. 285.

durch ihn wahrgenommen, sie doch zumindest von ihm finanziell getragen werden sollte.[111] Erstrebenswert wäre eine Kostenübernahme zu nur 80%, um die Sparsamkeit der Unternehmen zu gewährleisten, und die Kostentragung von der Erfüllung der Sicherheitsvorgaben abhängig zu machen.[112]

*7. Berufsgeheimnisträger*

Mitunter wird kritisiert, die Vorratsdatenspeicherung verringere die Bereitschaft, Kommunikation innerhalb bestimmter Vertrauensbeziehungen wahrzunehmen.[113] Wie eine *Forsa*-Umfrage aus dem Jahr 2008 zeigt, sind diese Bedenken keineswegs unbegründet.[114] Aus diesem Grund fordert das *BVerfG,* eine Übermittlung von Daten, die einer Kommunikation i.S.d. § 99 Abs. 2 TKG zugrunde liegen, auszuschließen.[115] Der Gesetzgeber geht insoweit über diese Vorgaben hinaus, als er die Erhebung von Daten jeder Kommunikation unterbindet, bei der ein Berufsgeheimnisträger beteiligt ist.[116] Hier zeigt sich eine gewisse Diskrepanz zur Speicherung der Daten, welche gestattet ist, solange es sich nicht um Verbindungen i.S.d. § 99 Abs. 2 TKG handelt.[117] Wenn jedoch Daten von Berufsgeheimnisträgern nicht übermittelt werden dürfen, entfällt insoweit der strafrechtliche Zweck, der einen Eingriff in das Telekommunikationsgeheimnis durch die Speicherung rechtfertigen würde.[118] Folglich muss auch eine Speicherung dieser Daten so weit wie möglich verhindert werden.[119] Es liegt nahe, zur Ermittlung der auszunehmenden Anschlüsse, Listensysteme anzulegen, auf welche die TKD zurückgreifen können. Hierfür müssten Berufsgeheimnisträger unter Nachweis ihrer Geheimnisträgereigenschaft verpflichtend die von ihnen beruflich genutzten Anschlüsse und Rufnummern angeben. Nach einer Variante würde diese Angabe direkt bei den TKD erfolgen, indem Bestandskunden einmalig und neue Kunden bei Vertragsschluss nach ihrer Berufsgeheimnisträgereigenschaft befragt werden.[120] Ebenso denkbar wäre, ein System einzuführen, bei welchem eine Ausnahme bei der *BNetzA* zu beantragen ist, welche wiederum die TKD über die von der Speicherung auszunehmenden Anschlüsse informiert.[121] Dieses Vorgehen hätte den Vorteil, dass so auch keine Daten des Kommunikationsgegenübers und Nicht-Kunden mit Berufsgeheimnisträgereigenschaft gespeichert würden, dessen Status dem Unternehmen ansonsten nicht bekannt wäre. Sinnvollerweise sollten regelmäßige Angaben über den aktuellen Status erfolgen.[122] Bei den Telekommunikationsunternehmen müssten nun automatisiert eben diese Anschlüsse und Rufnummern entweder von Beginn an aus der Speicherung herausgefiltert werden oder im Falle, dass die Daten für Zwecke nach §§ 96, 100 TKG genutzt werden sollen, nach Ablauf der zulässigen Speicherfrist, d.h. unverzüglich nach Zweckerfüllung, gelöscht werden.

111 *Nelles*, S. 384.
112 *Roßnagel et al.* (Fn. 41), S. 154.
113 *Bizer,* DuD 2007, 586 (587).
114 Forsa, Meinungen der Bundesbürger zur Vorratsdatenspeicherung, P8475/ 20186 Ma, 2.6.2008, abrufbar unter: http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf (zuletzt abgerufen am 5.5.2021), S. 1.
115 BVerfGE 125, 260 (334).
116 § 100g Abs. 4 StPO.
117 § 113b Abs. 6 TKG
118 So auch *Mayen,* in: Scheurle/Mayen, § 113b Rn. 32.
119 Vgl. *EuGH*, Tele2, Rn. 105.
120 *Gärtner/Kipker,* DuD 2015, 593 (598).
121 *Roßnagel et al.* (Fn. 41), S. 156.
122 Vgl. *Gärtner/Kipker,* DuD 2015, 593 (599).

8. Anforderungen an die Anlass- und Personenbezogenheit

*a) Anlass der Speicherung*

Gemäß § 113b TKG hat die Speicherung sämtlicher aufgezählter Daten jeglicher Telekommunikationsnutzer zu erfolgen, die Speicherung ist somit anlasslos und allgemein. Während das *BVerfG* eine anlasslose Speicherung für mit Art. 10 GG unter bestimmten Voraussetzungen vereinbar hält,[123] verbietet der *EuGH* prinzipiell eine derartige Datenspeicherung.[124] Nach dem Gerichtshof soll die Vorratsdatenspeicherung die Ausnahme, nicht die Regel sein.[125] Diese Aussage war es auch, die das *OVG Münster* zu der Annahme brachte, die § 113a, 113b TKG verstießen gegen Europarecht.[126] Darüber, dass die aktuelle anlasslose Vorratsdatenspeicherung so nicht länger möglich ist, besteht überwiegend Einigkeit.[127] Deutlich schwieriger gestaltet sich jedoch die Suche nach einer alternativen Ausgestaltung. Während viele Stimmen für eine gänzliche Abschaffung der Vorratsdatenspeicherung plädieren,[128] gilt sie Ermittlern als unverzichtbar.[129] Es empfiehlt sich somit, nach einem Weg zu suchen, um aus der anlasslosen eine begründete, anlassbezogene Vorratsdatenspeicherung zu machen. Der *EuGH* fordert eine Einschränkung des Kreises der betroffenen Personen anhand objektiver Kriterien.[130] Demnach muss zumindest ein mittelbarer geographischer, zeitlicher oder personeller Zusammenhang zwischen der Überwachung und möglichen schweren Straftaten bestehen.[131] Fraglich ist, wie dieser im Bereich der Strafverfolgung aussehen könnte.

*aa) Geographischer Bezug*

Relativ unproblematisch erscheint insoweit die Begründung des geographischen Bezuges. Demnach soll eine Vorratsdatenspeicherung in einem bestimmten örtlichen Umfeld möglich sein, solange anhand objektiver Anhaltspunkte anzunehmen ist, dass in einem bestimmten Gebiet das Risiko benannter Straftaten erhöht ist.[132] Der Gerichtshof enthält sich jedoch weiterer Spezifikationen insbesondere, wie eng dieser Kreis gezogen sein muss. Aufgrund der hohen Eingriffsintensität ist jedoch unter Verhältnismäßigkeitsgesichtspunkten eine enge Begrenzung zu fordern, eben damit die Speicherung ihren Ausnahmecharakter behält.[133] Für die meisten Katalogtaten des § 100g Abs. 2 ist nicht ersichtlich, dass ihre Wahrscheinlichkeit in erheblicher Weise örtlichen Bezug aufweist. Denkbar wäre allerdings in Hinblick auf die Taten der Nr. 1c) und f) eine Speicherung im Bereich von Rotlichtmilieus anzuordnen, ist hier doch durchaus ein höheres Vorkommen dieser Straftaten feststellbar.[134] In Bezug auf Betäubungsmitteldelikte könnte eine Überwachung an den objektiv messbar größten Handelsplätzen angedacht werden. Schließlich erscheint auch möglich, gewisse Orte (bspw. Hauptbahnhöfe oder „Problemecken“) zu überwachen, solange in diesen Bereichen eine objektiv gesteigerte Kriminalität feststellbar ist. Vermieden werden muss dabei jedoch eine undifferenzierte Ausweitung auf ganze Stadtviertel. Obligatorisch bleibt jeweils die regelmäßige Feststellung, ob der betroffene Ort noch den Kriterien für die Speicherung entspricht.

123 BVerfGE 125, 260 (318).
124 *EuGH*, Tele2, Rn. 107.
125 *EuGH*, Tele2, Rn. 104.
126 *OVG Münster*, NVwZ-RR 2018, 43 (48).
127 *Bulowski*, S. 51; *Derksen,* Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta (Ausarbeitung WD 11 – 3000 – 18/11), 2011, S. 24; *Kühling,* VerfBlog 2017, S. 2; *Marsch,* VerfBlog 2016, S. 3; *Roßnagel,* NJW 2017, 696 (698).
128 *AK Vorratsdatenspeicherung et al.,* Gemeinsame Erklärung zum 6-jährigen Bestehen der EU-Richtlinie zur Vorratsspeicherung, 14.12.2011, verfügbar unter http://www.vorratsdatenspeicherung.de/content/view/515/188/lang,de/ (zuletzt abgerufen am 12.10.20).
129 *Münch,* ZRP 2015, 130.
130 *EuGH*, Tele2, Rn. 111.
131 *EuGH*, Tele2, Rn. 106.
132 *EuGH*, Tele2, Rn. 111.
133 Vgl. *EuGH*, Privacy International, Rn. 68.
134 *BKA,* Menschenhandel und Ausbeutung. Bundeslagebild 2018, S. 37.

*bb) Zeitlicher Bezug*

In seinem Urteil vom 6.10.2020 präzisiert der *EuGH* seine Vorgaben dahingehend, dass eine allgemeine, lediglich zeitlich begrenzte Speicherung nur zum Schutze der nationalen Sicherheit, nicht zur Strafverfolgung zulässig ist.[135] Der zeitliche Bezug ist im Rahmen der Strafverfolgung folglich eher als weiteres eingrenzendes Kriterium für personen- oder ortsbegründete Überwachung zu verstehen.[136]

*cc) Personeller Bezug*

Schwieriger gestaltet sich eine Eingrenzung anhand persönlicher Merkmale.

*(1) Bestimmte Bevölkerungsgruppen*

Ein Abstellen auf einzelne, statistisch besonders delinquente Bevölkerungs- oder Berufsgruppen verbietet sich.[137] Bei einem Abstellen auf Abstammung oder Herkunft läge eine Verletzung des Art. 3 Abs. 3 GG vor. Auch in Bezug auf andere Kriterien ist von einer Verletzung des Art. 3 Abs. 1 GG auszugehen, wenn bei einer solchen Typisierung eine nicht nur sehr kleine Gruppe ungerecht behandelt wird und die Eingriffsintensität mehr als gering ist.[138] Da die meisten Menschen keine Straftaten begehen[139] und die Eingriffsintensität der Vorratsdatenspeicherung äußerst hoch ist,[140] läge wohl in jedem Falle eine Verletzung von Art. 3 Abs. 1 GG vor.

*(2) Bestimmte Individuen*

Eine weitere Möglichkeit wäre die Speicherung bezüglich Personen, die im Verdacht stehen, in Zukunft eine Straftat zu begehen, um – sollte dies tatsächlich eintreten – die Aufklärung zu erleichtern. Die personenbezogene antizipierte Strafverfolgung ist der deutschen Rechtsordnung keineswegs fremd.[141] Alldieweil in derartigen Konstellationen keine Anknüpfung an einen Anfangsverdacht verlangt werden kann,[142] knüpft die Rechtsordnung Maßnahmen antizipierter Strafverfolgung meist an das Vorliegen einer Anlasstat und fordert eine Negativprognose, d.h. die Annahme, dass bezüglich des Betroffenen weitere Strafverfahren zu erwarten sind.[143] Bezogen auf die Vorratsdatenspeicherung müssten die zu erwartenden Straftaten nun denen des Katalogs in § 100g Abs. 2 StPO entsprechen, da nur in diesem Fall die Daten auch erhoben werden könnten. Vom Ausgangspunkt der bereits bestehenden Normen sind aufgrund des hohen Eingriffscharakters der Vorratsdatenspeicherung drei weitere Modifikationen ratsam. Erstens sollte die Überwachung nicht schon bei jedem Beschuldigten, sondern nur in Fällen des § 81g Abs. 4 StPO, insbesondere bei rechtskräftig Verurteilten möglich sein. Insoweit, als die Verhältnismäßigkeit des langen Zeitraums, in dem so eine Anordnung möglich ist, bezweifelt wird,[144] wäre denkbar, eine Anordnung zwingend an die Verkündung des Urteilsspruches zu knüpfen. Drittens sollte die Anordnung der Speicherung wie schon die Datenerhebung[145] auch bei Gefahr in Verzug unter Richtervorbehalt gestellt werden.[146] Mit Hilfe gespeicherter Bestandsdaten können die TKD die Rufnummern und Anschlusskennungen ermitteln, deren Kommunikationsvorgänge gespeichert werden sollen. Eine Pflicht zur Benachrichtigung des Betroffenen sollte

135 *EuGH*, La Quadrature du Net, Rn. 137.
136 Vgl. *EuGH*, La Quadrature du Net, Rn. 168.
137 *Ziebarth,* ZUM 2017, 398 (402).
138 *Nußberger,* in: Sachs, Grundgesetz Kommentar, 8. Auflage (2018), Art. 3 Rn. 109.
139 Siehe *BKA,* Polizeiliche Kriminalstatistik. Bundesrepublik Deutschland. Jahrbuch, Band 3: Tatverdächtige, 67. Ausgabe (2019), S. 27.
140 BVerfGE 125, 260 (328).
141 Siehe §§ 81b, 81g Abs. 1 StPO.
142 *Rudolph*, Antizipierte Strafverfolgung. Zum Regelungsstandort der Strafverfolgungsvorsorge unter Beachtung strafverfahrensrechtlich-funktionaler Aspekte, 2005, S. 13.
143 *Bock,* ZIS 2007, 129 (132).
144 *Bosch,* in: KMR-StPO, § 81g Rn. 15.
145 Vgl. § 101a Abs. 1 S. 2 StPO.
146 Anders § 81g Abs. 3 StPO.

grundsätzlich bestehen, indessen nur solange die Strafverfolgung nicht (mehr) gefährdet wird.[147]

*(3) Daten zur Gefahrenabwehr*

Ebenfalls denkbar wäre die Verwertung von Daten, die bezüglich bestimmter Personen zum Zwecke der Gefahrenabwehr gespeichert worden sind.[148] Grundsätzlich gilt, dass ohne ausdrückliche Ermächtigungsgrundlage Daten, die zu bestimmten Zwecken gesammelt wurden, nicht zu anderen Zwecken gebraucht werden dürfen.[149] Eine explizite Ermächtigungsgrundlage findet sich hierbei in § 161 Abs. 1 S. 1 StPO, der nach den Maßgaben des § 101a Abs. 5 StPO eine Verwendung von nach Polizeirecht erlangten Daten i.S.d. § 113b TKG zur Strafverfolgung gestattet. § 101a Abs. 5 StPO bezieht sich jedoch lediglich auf „personenbezogene Daten", nicht auf jegliche Verkehrsdaten. Insoweit wäre also eine Anpassung erforderlich. Des Weiteren beschränkt er sich auf „erlangt[e]" Daten, welches streng genommen nur bereits erhobene Daten, nicht die nur gespeicherten umfasst.[150] Wendet man § 101a Abs. 5 StPO dennoch (analog) an, so kann eine Verwertung dann erfolgen, wenn die Daten auf Grund des § 100g Abs. 2 StPO hätten erhoben werden dürfen. § 100g Abs. 2 StPO gestattet allerdings eine Erhebung der Daten nur bei Vorliegen eines Anfangsverdachts, der zu Beginn der präventiven Speicherung ja noch gar nicht vorliegen konnte. Denkbar wäre somit nur noch, die Normen dahingehend anzupassen, dass eine Speicherung gemäß § 113b TKG hätte zulässig sein müssen. Wenn § 113b TKG an europarechtliche Maßgaben angepasst wird, folgt, dass eine Verwertung von Daten, die zum Zwecke der Gefahrenabwehr und bezüglich einer bestimmten Person gesammelt wurden, nur erfolgen kann, wenn diese Daten auch Bezug zu einem Ort aufweisen, an dem gesteigerte Kriminalität zu erwarten ist oder der von der Erhebung Betroffene die unter III. 8. a) cc) (2) genannten Kriterien erfüllt.

*dd) Kritik an den Lösungsvorschlägen*

Die vorgeschlagenen Lösungsansätze entbehren keineswegs erheblicher Schwächen. So ist bspw. bei der Anwendung des geografischen Kriteriums mitnichten evident, wann denn ein besonders belastetes Gebiet vorliegen soll bzw. wie eng oder genau dieses abzugrenzen ist. Auch bedeutet ein erhöhtes Kriminalitätsaufkommen innerhalb eines bestimmten Areals nicht, dass die Kommunikation innerhalb dieses Bereichs für Ermittler auch besonders ergiebig ist. Eine Überwachung einzelner Geräte andererseits würde einen immensen technischen, finanziellen und organisatorischen Aufwand bedeuten. Daneben träte stets auch das Problem der mannigfaltigen Ausweichmöglichkeiten. Ohne Weiteres ließe sich Kommunikation auf ein nicht überwachtes Gebiet oder Medium übertragen, so dass die Vorratsdatenspeicherung bei beiden Varianten ins Leere liefe. In jedem Fall wäre der Gewinn für die Ermittlungsbehörden denkbar gering, denn eine Strategie, die davon lebt, keine Unterschiede zu machen und alles zu erfassen, kann nicht funktionieren, wenn die Erfassung auf ein Minimum reduziert werden soll. Im Ergebnis präsentiert sich eine Vorratsdatenspeicherung nach Maßgaben des *EuGH* somit doch eher als Gedankenspielerei, denn als realistische Umsetzungsmöglichkeit.

*b) Ausnahme: IP-Adressen*

Im Oktober 2020 revidierte der *EuGH* seine Einschätzung teilweise. Eine anlasslose Speicherung solle nun in

147 *EuGH*, La Quadrature du Net, Rn. 190.
148 *Engelhardt,* Verwendung präventivpolizeilich erhobener Daten im Strafprozess: Eine Untersuchung am Beispiel der Telekommunikationsüberwachung, 2011, S. 2.
149 Vgl. BVerfGE 65, 1 (46); 92, 191 (197).
150 Vgl. *Bär,* in: BeckOK-StPO, § 101a Rn. 11.

Bezug auf IP-Adressen möglich sein,[151] solange keine Informationen bezüglich der Telekommunikationspartner aufbewahrt werden.[152] Dies wird mit der geringeren Eingriffsintensität und der besonderen Bedeutung von IP-Adressen für die Aufklärung von Online-Kriminalität begründet.[153] Wirklich überzeugen kann diese Argumentation, die sich in ihrer Essenz darauf stützt, die Speicherung sei weniger eingriffsintensiv, da sie nur eine Person betrifft, während sie gleichzeitig gesteht, dass auch diese Daten detaillierte Profilbildungen ermöglichen,[154] nicht. Dass Daten nur einer einzelnen Person gespeichert werden, macht im Ergebnis keinen Unterschied, werden sie es im Rahmen einer flächendeckenden anlasslosen Vorratsdatenspeicherung doch von *jeder* einzelnen Person. Gleichzeitig ist nicht ersichtlich, wieso Informationen über die Telekommunikation mit anderen Individuen mehr Erkenntnisse bringen sollten als die über Aktivitäten im Internet.[155] Letzten Endes wirkt es vielmehr so, als wäre die Standhaftigkeit des *EuGH* dem Drängen der Mitgliedsstaaten zum Opfer gefallen.[156] Folgt man allerdings der neuen Linie des *EuGH*, so wäre eine anlasslose Speicherung im Rahmen von § 113b Abs. 3 möglich.

*c) Personenbezug bei der Erhebung*

Enger setzt der *EuGH* die Voraussetzungen der Datenabfrage durch die Behörden. Eine Erhebung erachtet er nur als rechtmäßig, wenn sie sich auf Daten der Personen beschränkt, die in Verdacht stehen, eine schwere Straftat begangen zu haben oder in eine solche verwickelt zu sein.[157] Ausnahmen sollen nur in besonderen Fällen möglich sein, wobei eine Ausnahme in Bezug auf die Strafverfolgung nicht genannt wird.[158] Dies bedeutet im Ergebnis, dass eine Datenerhebung durch die Behörden auf Daten des Verdächtigen beschränkt bleiben muss, solange nicht das Gegenüber ebenfalls verdächtig ist, zumindest mit der Straftat in Zusammenhang zu stehen. Der *EuGH* konkretisiert nicht weiter, welcher Qualität dieser Zusammenhang sein muss. Sachdienlich dürfte ein Abstellen auf die dem StGB bekannten Beteiligungsformen[159] sein, da nur in solchen Fällen eine strafrechtliche Verfolgung möglich ist, die einen Eingriff in die Telekommunikationsfreiheit rechtfertigt.[160] Da nicht ausgeschlossen werden kann, dass ein betroffener Anschluss von einer anderen Person genutzt wurde, sind für den unwahrscheinlichen Fall, dass dies schon vor Erhebung bekannt sein sollte, ein Erhebungsverbot und für die Fälle nachträglicher Kenntniserlangung ein Beweisverwertungsverbot vorzusehen.

*d) Rekurs: Berufsgeheimnisträger*

Auch die Schutzbedürftigkeit der Berufsgeheimnisträger endet dort, wo sie selbst der Beteiligung verdächtig sind.[161] Eine – oben grundsätzlich ausgeschlossene– Speicherung ihrer Daten kann somit erfolgen, wenn sich eine Anordnung direkt gegen den Berufsgeheimnisträger richtet oder eine solche Anordnung hätte erlassen werden können. Da allein durch die Anlegung von Listen eine lückenlose Erfassung aller Kommunikation von Berufsgeheimnisträgern nicht gewährleistet werden kann, müsste bei der alten Ausgestaltung der Vorratsdatenspeicherung

151 *EuGH*, La Quadrature du Net, Rn. 152.
152 *EuGH*, La Quadrature du Net, Rn. 152.
153 *EuGH*, La Quadrature du Net, Rn. 154.
154 *EuGH*, La Quadrature du Net, Rn. 153.
155 Vgl III. 2. b) bb).
156 Vgl. *Rath,* Urteil zur Vorratsdatenspeicherung. Klug Nachgegeben, Die Tageszeitung 6.10.2020, verfügbar unter https://taz.de/Urteil-zu-Vorratsdatenspeicherung/!5716106/ (zuletzt aufgerufen am 14.10.20).
157 *EuGH*, Tele2, Rn. 119.
158 *EuGH*, Tele2, Rn. 119.
159 Vgl. §§ 25 ff. StGB.
160 Vgl. BVerfGE 125, 260 (330).
161 BVerfGE 129, 208 (266 f.); vgl. *Zöller,* in: Gercke et al., 6. Auflage (2019), § 160a Rn. 17.

im Rahmen der Übermittlung der Daten eine weitere Filterung erfolgen.[162] Folgt man jedoch den Vorgaben des *EuGH*, so kann eine Erhebung stets nur dann erfolgen, wenn die Betroffenen in Verdacht stehen, an einer Tat beteiligt zu sein. In solchen Fällen sind jedoch auch Geheimnisträger nicht mehr schützenswert,[163] sodass hier eine gesonderte Regelung zur Erhebung obsolet ist.

*e) Quick-Freeze als Alternative*

Im Rahmen der Anlassbezogenheit wird häufig auf das Quick-Freeze-Verfahren als Alternative zur Vorratsdatenspeicherung verwiesen.[164] Bei diesem Verfahren können Daten im Sinne des § 96 TKG bei Vorliegen eines Anfangsverdachts „eingefroren", d. h. ihre Löschung vorläufig verhindert werden.[165] Nach dem erforderlichen richterlichen Beschluss werden nun die Daten an die Strafverfolgungsbehörde übermittelt.[166] Auf diese Weise lässt sich eine reguläre Löschung für den Zeitraum, in dem das Vorliegen der weiteren Voraussetzungen des § 100g Abs. 1 S. 1 StPO validiert werden und der richterliche Beschluss eingeholt wird, verhindern. Eine voreilige Erhebung in dem Wissen, dass die Daten bald nicht mehr vorhanden sein werden, dürfte so eher unterbleiben. Im Gegensatz zur anlasslosen Vorratsdatenspeicherung erfolgt hier staatliches Handeln erst bei Vorliegen eines Anfangsverdachtes, so dass auch die Eingriffsintensität geringer ist.[167] 2010 schlug die *FDP*-Fraktion die Einführung eines Quick-Freeze-Verfahrens in die StPO vor. Die Anordnung zum Einfrieren sollte hierbei von der Staatsanwaltschaft mit dreimonatiger Wirkung, in Eilfällen durch die Polizei für drei Tage erfolgen. Eine begründete Verlängerung wäre möglich. [168] Auch der *EuGH* gestattet ein Quick-Freeze-Vorgehen, wobei er betont, dass derartige Maßnahmen nicht auf Tatverdächtige beschränkt bleiben müssen.[169] Um einen möglichst grundrechtsschonenden Eingriff zu gewährleisten, müssen spätestens ab dem Moment des Einfrierens und damit dem Zeitpunkt, ab dem staatliche Behörden aktiv werden, dieselben Sicherheitsanforderungen wie bei der Vorratsdatenspeicherung gestellt und erfüllt werden.[170] Dieses Verfahren mag zwar weniger einschneidend sein als die klassische Vorratsdatenspeicherung, ist jedoch bei weitem nicht so effektiv.[171] Dies liegt vor allem daran, dass eine derartige Anordnung innerhalb sehr kurzer Zeit, nämlich vor der routinemäßigen Löschung, erfolgen muss und sich nur auf Daten erstrecken kann, die das Unternehmen aus geschäftlichen Gründen speichert.[172] Doch statt das Quick-Freeze-Verfahren als ungeeignet abzutun, bietet es sich an, diese Vorgehensweise als Ergänzung zur nunmehr sehr eingeschränkten Vorratsdatenspeicherung zu sehen.

## IV. Nutzen einer Vorratsdatenspeicherung

Trotz vielfältigen Problembewusstseins schweigen *EuGH* und *BVerfG*, wenn es um die Frage nach dem tatsächlichen Nutzen der Vorratsdatenspeicherung geht. Beide Gerichte gehen somit wohl davon aus, dass der Nutzen die

162 *Roßnagel et al*. (Fn. 41), S. 156.
163 BVerfGE 129, 208 (266 f.); vgl. *Zöller,* in: Gercke et al., § 160a Rn. 17.
164 *Bizer,* DuD 2007, 586 (588); *Kiparski,* in: Specht/Mantz, 2019, § 18 Rn. 49; *Kunnert,* DuD 2014, 774 (783); *Szuba*, S. 100.
165 *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, 2009, S. 37.
166 *Derksen,* S. 16; MPI, S. 40 f.
167 Vgl. *Sierck et al.,* Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht (Ausarbeitung WD 3 – 282/06), 2006, S. 14; *Szuba*, S. 100.
168 FDP-Bundestagsfraktion: Eckpunkte zur Verbesserung der Kriminalitätsbekämpfung im Internet. Freiheit und Sicherheit im Internet bewahren, 9.11.2010, abrufbar unter: https://web.archive.org/web/20121122054959/http://www.fdp-fraktion.de/files/1228/Eckpunkte_Kriminalitaetsbekaempfung_Internet.pdf (zuletzt abgerufen am 13.10.20), S. 8.
169 *EuGH*, La Quadrature du Net, Rn. 163, 165.
170 Zu dieser Problematik *Nelles*, S. 187.
171 BVerfGE 125, 260 (318); *Nelles*, S. 188 f.
172 MPI, S. 41.

Kosten der Vorratsdatenspeicherung nach den von ihnen aufgestellten Maßgaben aufwiegen kann.[173] Diese Annahme ist jedoch alles andere als zwingend. Sogar wenn man die Effektivitätsdefizite einer anlassbezogenen Speicherung für einen Moment beiseite lassen möchte, ist es doch mehr als umstritten, wie viel selbst die anlasslose Vorratsdatenspeicherung wirklich zur Verbrechensaufklärung beitragen kann.[174] Nach einer zurückhaltenden, jedoch auf umfassende Daten gestützten Einschätzung des Max-Planck-Instituts für ausländisches und internationales Strafrecht ist keine Verbesserung der Aufklärungsquote anzunehmen.[175] Auch eine Studie des Europäischen Parlaments kann keinen messbaren Zusammenhang zwischen Speicherung und Aufklärung feststellen.[176] Gleichzeitig zeugen Einzelfälle davon, dass auf Vorrat gespeicherte Daten zumindest in bestimmten Situationen zur Aufklärung unabdingbar sind.[177] Doch gerade Täter in den Deliktsbereichen Kinderpornografie und organisierte Kriminalität, welche in ihrer Schwere meist als Hauptargument für eine Vorratsdatenspeicherung herangezogen werden, dürften wohl in Anbetracht ihrer an den Tag gelegten Professionalität und der hohen Strafandrohung auf Ausweichmöglichkeiten wie das Darknet oder die Verschleierung von IP-Adressen zurückgreifen.[178] Tritt nun hinzu, dass – wie vom *EuGH* gefordert – nur IP-Adressen anlasslos gespeichert werden dürfen, folgt aus der einerseits zweifelhaften Sinnhaftigkeit der anlassbezogenen Speicherung[179] und den andererseits vielfältigen Umgehungsmöglichkeiten im Bereich der IP-Adressspeicherung, dass sich der Wert dieses Vorgehens der Null annähern dürfte. Dass eine (anlasslose) Vorratsdatenspeicherung wirklich in dem Maße nützt, welches diesen schweren Grundrechtseingriff zu rechtfertigen vermag, kann somit entgegen der Vorstellungen von *EuGH* und *BVerfG* durchaus bezweifelt werden.

## V. Fazit

Die aktuelle Regelung der Vorratsdatenspeicherung genügt in vielerlei Hinsicht nicht den Anforderungen des *EuGH*. Eine Reform müsste insbesondere die Anlassbezogenheit der Speicherung und die Zweckgebundenheit sowie Erforderlichkeit der Erhebung garantieren. Jenseits dessen besteht auch in praktischer Hinsicht Verbesserungspotential. Und wie immer im Spannungsfeld zwischen Sicherheit und Freiheit kann eine Lösung nur bei Zugeständnissen auf beiden Seiten gefunden werden. Eine europa- und verfassungsrechtskonforme Regelung ist wohl möglich. Ob sie aber auch sinnvoll ist, ist eine ganz andere Frage. Eine Vorratsdatenspeicherung 3.0 würde nicht nur enormen strukturellen und finanziellen Aufwand für Staat und Unternehmen bedeuten. Abgesehen von der Frage, ob die Vorgaben, bspw. zum Schutz der Berufsgeheimnisträger,[180] überhaupt technisch umsetzbar wären, führten die Einschränkungen von Anwendungsbereich und Zweckdienlichkeit über den ohnehin schon zweifelhaften Nutzen der Vorratsdatenspeicherung hinaus wohl zur kompletten Sinnlosigkeit dieses Vorgehens. Eine anlassbezogene Vorratsdatenspeicherung passt einfach nicht zur Strafverfolgung.

173 *EuGH*, Tele2, Rn. 108; BVerfGE 125, 260 (317).
174 *Derksen*, S. 15; *Moser-Knierim*, S. 191, *Puschke,* ZIS 2019, 308 (313); *Szuba*, S. 99.
175 MPI, S. 129.
176 European Parliament, General data retention/effects on crime, 27.1.2020, S. 3.
177 MPI, S. 82, 143 f.; *Münch,* ZRP 2015, 130.
178 Vgl. Hoppenstedt, Wie Pädokriminelle das Internet nutzen – und wie Ermittler sie finden können, Spiegel Netzwelt 1.7.2020, abrufbar unter: https://www.spiegel.de/netzwelt/web/kindesmissbrauch-wie-taeter-das-internet-nutzen-und-wie-ermittler-sie-finden-koennen-a-868362db-8a11-4847-a280-d748d79dbbf3 (zuletzt abgerufen am 15.12.20).
179 Siehe III. 8. a) dd).
180 Vgl. BT-Drs. 18/5088, S. 33.

## VI. Schluss

Aktuell mehren sich erneut die Stimmen, die eine Vorratsdatenspeicherung zumindest bezüglich IP-Adressen fordern.[181] Es ließe sich wohl behaupten, dies sei die Schuld des *EuGH,* welcher, statt der Vorratsdatenspeicherung ein klares Ende zu setzen, in seinen Urteilen immer wieder Hintertüren für eine zumindest eingeschränkte Speicherung offen hält. So ergreift der Gerichtshof auch im jüngsten Urteil vom 02.03.2021 nicht die Chance, ein für alle Mal Klarheit zu schaffen.[182] Doch die Politik geht noch weiter. Diskutiert, gefordert und geplant wird nach wie vor eine anlasslose, allgemeine Vorratsdatenspeicherung, die eigentlich zwingenden Vorgaben des *EuGH* werden blindlings ignoriert.[183] Dabei wäre es vielleicht an der Zeit, zu akzeptieren, dass eine sinnvolle und legale Form der Vorratsdatenspeicherung nicht möglich ist. Der Rechtsstaat ist kein leerer Begriff. Er setzt feste Grenzen, über die sich staatliches Handeln nicht hinwegsetzen darf und wenn es bedeuten mag, dass eine Vorratsdatenspeicherung nicht effektiv umgesetzt werden kann. Dennoch: die Vorratsdatenspeicherung ist und bleibt Thema. Und so wie die Geschichte 2005 (*"The Never-Ending Story "*[184]) oder 2015 nicht endete (*A Never-Ending Story: Die Vorratsdatenspeicherung*[185]*, „Die unendliche Geschichte der Vorratsdatenspeicherung: Bürger unter Generalverdacht"*[186]*, „Es ist eine unendliche Geschichte"*[187]*, Vorratsdatenspeicherung: Eine unendliche (nervige) Geschichte*[188]), tat sie es auch 2016 (*Nein! Doch! Oh! Die unendliche Geschichte der Vorratsdatenspeicherung*[189]), 2017 (*Hintergrund: Vorratsdatenspeicherung, die endlose Geschichte*[190]) und 2019 *(„Die unendliche Geschichte der Vorratsdatenspeicherung"*[191]) nicht. Dass sie es 2021 tun wird, ist mehr als unwahrscheinlich und so bleibt nur abzuwarten, ob *BVerfG* und *EuGH* einen Schlusspunkt setzen und der Gesetzgeber die Urteile akzeptiert oder eine neue Runde im ewigen Kreislauf der Vorratsdatenspeicherung eröffnet werden wird.



181 Briegleb, Drei Bundesländer fordern Wiederaufnahme der Vorratsdatenspeicherung, Heise online 19.11.20, abrufbar unter: https://www.heise.de/news/Drei-Bundeslaender-fordern-Wiederaufnahme-der-Vorratsdatenspeicherung-4966157.html (zuletzt abgerufen am 10.1.21); European Council, European Council meeting (10 and 11 December 2020) – Conclusions, 11.12.2020, Rn. 26.

182 *EuGH*, Urt. v. 2.3.2021, C-746/18, ECLI:EU:C:2021:152- Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques).

183 Vgl. BMWi/BMVI, § 175 I TKG-E; Council of the European Union, Informal Outcome of Proceedings of the informal VTC of the members of CATS on 8 February 2021, 26.2.21, S. 4.

184 *Hülsmann,* The Never-Ending Story, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. -Kommunikation 3/2005, S. 48.

185 *Spiecker/Simitis,* VerfBlog 5.5.2015, abrufbar unter: https://verfassungsblog.de/a-never-ending-story-die-vorratsdatenspeicherung/ (zuletzt abgerufen am 13.10.20).

186 ZDF-Frontal 21, Die unendliche Geschichte der Vorratsdatenspeicherung. Bürger unter Generalverdacht, 2015.

187 *Kurz,* Vorratsdatenspeicherung. An der Grenze geltenden Rechts, Frankfurter Allgemeine Zeitung 1.6.2015, abrufbar unter: https://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/vorratsdatenspeicherung-an-der-grenze-des-geltenden-rechts-13622263.html (zuletzt abgerufen am 13.10.20).

188 *Rieß,* Vorratsdatenspeicherung, Eine unendliche (nervige) Geschichte, ComputerWeekly 20.4.2015, abrufbar unter: https://www.computerweekly.com/de/meinung/Vorratsdatenspeicherung-Eine-unendliche-nervige-Geschichte (zuletzt abgerufen am 13.10.20).

189 *Miraus,* Nein! Doch! Oh! Die unendliche Geschichte der Vorratsdatenspeicherung, BasicThinking 29.12.2016, abrufbar unter: https://www.basicthinking.de/blog/2016/12/29/vorratsdatenspeicherung-illegal/ (zuletzt abgerufen am 13.10.20).

190 *Faisst,* Hintergrund. Vorratsdatenspeicherung, die endlose Geschichte, Südwest Presse 12.8.2017, abrufbar unter: https://www.swp.de/politik/inland/hintergrund_-vorratsdatenspeicherung_-die-endlose-geschichte-23608613.html (zuletzt abgerufen am 13.10.20).

191 o.V., Vorratsdatenspeicherung: Deutsche Gerichte verweisen auf den EuGH, t3n 29.9.2019, abrufbar unter: https://t3n.de/news/vorratsdatenspeicherung-deutsche-1201909/ (zuletzt abgerufen am 13.10.20).