Die Vorratsdatenspeicherung auf dem Prüfstand

Livia Matter *

Die seit dem 1. Januar 2002 gesetzlich vorgesehene Vorratsdatenspeicherung von Randdaten im Bereich des Fernmeldeverkehrs wurde vom Bundesgericht am 2. März 2018 bestätigt. Nun soll der EGMR darüber befinden. Unter Berücksichtigung der Rechtsprechung desselben sowie des EuGH darf ein spannendes Urteil erwartet werden. Zu beobachten ist nämlich, dass die Bedeutung der Vorratsdatenspeicherung von den Gerichten unterschiedlich bewertet wird. Dies ist wohl nicht zuletzt darauf zurückzuführen, dass es sich bei dieser Thematik letztlich um eine Abwägung zwischen dem Schutz der Grundrechte der betroffenen Personen und dem Bedürfnis nach Sicherheit handelt.

Zitiervorschlag: Livia Matter, Die Vorratsdatenspeicherung auf dem Prüfstand, in: *sui-generis* 2019, S. 257

URL: sui-generis.ch/108

DOI: https://doi.org/10.21257/sg.108

* Livia Matter (livia.matter[at]unifr.ch) ist Doktorandin und Diplomassistentin am Institut für Europarecht der Universität Freiburg i.Ü.

I. Einführung

1 Die Vorratsdatenspeicherung von sogenannten Randdaten (also Angaben, wann eine Person mit wem, wie lange und von wo aus[1] Kontakt gehabt hat sowie die technischen Merkmale der jeweiligen Verbindung[2]) ist im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs[3] (BÜPF) vorgesehen und wird mit Bestimmungen der Strafprozessordnung[4] ergänzt.[5] Zudem ist auch das materielle Strafrecht[6] zu berücksichtigen.[7]

2 Gemäss der gesetzlichen Regelung wird ein umfassender Kreis von AnbieterInnen im Post-, Fernmelde- sowie im Internetbereich[8] verpflichtet, die Randdaten aller NutzerInnen ihrer Dienste während sechs Monaten[9] zu speichern.[10] Die vom Gesetz vorgesehen Behörden können dann im entsprechenden Verfahren[11] u.a. zwecks Strafverfolgung Einsicht in diese Daten erhalten.[12]

3 Seit dem 1. Januar 2002 ist diese Massnahme gesetzlich vorgesehen, wobei bereits bei deren Einführung die Bedeutung der Speicherung der Randdaten für die Strafverfolgung betont wurde, da damit Daten aus der Vergangenheit – also retrograd – eingesehen werden können. Schon damals wurde anerkannt, dass damit erheblich in die persönliche Geheimsphäre der betroffenen Personen eingegriffen wird.[13]

4 Per 1. März 2018 wurde das BÜPF einer Totalrevision unterzogen. Bezweckt wurde dabei explizit nicht die umfangreichere, sondern die «bessere» Überwachung des Post- und Fernmeldeverkehrs.[14]

5 Tatsächlich wurde jedoch u.a. der persönliche Geltungsbereich erweitert.[15] Ebenfalls wurde der sachliche Anwendungsbereich auf vermisste Personen sowie zur Fahndung ausgeschriebene Personen ausgedehnt.[16] Des Weiteren wurden neu straf- und verwaltungsrecht-

1 Da moderne Smartphones mittlerweile ständig – auch wenn keine aktive Kommunikation stattfindet – mit dem Internet verbunden sind, werden dadurch quasi ununterbrochen die Aufenthaltsorte der BenutzerInnen aufgezeichnet. Vgl. dazu Kire, Faktenblatt zur «Vorratsdatenspeicherung» vom 27. September 2018.

2 Art. 8 lit. b BÜPF.

3 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (BÜPF; SR 780.1).

4 Schweizerische Strafprozessordnung vom 5. Oktober 2007 (StPO; SR 312.0).

5 Botschaft vom 27. Februar 2013 zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) (BBl 2013 2683), S. 2690, 2738 ff.

6 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB; SR 311.0).

7 Vgl. dazu Art. 269 Abs. 2 lit. a StPO sowie Botschaft vom 1. Juli 1998 zu den Bundesgesetzen betreffend die Überwachung des Post- und Fernmeldeverkehrs und über die verdeckte Ermittlung (BBl 1998 IV 4241), S. 4254.

8 Vgl. dazu Art. 2 BÜPF.

9 Die Aufbewahrungsfrist der Daten wurde damals auf 6 Monate festgesetzt, weil während dieser Frist die AnbieterInnen von Post- und Fernmeldediensten die Verkehrs- und Rechnungsdaten aufbewahren mussten, um die ausgestellte Rechnung bei Bedarf mit einem Beweis versehen zu können, vgl. dazu BBl 1998 IV 4241 (Fn. 7), S. 4268.

10 Art. 19 Abs. 4 und Art. 26 Abs. 5 BÜPF. Der vorliegende Beitrag beschränkt sich auf eine Auseinandersetzung mit der Vorratsdatenspeicherung im Fernmeldeverkehr, da sich das Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018 nur mit dieser befasst. Vgl. zur Vorratsdatenspeicherung von Randdaten im Postverkehr Art. 19 BÜPF.

11 Im Folgenden wird darauf verzichtet auf die Einzelheiten des Verfahrens hinsichtlich des Zugangs zu den Daten einzugehen. Siehe dazu jedoch Rn. 48 ff.

12 Art. 1 BÜPF.

13 BBl 1998 IV 4241 (Fn. 7), S. 4259.

14 BBl 2013 2683 (Fn. 5), S. 2689.

15 Ebd. S. 2694 f.; vgl. dazu Györffi Viktor, Mehr Überwachung im Strafprozess, in: plädoyer 2/14, S. 20.

16 BBl 2013 2683 (Fn. 5), S. 2698 f.

liche Sanktionen für AnbieterInnen aufgenommen, falls diese ihren Pflichten nicht nachkommen.[17] Aufgrund dessen ist also – entgegen der Absicht der Totalrevision – von einer Ausweitung der Vorratsdatenspeicherung auszugehen.[18]

6 Bereits vor der Totalrevision führte die Vorratsdatenspeicherung von Randdaten dazu, dass bestimmte Behörden in Erfahrung bringen konnten, wann eine Person mit wem wie oft Kontakt hatte, welche Personen zu ihrem sozialen Umfeld gehören, an welchen Orten sie sich aufhält[19] sowie welchen Interessen sie im Internet nachgeht. Auch wenn der eigentliche Inhalt der Kommunikation nicht von dieser Vorratsdatenspeicherung erfasst ist, lässt sich anhand der Randdaten dennoch ein Profil einer Person erstellen.[20]

7 In Anbetracht dessen drängt sich die Frage auf, inwiefern die Vorratsdatenspeicherung von Randdaten in die Grundrechte der betroffenen Personen eingreift. Insbesondere das Recht auf Achtung des Intim-, Privat- und Familienlebens, das Recht auf Privatsphäre, die Achtung des Brief-, Post- und Fernmeldeverkehrs, das Recht auf Schutz vor Missbrauch persönlicher Daten, die Meinungs- und Medienfreiheit, das Recht auf persönliche Freiheit, die Bewegungsfreiheit sowie die Unschuldsvermutung könnten verletzt sein.[21]

8 Angesichts der anstehenden Entscheidung des EGMR soll im Folgenden die Vorratsdatenspeicherung der Randdaten im Fernmeldeverkehr zwecks Strafverfolgung im Lichte des Datenschutzes, welcher als Teilgehalt des Rechts auf Privatsphäre in Art. 13 Abs. 2 BV grundrechtlich verankert ist, näher beleuchtet werden.

II. Datenschutzrechtliche Grundsätze

9 Dem Datenschutz sind verschiedene Bearbeitungsgrundsätze zu entnehmen, welche in den Art. 4-7 des Bundesgesetzes über den Datenschutz[22] (DSG) festgehalten sind. So muss die Datenbearbeitung u.a. verhältnismässig und zweckgebunden sein. Der Zweck sowie die Bearbeitung als solche müssen zudem für die betroffenen Personen erkennbar[23] sein.[24]

10 Trotz dieser datenschutzrechtlichen Bearbeitungsgrundsätze gilt es zu beachten, dass insbesondere im Namen der inneren Sicherheit resp. Verbrechensbekämpfung formelle Gesetze geschaffen werden, welche nicht unbedingt diesen Grundsätzen entsprechen.[25] Da einige dieser Bearbeitungsgrundsätze jedoch direkt der Bundesverfassung entnommen werden können, sind solche gesetzlichen Regelungen

17 Ebd. S. 2699 ff.
18 Auch die technische Entwicklung hat zur Ausweitung der Vorratsdatenspeicherung beigetragen. Vgl. dazu Fn. 2.
19 Ebd. hinsichtlich BenutzerInnen von Smartphones.
20 Vgl. dazu den Beitrag: Privatsphäre contre Suisse, erschienen in der WOZ am 27. September 2018.
21 Vgl. dazu das Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018, E. 4.
22 Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR. 235.1).
23 Im Polizei- und Sicherheitsbereich sind jedoch auch Ausnahmen davon möglich. Vgl. dazu Art. 14 Abs. 1 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997 (BWIS; SR. 120). Hier handelt es sich um eine Ausnahme von den datenschutzrechtlichen Grundsätzen, welche als nicht unproblematische Grundrechtseinschränkung zu werten ist. Siehe dazu auch Schweizer Rainer J., in: St. Galler Kommentar, 3. Aufl. 2014, N 96 zu Art. 13 BV.
24 Vgl. Art. 4 Abs 2-4 DSG.
25 Vgl. dazu Eidgenössischer Datenschutzbeauftragter (EDÖB), 1. Tätigkeitsbericht 1993/94, S. 11 ff.

als verfassungswidrig anzusehen. Vom Vorliegen einer gesetzlichen Grundlage kann deshalb nicht darauf geschlossen werden, dass die datenschutzrechtlichen Grundsätze eingehalten werden.[26] Vor diesem Hintergrund drängt sich deshalb – trotz der gesetzlichen Grundlage – eine genauere Betrachtung der vorliegenden Vorratsdatenspeicherung auf.

11 Die Vorratsdatenspeicherung von Randdaten wurde u.a. eingeführt, um Straftaten zu verhindern und zu verfolgen. Ihre Bedeutung in der Strafverfolgung liegt insbesondere darin, dass sie die rückwirkende Teilnehmeridentifikation ermöglicht.[27] Da sich bei der Vorratsdatenspeicherung der Randdaten jedoch erst nach der Speicherung der Daten herausstellt, ob diese tatsächlich verwendet resp. eingesehen werden, stellt sich die Frage, ob überhaupt von einer Zweckgebundenheit dieser Vorratsdatenspeicherung ausgegangen werden kann oder ob diese – zumindest anfänglich – fehlt.[28]

12 Hinsichtlich der Erkennbarkeit der Datenbearbeitung ist zwar festzuhalten, dass die Vorratsdatenspeicherung der Randdaten gesetzlich vorgesehen ist und somit die betroffenen Personen Kenntnis davon haben können.[29] Trotzdem ist es für die betroffenen Personen oftmals nur schwer nachzuvollziehen, in welcher Form die Datenbearbeitung stattfindet. Häufig sind sie sich nicht bewusst, dass resp. in welcher Weise sie von einer Datenbearbeitung betroffen sind. Hinzu kommt, dass die eigene Betroffenheit der Datenbearbeitung sowie deren Folgen regelmässig unterschätzt werden.[30] Demnach erscheint es fraglich, ob sich die betroffenen Personen tatsächlich bewusst sind, dass mit der Einsicht in die Randdaten ihrer Kommunikation regelmässig ein wohl – je nach Häufigkeit der Benutzung der Kommunikationsmittel – sehr umfangreicher Einblick in ihre eigene Lebensgestaltung verbunden sein kann.[31]

13 Gemäss dem ebenfalls in der Bundesverfassung verankerten Grundsatz der Verhältnismässigkeit muss das eingesetzte Mittel geeignet und erforderlich sein, um das angestrebte Ziel zu erreichen. Zudem muss die Datenbearbeitung in einem vernünftigen Verhältnis zum Eingriff in die Privatsphäre stehen. Die Datenbearbeitung muss demnach u.a. das mildeste Mittel zur Erreichung des angestrebten Zwecks darstellen, wobei insbesondere der Umfang der Daten sowie auch die Intensität der Bearbeitung zu berücksichtigen sind.[32]

14 Hinsichtlich der Aufbewahrungsdauer der Daten gilt es zu berücksichtigen, dass die Daten nur so lange gespeichert werden dürfen, wie dies die Erforderlichkeit

---

[26] Maurer-Lambrou Urs/Steiner Andrea, in: Basler Kommentar zum DSG, 3. Aufl. 2014, N 2 der Vorbemerkungen zum 2. Abschnitt.

[27] BBl 1998 IV 4241 (Fn. 7), S. 4255 ff.

[28] Vgl. Sigrist Martin, Staatsschutz oder Datenschutz? Die Vereinbarkeit präventiver Datenbearbeitung zur Wahrung der inneren Sicherheit mit dem Grundrecht auf informationelle Selbstbestimmung, Diss., Zürich 2014, S. 228.

[29] Davon geht das Bundesgericht auch aus. Vgl. Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018, E. 6.2.

[30] Rudin Beat, Die Erosion der informationellen Privatheit – oder: Rechtsetzung als Risiko?, in: Risiko und Recht, Festgabe zum Schweizerischen Juristentag 2004, S. 426 ff.

[31] Vgl. dazu als anschauliches Beispiel Kire, Das überwachte Leben von Nationalrat Balthasar Glättli – Interaktive Visualisierung zur Vorratsdatenspeicherung in der Schweiz vom 27. April 2014.

[32] Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht – Grundlagen und öffentliches Recht, Bern 2011, S. 528 ff.

zulässt. Es ist somit in jedem Einzelfall eine Güterabwägung zwischen den öffentlichen sowie den privaten Interessen vorzunehmen. Zu beachten gilt es dabei, dass mit zunehmender Aufbewahrungsdauer grundsätzlich die Schwere des Eingriffs, das Risiko der Zweckentfremdung, die Gefahr der Unrichtigkeit der Daten sowie die Missbrauchsgefahr zunehmen.[33]

15 Vor diesem Hintergrund muss einerseits danach gefragt werden, ob die Vorratsdatenspeicherung der Randdaten ein wirksames Mittel ist, das angestrebte Ziel (also hier die Strafbekämpfung) zu erreichen. Da die vorliegende Vorratsdatenspeicherung andererseits weit mehr Personendaten umfasst als schliesslich eingesehen – also benötigt – werden, ist fraglich, ob diese Sammlung von Daten überhaupt erforderlich ist.[34] Zudem ist auch danach zu fragen, ob es allenfalls eine mildere Massnahme als die Vorratsdatenspeicherung der Randdaten gibt resp. ob die sechsmonatige Aufbewahrungsdauer angemessen erscheint. Auf diese Fragen soll im Folgenden noch vertieft eingegangen werden.

III. Rechtsprechung zur Vorratsdatenspeicherung von Randdaten

16 Bis anhin haben sich bereits mehrere Gerichte zur Vorratsdatenspeicherung von Randdaten geäussert. Vor dem Hintergrund des bevorstehenden Urteils des EGMR soll der eingangs erwähnte Entscheid des Bundesgerichts vom 2. März 2018[35] sowohl mit der relevanten Rechtsprechung des EGMR sowie des EuGH (da die Beschwerdeführer im genannten Bundesgerichts-Entscheid darauf verweisen[36]) verglichen werden.

1. Rechtsprechung des Bundesgerichts

17 Das Bundesgericht ging in seinem Urteil vom 2. März 2018[37] lediglich auf die Frage nach der Speicherung und Aufbewahrung der Randdaten im Fernmeldeverkehr gemäss Art. 15 Abs. 3 aBÜPF[38] ein. Auf die Frage nach dem Zugriff der Behörden auf diese Daten, welcher in der Strafprozessordnung geregelt ist[39], trat das Bundesgericht – mangels schützenswertem Interesse – nicht ein.[40]

18 Relativ knapp hielt das Bundesgericht in seinem Urteil fest, dass die Speicherung und Aufbewahrung von Randdaten einen Eingriff in die informationelle Selbstbestimmung darstellen.[41] Anders als die

33 Sigrist (Fn. 28), S. 236 ff.

34 Vgl. zur generellen Zulässigkeit einer Datenspeicherung auf Vorrat BGE 125 II 473 E. 4.b.; Schweizer (Fn. 23), N 82 zu Art. 13 BV. Diggelmann Oliver, in: Basler Kommentar, 2015, N 34 zu Art. 13 BV; Biaggini Giovanni, in: Orell Füssli Kommentar, 2. Aufl. 2017, N 15 zu BV 13.

35 Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018.

36 Vgl. dazu Ebd. E. 8.2.2.

37 Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018.

38 Dem Urteil lagen noch die Bestimmungen des «alten» BÜPF (aBÜPF) zugrunde. Vgl. dazu Ebd. E. 1.3.

39 Art. 269 ff. StPO.

40 Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018, E. 2 ff. Dies wird jedoch insoweit kritisiert, als das Bundesgericht hinsichtlich des öffentlichen Interesses bei der Grundrechtsprüfung insbesondere auf die Strafverfolgung verweist. Siehe dazu den Beitrag von Meyerlustenberger Lachenal vom 15. April 2018.

41 Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018, E. 4.2. Dabei verweist das Bundesgericht auf die Rechtsprechung des EGMR, wonach insbesondere die systematische Erfassung von Informationen betreffend das Privatleben einen Eingriff in Art. 8 EMRK darstellt, unabhängig davon, ob die Daten später verwendet werden. Siehe dazu die EGMR-Urteile Nr. 35623/05 vom 2. September 2010 (Uzun gegen Deutschland),

Vorinstanz[42] kam das Bundesgericht jedoch zum Schluss, dass es sich vorliegend nicht um einen schweren Eingriff[43] in das Grundrecht handelt. Im Gegensatz zu der inhaltlichen Kontrolle der Kommunikation wertete das Bundesgericht die Speicherung und Aufbewahrung von Randdaten – ohne dies eingehender zu begründen – als «deutlich weniger einschneidend».[44]

19 Im Rahmen der Verhältnismässigkeitsprüfung begnügte sich das Bundesgericht – auf den Vorwurf, dass die Effektivität der Massnahme nicht empirisch erwiesen sei – mit der Feststellung, dass Massnahmen geeignet seien, wenn sie «mit Blick auf den angestrebten Zweck Wirkungen zu entfalten vermögen und nicht gänzlich daran vorbei zielen».[45] Des Weiteren wies das Bundesgericht darauf hin, dass sich der schweizerische Bundesgesetzgeber ausdrücklich für das System der umfassenden und verdachtsunabhängigen Speicherung und Aufbewahrung von Randdaten entschieden habe.[46] Hinsichtlich der von den Beschwerdeführern vorgebrachten Rechtsprechung des EuGH[47] hielt das Bundesgericht lediglich fest, dass die Schweiz nicht daran gebunden sei.[48]

20 Die Zweck-Mittel-Relation bejahte das oberste schweizerische Gericht schliesslich vor dem Hintergrund, dass die Strafverfolgungsbehörden keinen direkten und uneingeschränkten Zugriff auf die Daten hätten, sondern dass dieser «strengen Anforderungen» unterworfen sei.[49] Zudem befand das Bundesgericht, dass angemessene Schutzvorkehrungen vorhanden seien, um Missbräuche zu vermeiden.[50] Es rechtfertigte die sechsmonatige Speicherungsdauer insbesondere dahingehend, dass die Bekämpfung schwerer Delikte (Terrorismus und organisiertes Verbrechen) in der Regel äusserst zeitintensiv sei und es sich dabei um komplexe Sachverhalte handle.[51]

21 Wie bereits oben erwähnt, haben die Beschwerdeführer dieses Urteil an den EGMR weitergezogen.[52]

2. Rechtsprechung des EuGH

22 Der EuGH befasste sich bereits vor dem genannten Entscheid des Bundesgerichts in zwei Urteilen mit der Vorratsdatenspeicherung.

23 Im Urteil vom 8. April 2014 bezeichnete der EuGH den mit der sog. Vorratsdatenspeicherungsrichtlinie[53] (Richtlinie

§ 46; Nr. 28341/95 vom 4. Mai 2000 (Rotaru gegen Rumänien), § 43 und 46.

42 Urteil des Bundesverwaltungsgerichts A-4941/2014 vom 9. November 2016, E. 9.4.

43 Anders Sigrist (Fn. 28), S. 122; BVerfGE 125, 260 (318 ff.).

44 Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018, E. 5. Diese Ansicht des Bundesgerichts rührt wohl auch daher, dass es den Zugriff durch die Strafverfolgungsbehörden ausser Acht lässt.

45 Ebd. E. 8.1.

46 Dieses Argument dürfte wohl etwas zu kurz greifen, da Art. 36 BV neben dem Erfordernis der gesetzlichen Grundlage auch explizit die Verhältnismässigkeit einer Massnahme verlangt. Vgl. auch oben Rn. 7.

47 Siehe dazu Rn. 14 ff.

48 Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018, E. 8.2.2.

49 Ebd. E. 8.3.2. f.

50 Ebd. E. 8.3.4. ff.

51 Ebd. E. 8.3.9.

52 Siehe dazu die Beschwerde der Digitalen Gesellschaft.

53 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kom-

2006/24) verbundenen Eingriff in die Grundrechte[54] der betroffenen Personen als «schwerwiegend». Zudem wurde die Vorratsdatenspeicherung, wonach u.a. die Verkehrs- sowie Standortdaten[55] von den Mitgliedstaaten vorrätig zu speichern sind, als geeignet betrachtet, bei den BürgerInnen das Gefühl zu erwecken, im privaten Bereich ständig überwacht zu werden.[56]

24 Nachdem der EuGH die vorliegende Vorratsdatenspeicherung zwar als eine geeignete Massnahme hinsichtlich des angestrebten Zwecks – der Bekämpfung schwerer Kriminalität – bejaht hatte, verneinte er allerdings die Erforderlichkeit der Vorratsdatenspeicherung gemäss der genannten Richtlinie.[57] Diesbezüglich äusserte sich das Gericht dahingehend, dass Eingriffe in die Grundrechte auf das «absolut Notwendige» zu beschränken seien.[58] Des Weiteren führte das Gericht aus, dass von der besagten Richtlinie generell «alle Personen», «alle elektronischen Kommunikationsmittel» sowie auch «sämtliche Verkehrsdaten» betroffen seien und weder eine «Differenzierung, Einschränkung noch eine Ausnahme» vorgesehen sei.[59] Denkbar seien Einschränkungen beispielsweise bezüglich des Zeitraums, «eines bestimmten geografischen Gebiets» sowie des Personenkreises.[60]

25 Ausserdem bemängelte der EuGH, dass in der Richtlinie 2006/24 keine Möglichkeit vorgesehen ist, den Zugang zu den Daten seitens der nationalen Behörden zu beschränken.[61] Des Weiteren seien in der Richtlinie 2006/24 im Allgemeinen keine materiell- und verfahrensrechtlichen Voraussetzungen in Bezug auf den Zugang der nationalen Behörden zu den Daten enthalten. Vielmehr ermächtige die Richtlinie die Mitgliedstaaten, das entsprechende Verfahren sowie die diesbezüglichen Bedingungen zu definieren.[62] Hinzu komme, dass keine Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle vorgesehen sei, welche den Zweck und die Notwendigkeit vor der Einsichtnahme der nationalen Behörde in die Daten überprüfen und allenfalls beschränken darf.[63]

26 Auch hinsichtlich der Dauer der Speicherung (min. sechs bis max. 24 Monate) bemängelte der EuGH, dass der allfällige Nutzen der Daten bei der Speicherdauer nicht berücksichtigt werde und zudem bezüglich der Festlegung der doch sehr langen Speicherdauer keine Kriterien vorgesehen seien, welche diese auf das absolut Notwendige beschränkten.[64]

27 Vor dem Hintergrund der grossen Menge an Daten, deren Sensibilität sowie der Missbrauchsgefahr kritisierte der EuGH weiter, dass die Richtlinie 2006/24 keine spezifischen Vorgaben in Bezug auf die Datensicherheit enthalte. Ausserdem sei

munikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13. April 2006, S. 54 ff.

54 Art. 7 und 8 Charta der Grundrechte der Europäischen Union, ABl. 2012 C 326/391 vom 26. Oktober 2012.

55 Art. 2 Abs. 2 lit. a und Art. 5 der Richtlinie 2006/24 (Fn. 53).

56 Urteil des EuGH Rs. C-293/12 und 0594/12 vom 8. April 2014 (Digital Rights gegen Ireland), Rn. 37.

57 Ebd. Rn. 45 ff.

58 Ebd. Rn. 52.

59 Ebd. Rn. 56 f., explizit erwähnt wurde hier das Berufsgeheimnis, Rn. 58.

60 Ebd. Rn. 59.

61 Ebd. Rn. 60.

62 Ebd. Rn. 61.

63 Ebd. Rn. 62.

64 Ebd. Rn. 63 f.

keine entsprechende Verpflichtung für die Mitgliedstaaten vorgesehen, diesbezüglich Bestimmungen zu erlassen.[65] Des Weiteren seien auch die AnbieterInnen der entsprechenden Dienste nicht gehalten, mittels technischer und organisatorischer Massnahmen für ein angemessenes Schutzniveau zu sorgen. Vielmehr dürften diese sogar wirtschaftliche Gründe beim Erlass von Sicherheitsmassnahmen berücksichtigen. Zudem sei die unwiderrufliche Löschung der Daten durch die AnbieterInnen mittels der Richtlinie 2006/24 nicht gewährleistet.[66] Aufgrund dieser Mängel erklärte der EuGH die Richtlinie 2006/24 wegen der Nichteinhaltung des Verhältnismässigkeitsgrundsatzes für ungültig.[67]

28 Da in der Folge der Ungültigerklärung der Richtlinie 2006/24 ein Betreiber elektronischer Kommunikationsdienste davon absah, weiterhin die erwähnten Daten auf Vorrat zu speichern und die gespeicherten zu löschen, befasste sich der EuGH im Urteil vom 21. Dezember 2016[68] erneut – jedoch diesmal im Rahmen der Richtlinie 2002/58[69] – mit der Vorratsdatenspeicherung.[70] Dabei hielt der EuGH fest, dass die gespeicherten Daten Rückschlüsse auf das Privatleben von Personen zulassen. So könnten u.a. die Angaben bezüglich der Aufenthaltsorte sowie des sozialen Umfelds die Erstellung eines Profils der Person ermöglichen. Dabei handle es sich um ebenso sensible Angaben wie beim eigentlichen Inhalt der Kommunikation.[71] Im besagten Urteil wies der EuGH zudem darauf hin, dass eine nationale Regelung, welche die Vorratsdatenspeicherung von Verkehrs-[72] und Standortdaten zwecks Bekämpfung schwerer Straftaten vorsehe, nicht grundsätzlich verboten sei. Diese müsse jedoch bezüglich der Datenarten, der Kommunikationsmittel, dem Personenkreis sowie der Speicherdauer auf das absolut Notwendige beschränkt werden. Eine «allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel» sei jedenfalls nicht mit der Richtlinie 2002/58 vereinbar.[73]

29 Diverser bereits anhängig gemachten Vorabentscheidungsersuchen ist zu entnehmen, dass die vorlegenden Gerichte der Mitgliedstaaten daran zweifeln, ob dem vorhin aufgezeigten Entscheid des EuGH tatsächlich ein generelles Verbot hinsichtlich einer anlasslosen Vorratsdatenspeicherung entnommen werden kann. Nun hat auch das Bundesverwaltungsgericht Leipzig beim EuGH die Frage aufgeworfen, ob eine nationale Regelung, welche eine anlasslose Vorratsda-

65 Ebd. Rn. 66.
66 Ebd. Rn. 67.
67 Ebd. Rn. 69 ff.
68 Urteil des EuGH Rs. C-203/15 und 0698/15 vom 21. Dezember 2016 (Tele2 gegen Sverige).
69 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 12. Juli 2002, S. 37 ff.
70 Urteil des EuGH Rs. C-203/15 und 0698/15 vom 21. Dezember 2016 (Tele2 gegen Sverige) (Fn. 68), Rn. 44 ff.
71 Ebd. Rn. 98 f.
72 Gemäss Art. 2 lit. b der Richtlinie 2002/58 (Fn. 69) handelt es sich dabei um «Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden».
73 Urteil des EuGH Rs. C-203/15 und 0698/15 vom 21. Dezember 2016 (Tele2 gegen Sverige) (Fn. 68), Rn. 108 ff. m.w.H.

tenspeicherung vorsehe, nie gemäss Art. 15 Abs. 1 der Richtlinie 2002/58/EG gerechtfertigt werden könne. Ein solches Verbot würde zu einer nicht unbeachtlichen Einschränkung der nationalen Befugnisse der Mitgliedstaaten im Bereich der Strafverfolgung sowie der öffentlichen Sicherheit gemäss Art. 4 Abs. 2 Satz 3 EUV führen. Die infrage stehende gesetzliche Regelung in Deutschland beschränkt die Speicherpflicht im Gegensatz zu den bisher vom EuGH überprüften nationalen Gesetzen auf weniger Kommunikationsmittel und weist eine kürzere Speicherdauer auf (vier resp. zehn Wochen). Ausserdem wurde der Datenschutz gestärkt sowie der Zugang zu den Daten streng reguliert. Bis anhin hat sich der EuGH noch nicht zu dieser Fragestellung geäussert.[74]

3. Rechtsprechung in EU-Mitgliedstaaten

30 In den einzelnen Mitgliedstaaten der EU wird die Frage nach einer gesetzlichen Regelung einer Vorratsdatenspeicherung sehr unterschiedlich beantwortet. Während Länder wie z.B. Österreich, Niederlande und Slowenien keine Vorratsdatenspeicherung zulassen, sind in vielen Ländern entsprechende Regelungen vorgesehen, gegen welche jedoch teilweise noch Beschwerden bei den nationalen Gerichten hängig sind.[75]

4. Rechtsprechung des EGMR

31 Aufgrund der Snowden-Enthüllungen hatte sich der EGMR zu den Überwachungsmassnahmen in Grossbritannien zu äussern.[76]

32 Der EGMR kam in seinem Urteil vom 13. September 2018 zum Schluss, dass es grundsätzlich im Ermessen der Vertragsparteien stehe, ein Massenüberwachungssystem («bulk interception regime») zu betreiben. Da solche Systeme jedoch ein grosses Missbrauchspotenzial besässen, seien gewisse Mindeststandards zu erfüllen.[77]

33 Neben anderen Aspekten der in Grossbritannien erlassenen Überwachungsmassnahmen beurteilte der EGMR die gesetzlich vorgesehene Massenüberwachung von dazugehörigen Kommunikationsdaten («related communications data»), also von Angaben bezüglich der Person, dem Zeitpunkt sowie dem Ort der jeweiligen Kommunikation.[78]

34 Entgegen der Ansicht der britischen Regierung befand der EGMR, dass diese Daten nicht weniger in die Rechte der betroffenen Personen eingreifend («less intrusive») seien als Daten bezüglich des Inhalts der Kommunikation. Vielmehr hielt der Gerichtshof fest, dass der Inhalt verschlüsselt werden könne, wobei auch die Entschlüsselung des Inhalts nicht unbedingt Informationen hinsichtlich des Senders oder Empfängers hervorbringe. Die dazugehörigen Kommunikationsdaten hingegen geben Auskunft über die Identität der KommunikationsteilnehmerInnen, deren Aufenthaltsort sowie das Kommunikationsmittel. Werden solche Daten nun in grosser Menge

74 Pressemitteilung Nr.66/2019 des Bundesverwaltungsgerichts vom 25. September 2019.

75 Vgl. dazu Mrohs Lorenz/Meister Andre/Biselli Anna/Fanta Alexander, Vorratsdatenspeicherung in Europa: Wo sie in Kraft ist und was die EU plant vom 4. Juni 2019.

76 Urteil des EGMR Nr. 58170/13, 62322/14 und 24960/15 vom 13. September 2018 (Big Brother and others v. the United Kingdom).

77 Ebd. § 307, 314 f.

78 Ebd. § 348.

gesammelt, so ergebe sich daraus ein umfassendes Bild einer Person.[79]

35 In casu hielt der EGMR zwar fest, dass mit dem Zugriff auf die dazugehörigen Kommunikationsdaten ein wichtiges Instrument zur Bekämpfung von Terrorismus sowie schwerer Straftaten bestehe. Er bemängelte jedoch, dass keine Schutzmassnahmen bezüglich der Bearbeitung dieser Daten vorgesehen seien. Somit sei nicht von einem Gleichgewicht zwischen öffentlichen und privaten Interessen auszugehen.[80] Im Rahmen der – eher kurz gehaltenen – Verhältnismässigkeitsprüfung betonte der EGMR gleichwohl, dass es keine Alternative zur Massenüberwachung gebe.[81] Der EGMR bejahte unter Berücksichtigung der vorgenannten Umstände eine Verletzung von Art. 8 EMRK.[82] Der Fall wurde an die Grosse Kammer des EGMR weitergezogen.[83]

5. Fragmentierung der aufgezeigten Rechtsprechung

36 Die Beurteilungen des Bundesgericht, des EuGH sowie des EGMR hinsichtlich der Vorratsdatenspeicherung weisen – teilweise beachtliche – Unterschiede auf. Im Folgenden soll nur auf ausgewählte Punkte eingegangen werden.

37 Grundlegend anders bewerteten die Gerichte die Bedeutung von Randdaten[84]. Während das Bundesgericht die Speicherung und Aufbewahrung dieser Daten im Vergleich zu Daten bezüglich des Inhaltes der Kommunikation als weniger einschneidend bezeichnete, sind im Gegensatz dazu der EuGH sowie der EGMR der Ansicht, dass auch aus diesen Angaben wertvolle Informationen gewonnen werden können. Sie setzen deshalb die Randdaten betreffend ihren «Informationswert» den inhaltsbezogenen Daten der Kommunikation gleich. Der EGMR geht sogar noch weiter, indem er betont, dass die Inhaltsüberwachung nicht immer «nützliche» Informationen liefert, die Randdaten – in ihrer Fülle – jedoch weitreichende Auskünfte ermöglichen.[85]

38 Ferner lässt sich zur generellen Zulässigkeit einer anlasslosen Vorratsdatenspeicherung ausführen, dass gemäss dem EGMR Massenüberwachungssysteme grundsätzlich eingesetzt werden dürfen, jedoch gewisse Sicherheitsmassnahmen resp. Kontrollinstanzen vorzusehen sind. In der EU hingegen scheint die Frage nach der generellen Zulässigkeit einer anlasslosen Vorratsdatenspeicherung –

---

79 Ebd. § 356.

80 Ebd. § 355 ff. Vgl. auch Beitrag «Big Brother Watch and others v. the United Kingdom: A Victory of Human Rights over Modern Digital Surveillance» auf verfassungsblog.de.

81 Urteil des EGMR Nr. 58170/13, 62322/14 und 24960/15 vom 13. September 2018 (Big Brother and others v. the United Kingdom) (Fn. 76), § 384 ff.

82 Ebd. § 388. Es ist jedoch zu beachten, dass sich die gesetzliche Regelung im Laufe des Verfahrens vor dem EGMR geändert hatte und sich der EGMR nicht mit diesen Änderungen zu befassen hatte. Vgl. dazu Beitrag vom 13. September 2018 von Netzpolitik.org.

83 Press release ECHR 258 (2019) vom 10. Juli 2019; vgl. dazu auch Grand Chamber hearing vom 10. Juli 2019.

84 Es wird im Folgenden der Begriff Randdaten verwendet, auch wenn teilweise andere Bezeichnungen wie Verkehrsdaten und dazugehörige Kommunikationsdaten zur Anwendung kommen. Die Autorin enthält sich der Aussage, ob es sich dabei jeweils exakt um die gleichen Daten handelt oder ob kleine Abweichungen in den Definitionen bestehen. Die Unterscheidung ist für den vorliegenden Beitrag jedoch nicht weiter von Relevanz.

85 Vgl. dazu auch Beitrag «Big Brother Watch and others v. the United Kingdom: A Victory of Human Rights over Modern Digital Surveillance» auf verfassungsblog.de.

wie oben aufgeführt – noch nicht abschliessend geklärt zu sein. Sollte sich der EuGH für ein generelles Verbot aussprechen, so würde die Rechtsprechung des EGMR sowie des EuGH in einem zentralen Punkt voneinander abweichen.[86]

39 Die in der Schweiz vorgenommene Vorratsdatenspeicherung der Randdaten ist insbesondere aufgrund der systematischen und verdachtsunabhängigen Vornahme heikel. Unter Berücksichtigung der Rechtsprechung des EGMR wäre die Massnahme als solche grundsätzlich zulässig. Fraglich bleibt jedoch, ob die aktuelle Ausgestaltung in der Schweiz den geforderten Schutzvorkehrungen resp. Einschränkungen entspricht. Hinsichtlich der Rechtsprechung des EuGH ist festzuhalten, dass diese zwar für die Schweiz nicht verbindlich ist, aber dennoch grundsätzlich Auswirkungen auf die Interpretation der EMRK haben kann. Diese wiederum ist von der Schweiz einzuhalten.[87]

40 Auffällig ist zudem, dass sich alle drei Gerichte kaum mit der Frage der effektiven Wirksamkeit der Massenüberwachung von Randdaten im Rahmen der Strafbekämpfung auseinandergesetzt haben.[88]

IV. Ausgewählte Aspekte der Verhältnismässigkeit

41 Auch unter Berücksichtigung der Rechtsprechung des EuGH sowie des EGMR wird im Folgenden noch auf ausgewählte Aspekte der Verhältnismässigkeit der Vorratsdatenspeicherung in der Schweiz eingegangen.

1. Wirksamkeit der Vorratsdatenspeicherung von Randdaten

42 Gemäss den genannten Urteilen sind die Gerichte meist ohne grosse Kommentierung von der Wirksamkeit resp. Eignung der Vorratsdatenspeicherung im Bereich der Kriminalitätsbekämpfung ausgegangen.[89] Eine solche Beurteilung ist vielschichtig. So muss u.a. danach gefragt werden, wie viele Delikte ohne die Überwachung nicht hätten geklärt werden können, wie viele Drittpersonen ebenfalls von der Überwachung betroffen sind oder inwiefern sich Umgehungsmassnahmen auf die Wirksamkeit niederschlagen (Verlagerung der Kriminalität auf Orte, welche nicht überwacht werden).[90] Vor diesem Hintergrund drängt sich eine Suche nach entsprechenden Statistiken auf.

a) Datenerhebungen in der Schweiz

43 In der Schweiz werden seit dem Jahr 2009 vom Bundesamt für Statistik (BfS) landesweit Daten bezüglich der Aufklärungsquote von Straftaten erhoben.[91] Da

---

86 Vgl. dazu Pressemitteilung (Fn. 74); Christakis Theodore, a fragmentation of eu/echr law on mass surveillance: initial thoughts on the big brother watch judgment, vom 20. September 2018.

87 Vgl. dazu auch Epiney Astrid, Staatliche Überwachung versus Rechtsstaat: Wege aus dem Dilemma?, in: AJP 2016, S. 1507.

88 Vgl. dazu immerhin Urteil des EGMR Nr. 58170/13, 62322/14 und 24960/15 vom 13. September 2018 (Big Brother and others v. the United Kingdom) (Fn. 76), § 384 ff.

89 Vgl. dazu Schlauri Simon/Ronzani Daniel, EuGH: Vorratsdatenspeicherungsrichtlinie 2006/24/EG für ungültig erklärt, in: sic 2014, S. 576.

90 Vgl. Rudin (Fn. 30), S. 435.

91 Vgl. dazu z.B. Polizeiliche Kriminalstatistik (PKS), Jahresbericht 2018 der polizeilich registrierten Straftaten, Neuchâtel 2019, S. 75. Diese Statistiken sind jedoch mit Vorsicht zu genies-

die Vorratsdatenspeicherung von Randdaten bereits im Jahr 2002 eingeführt wurde, kann also aus diesen Statistiken keine Aussage darüber entnommen werden, ob diese Massnahme zur Erhöhung der Aufklärungsquote beigetragen hat.

44 Fedpol äusserte sich im Jahr 2009 dahingehend, dass die technische Entwicklung die Identifikation von InternetteilnehmerInnen erschwere, weshalb trotz der Randdatenspeicherung eine eindeutige Identifikation der Person teilweise nicht möglich sei.[92]

45 Obwohl diese Erkenntnis die Wirksamkeit der Erhebung von Randdaten zumindest infrage stellen kann, muss festgehalten werden, dass in der Schweiz keine aussagekräftige Statistik vorliegt, welche belegt, dass die Vorratsdatenspeicherung in der Strafverfolgung tatsächlich von Nutzen ist oder eben nicht. [93]

b) Gutachten Max-Planck-Institut

46 Aufgrund der Entwicklung der Rechtsprechung in Deutschland im Bereich der Vorratsdatenspeicherung[94] wurde das Max-Planck-Institut beauftragt, ein Gutachten zu erstellen, welches die Vorratsdatenspeicherung von Randdaten in der Strafbekämpfung näher untersucht. Auch wenn sich dieses auf die Situation in Deutschland bezieht und deshalb nicht tel quel für die Schweiz übernommen werden kann, lohnt sich dennoch ein Blick auf die Erkenntnisse dieses Gutachtens.

47 Im Rahmen der Interviews mit den PraktikerInnen (z.B. PolizistInnen, RichterInnen) machten diese darauf aufmerksam, dass die Vorratsdatenspeicherung von Randdaten neben ihrem hauptsächlichen Zweck (Identifikation, Standortermittlung, Tatzeitbestimmung) auch anderweitig genutzt werden könne. So hätten u.a. Standortdaten für die Durchführung von Observationen ermittelt werden können, Aussagen hätten auf ihren Wahrheitsgehalt hin überprüft werden können (z.B. bei Alibis) und zudem hätten die Daten Personen anlässlich Vernehmungen vorgehalten werden können.[95]

48 Des Weiteren wurde die sechsmonatige Speicherungsfrist von den Personen in der Praxis als Untergrenze angesehen. Insbesondere im Bereich der organisierten Kriminalität resp. des Staatsschutzes seien sogar längere Speicherungsfristen wünschenswert, um die Täterstrukturen besser aufdecken zu können.[96]

49 Gemäss den Aussagen der befragten RichterInnen hätten die retrograden Daten oft zu Erkenntnissen geführt, welche bezüglich der Überführung von TäterInnen zentral gewesen seien. Konkrete Zahlen, welche dies belegen würden, fehlen jedoch.[97]

sen, da gewisse Straffälle als aufgeklärt gelten, obwohl sie es eigentlich gar nicht sind. Vgl. dazu Baumgartner Fabian, Wundersam hohe Aufklärungsquote, NZZ vom 3. Dezember 2012.

92 Bundesamt für Polizei fedpol: Kriminalitätsbekämpfung Bund, Jahresbericht 2009, Bern 2010, S. 28 f.

93 Györffi (Fn. 15), S. 21.

94 Siehe dazu BVerfGE 125, 260.

95 Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, Gutachten, 2. erweiterte Fassung, Freiburg i.Br., Juli 2011, S. 159.

96 Ebd. S. 162.

97 Ebd. S. 172.

50 Das Gutachten hob zudem hervor, dass Aussagen betreffend die quantitative Abfrage solcher Daten mangels umfassender statistischer Erhebungen nicht einfach getroffen werden können. Im Bereich der Strafverfolgung seien solche Abfragen äusserst selten erfolgt, wobei hauptsächlich Daten des vergangenen Monats abgefragt worden seien. Das Abfrageverhalten der zugriffsberechtigten Behörden zeige zudem regionale Unterschiede.[98]

51 Des Weiteren ist dem Gutachten zu entnehmen, dass die Vorratsdatenspeicherung von Randdaten insbesondere bei solchen Straftaten hilfreich sei, wo die kriminelle Person zuerst noch identifiziert werden müsse. Löst hingegen eine physisch anwesende Person direkt den Anfangsverdacht bezüglich einer Straftat aus, so sei der Nutzen der Einsicht in die Randdaten nicht von gleicher Bedeutung.[99]

52 Anhand der vorhandenen Daten konnte letztlich kein Einfluss der Vorratsdatenspeicherung der Randdaten auf die Aufklärungsquote festgestellt werden.[100] Auch seien keine Hinweise erkennbar, dass auf Vorrat gespeicherte Daten zur Verhinderung von Terroranschlägen beigetragen hätten.[101] Die Wirksamkeit der vorliegenden Vorratsdatenspeicherung konnte somit im Gutachten nicht empirisch belegt werden.

c) Evaluationsbericht der Europäischen Kommission

53 Der Evaluationsbericht der Europäischen Kommission[102] bezüglich der Richtlinie 2006/24 misst insbesondere älteren Daten im Rahmen der Ermittlungstätigkeit grosse Bedeutung zu (so beispielsweise bei langer Planung einer Straftat, um Komplizen zu identifizieren oder Zusammenhänge zwischen unterschiedlichen Straftaten zu entdecken). Zudem seien die Mitgliedstaaten der Ansicht, dass die Vorratsdatenspeicherung von Randdaten in der Kriminalitätsbekämpfung generell wertvoll sei.[103]

54 Die von den Mitgliedstaaten für den Evaluationsbericht der Europäischen Kommission zur Verfügung gestellten Daten beziehen sich jedoch nicht ausschliesslich auf die Vorratsdatenspeicherung von Randdaten. Demnach lassen sich keine Schlüsse daraus ziehen, inwieweit die Einsichtnahme in Randdaten zu Erfolgen in den strafrechtlichen Ermittlungen beigetragen hat. Des Weiteren wurden die Daten keinen bestimmten Delikten zugeordnet, weshalb nicht geprüft werden kann, ob die Vorratsdatenspeicherung tatsächlich nur für die Aufklärung von «schweren» Delikten benutzt wird.[104]

d) Schlussfolgerung

55 Aus subjektiver Sicht der Personen aus der Praxis fällt das Fazit zum Nutzen der Vorratsdatenspeicherung von Randdaten in der Kriminalitätsbekämpfung positiv aus.

98 Ebd. S. 44 ff.
99 Ebd. S. 71 ff.
100 Ebd. S. 219 ff.
101 Ebd. S. 219.

102 Bericht der Kommission an den Rat und das Europäische Parlament, Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG), KOM (2011) 225 endgültig, vom 18. April 2011.
103 Ebd. S. 26 ff.
104 Max-Planck-Institut, Gutachten (Fn. 95), S. 130 ff.

56 Wie aufgeführt, lässt sich jedoch die Wirksamkeit der Vorratsdatenspeicherung von Randdaten empirisch nicht belegen. Dies ist darauf zurückzuführen, dass die benötigten Daten schlichtweg nicht erhoben werden. Trotzdem ist wohl aufgrund der Aussagen der PraktikerInnen im Rahmen des genannten Gutachtens davon auszugehen, dass die Vorratsdatenspeicherung der Randdaten in der Strafbekämpfung nicht gänzlich unnützlich ist.

57 Zu beachten ist dennoch, dass – wie oben aufgezeigt – zumindest in Deutschland in der Strafbekämpfung relativ wenige Abfragen der Randdaten erfolgen. Empirisch belegte Aussagen hinsichtlich der Wirksamkeit der Vorratsdatenspeicherung der Randdaten in der Kriminalitätsbekämpfung sowie zur quantitativen Abfrage wären aber von zentraler Bedeutung bei der Beurteilung der Verhältnismässigkeit der vorliegenden Vorratsdatenspeicherung. So dürfte doch eine Massnahme, welche keine resp. eine geringe Wirksamkeit bezüglich des angestrebten Zwecks aufweist und von dieser zudem nur in Einzelfällen Gebrauch gemacht wird, vor dem Hintergrund der grossen Anzahl der betroffenen Personen und der Menge der gesammelten Daten zumindest fraglich erscheinen.

2. Mildere Massnahmen

58 Gerade weil die Vorratsdatenspeicherung der Randdaten auf eine grosse Menge von Daten abzielt, wovon aber nur sehr wenige gebraucht werden, stellt sich die Frage, ob nicht eine weniger invasive Massnahme zur Verfügung stehen würde. Diesbezüglich wird das Quick-Freeze-Verfahren als Alternative genannt.[105]

a) Quick-Freeze-Verfahren

59 Das Quick-Freeze-Verfahren unterscheidet sich insbesondere dahingehend vom aktuellen Verfahren bezüglich der Speicherung der Randdaten in der Schweiz, als bei letzterem retrograd auf gewisse Daten zugegriffen werden kann, beim Quick-Freeze-Verfahren hingegen zukunftsgerichtet bestimmte Daten, welche aktuell noch vorhanden sind, von der regulären Löschung ausgenommen werden.[106]

60 Das Quick-Freeze-Verfahren ist im Rahmen der sog. Cybercrime Konvention[107] im Bereich der Bekämpfung der Computerkriminalität im Einsatz. Vorausgesetzt wird ein spezifischer Verdachtsfall, aufgrund dessen die zuständige Behörde die Speicherung der benötigten Daten anordnet. Die Anordnung bewirkt, dass die genannten Daten nicht wie vorgesehen gelöscht, sondern für eine bestimmte Zeit gespeichert werden. Dadurch wird der anordnenden Behörde Zeit verschafft, die vorgesehenen Berechtigungen einzuholen. Erst durch einen Richterspruch erhält die anordnende Behörde allenfalls Einsicht in die «eingefrorenen» Daten.[108]

61 Einig waren sich die PraktikerInnen, welche im Rahmen des Gutachtens vom Max-Planck-Institut befragt worden sind, dass das Quick-Freeze-Verfahren keine Alternative zur Vorratsdatenspeicherung

[105] Ebd. S. 41. Der Autorin sind keine weiteren Alternativen bekannt.
[106] Ebd. S. 41.
[107] Art. 16 des Übereinkommens des Europarates über Computerkriminalität, CETS 185, unterzeichnet am 23. November 2001 in Budapest.
[108] Max-Planck-Institut, Gutachten (Fn. 95), S. 38 ff.

darstellt. Sie begründeten diese Ansicht damit, dass mit dem Quick-Freeze-Verfahren die für die Ermittlung benötigten Daten – also die retrograden Daten – nicht erhältlich gemacht werden könnten.[109] Auch in der Schweiz wird mehrheitlich die rückwirkende Überwachung verwendet.[110]

b) Schlussfolgerung

62 Da beim Quick-Freeze-Verfahren lediglich ausgewählte Daten gespeichert und alle übrigen regulär gelöscht werden, ist dieses Verfahren als grundsätzlich milder im Hinblick auf die Eingriffsintensität als die systematische Vorratsdatenspeicherung zu werten. Es ist jedoch nicht von der Hand zu weisen, dass dabei nicht dieselben Daten wie bei der Vorratsdatenspeicherung erhältlich gemacht werden können. Wie jedoch bereits ausgeführt, fehlen entsprechende Studien, inwiefern die retrograden Daten von Bedeutung in der Strafbekämpfung sind. Jedoch auch in Bezug auf die im Quick-Freeze-Verfahren gewonnenen Daten fehlt eine entsprechende empirische Grundlage. Somit kann keine Aussage darüber gemacht werden, ob und inwiefern das Quick-Freeze-Verfahren eine wirksame Alternative zur Vorratsdatenspeicherung darstellt.

3. Beschränkung der Vorratsdatenspeicherung

63 Wie insbesondere der Rechtsprechung des EuGH entnommen werden kann, werden Einschränkungen hinsichtlich der Datenerhebung (z.B. Zeitraum, Örtlichkeit, Personenkreis) verlangt.[111]

64 Übertragen auf die Schweiz, ist also danach zu fragen, inwiefern die Menge der Daten, welche auf Vorrat gespeichert werden, reduziert werden kann, um die Vorratsdatenspeicherung auf das absolut Notwendige zu beschränken.

65 Denkbar wäre diesbezüglich eine Kürzung der Speicherfrist von aktuell sechs Monaten.[112] So wurde beispielsweise in Deutschland die Aufbewahrungsdauer von Standortdaten auf vier und diejenige der allgemeinen Verkehrsdaten auf zehn Wochen reduziert.[113] Anhand einer Auswertung der eingesehenen Daten könnte zudem eine Beurteilung erfolgen, welche Daten regelmässig für die Strafverfolgung nicht nützlich sind und somit nicht mehr von der Vorratsdatenspeicherung erfasst werden müssten.

66 Eine Beschränkung könnte auch bei den Zugriffsmöglichkeiten erfolgen (wobei in diesem Fall nicht weniger Daten gespeichert werden würden). So könnten die im Straftatenkatalog[114] aufgeführten Delikte, für deren Aufklärung die Überwachung des Fernmeldeverkehrs vorgesehen ist, angepasst werden. Einerseits könnte eine Reduktion auf Strafnormen erfolgen, für welche der Zugriff auf Randdaten sinn-

[109] Ebd. S. 227.
[110] Vgl. dazu Statistik der Bundesverwaltung.
[111] Urteil des EuGH Rs. C-293/12 und 0594/12 vom 8. April 2014 (Digital Rights gegen Ireland) (Fn. 56), Rn. 59. Vgl. dazu auch Schlauri/Ronzani (Fn. 89), S. 576 f.
[112] Die Botschaft zum neuen BÜPF sah noch eine Verlängerung der Speicherfrist auf zwölf Monate vor. Vgl. dazu BBl 2013 2683 (Fn. 5), S. 2686.
[113] Vgl. dazu Gastbeitrag bei der Friedrich Haumann Stiftung zum Vorlagebeschluss des 6. Senats des Bundesverwaltungsgerichts in Sachen Vorratsdatenspeicherung.
[114] Art. 269 StPO; Straftatenkatalog.

voll erscheint.[115] Andererseits könnte die Überwachung auf besonders schwere Kriminalität begrenzt werden. So könnten wenigstens die Vergehen vom Deliktskatalog gestrichen werden.[116]

4. Datensicherheit

67 In Anbetracht der grossen Menge von Daten, welche die Mitwirkungspflichtigen gemäss Art. 2 BÜPF zu speichern haben und für die sie bis zur Übergabe an den Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) die Verantwortung haben, stellt sich auch die Frage nach der Datensicherheit.[117] Diese kann generell mittels technischer sowie auch organisatorischer Vorkehrungen gewährleistet werden.[118]

68 Ohne im Folgenden im Einzelnen auf die einschlägigen gesetzlichen Bestimmungen betreffend die Datensicherheit und das Abrufverfahren im Bereich der Vorratsdatenspeicherung der Randdaten eingehen zu wollen,[119] soll nur kurz die Problematik der Übermittlung der Daten an sich thematisiert werden.

69 Aufgrund der zunehmenden Menge gesammelter Daten werden diese nicht mehr wie bis anhin gespeichert auf einem Datenträger per Post verschickt, sondern im Dienst ÜPF in einem Informatiksystem für eine gewisse Zeit aufbewahrt. Die Daten können schliesslich per Online-Zugriff nicht nur von den Strafverfolgungsbehörden, sondern auch von den Parteien (also der beschuldigten Person und deren rechtlichen Vertretung) abgerufen werden.[120]

70 Dieses Informatiksystem bringt hinsichtlich der grossen Datenmengen wohl eine einfachere Handhabung mit sich. Trotzdem stellen sich auch hier datenschutzrechtliche Fragen (z.B. personelle sowie technische Zugriffsmöglichkeiten, Schutz vor Missbrauch etc.). Nicht unbedenklich ist zudem die Möglichkeit, die im Informatiksystem des Dienstes ÜPF gespeicherten Daten in andere Informationssysteme zu «kopieren».[121]

5. Sicherheit vs. Privatsphäre

71 Vorliegend handelt es sich letztlich um eine schwierige Abwägung zwischen Strafverfolgungseffizienz, Sicherheit sowie dem (grundrechtlichen) Schutz der betroffenen Personen.[122] Mit der Steigerung der Sicherheit ist jedoch oftmals eine Einschränkung der Freiheit Einzelner verbunden.[123]

72 Die höchstrichterliche Rechtsprechung gewichtet das öffentliche Interesse oftmals höher, sofern jedenfalls der Nutzen der Daten nicht vollkommen ausgeschlossen werden kann.[124] Da das Sicherheitsbedürfnis allgemein einen hohen Stellenwert hat, besteht jedoch die Gefahr, dass dieses als überwiegendes Interesse jeden Eingriff zu rechtfertigen

115 Vgl. dazu Max-Planck-Institut, Gutachten (Fn. 95), S. 71 ff.
116 Vgl. dazu Art. 10 StGB und z.B. Art. 180 (Drohung) und Art. 181 (Nötigung) StGB. Vgl. auch Schlauri/Ronzani (Fn. 89), S. 577.
117 Art. 12 Abs. 3 BÜPF.
118 Vgl. dazu Art. 7 DSG.
119 Vgl. dazu das Urteil des Bundesgerichts 1C_598/2016 vom 2. März 2018, E. 8.3.5.
120 BBl 2013 2683 (Fn. 5), S. 2695. Vgl. zu den Einzelheiten Art. 6 ff. BÜPF.
121 Vgl. dazu Art. 14 f. BÜPF.
122 Vgl. dazu Max-Planck-Institut, Gutachten (Fn. 95), S. 2.
123 Sigrist (Fn. 28), S. 257.
124 Vgl. dazu Urteil des Bundesgericht 1C_439/2011 vom 25. Juni 2012 E. 6.3.

droht.[125] Das «Terrorismusargument» hat denn schon zu der Akzeptanz einer neuen Regelung verholfen, welche einige Zeit davor noch abgelehnt worden war.[126]

73 Die Gewichtung der einzelnen Interessen ist nicht primär eine rechtliche, sondern vielmehr eine gesellschaftliche Frage.[127] Dies wird auch durch die oben aufgezeigte unterschiedliche Beurteilung der Vorratsdatenspeicherung durch die nationalen Gerichte der Mitgliedstaaten der EU deutlich.[128]

V. Fazit und Ausblick

74 Die dargelegte Thematik zeigt anschaulich das Spannungsverhältnis zwischen der Gewährleistung der grösstmöglichen Sicherheit und dem grundrechtlichen Schutz der Privatsphäre auf. Angestrebt werden soll ein Ausgleich zwischen Freiheit und Sicherheit.[129]

75 Im Bereich der Vorratsdatenspeicherung von Randdaten werden diesbezüglich in Europa jedoch divergierende Meinungen vertreten. So veranschaulicht ein Vergleich der oben aufgezeigten Rechtsprechung des Bundesgerichts, des EGMR sowie des EuGH, dass die Gewichtung dieser Interessen deutlich anders ausfallen kann.

76 Gemäss den obigen Ausführungen erscheint es fraglich, ob der erwähnte Entscheid des Bundesgerichts – insbesondere aufgrund der systematischen und anlasslosen Vornahme der vorliegenden Vorratsdatenspeicherung – mit der dargelegten Rechtsprechung des EGMR vereinbar ist. Ob und inwiefern die Vorratsdatenspeicherung der Randdaten in der Schweiz angepasst werden muss, werden in hoffentlich absehbarer Zeit die RichterInnen in Strassburg entscheiden.

77 Zu beachten gilt es ferner, dass durch den technologischen Fortschritt die Datenbearbeitung sowohl durch Private als auch durch staatliche Behörden stets zunimmt und es für die betroffenen Personen zunehmend schwieriger wird, den Umfang der Bearbeitung ihrer Daten zu erkennen. Dies führt zu einem gewissen Kontrollverlust der BürgerInnen. Im Sicherheitsbereich hat sich die Situation seit dem 11. September 2001 verschärft. Insbesondere im Namen der Terrorismusbekämpfung wird der Datenschutz vermehrt eingeschränkt, wobei die Tendenz in Richtung der Überwachung aller abzielt. Zu beobachten ist auch, dass sich der Schutz der öffentlichen Sicherheit zusehends von repressiven zu präventiven Massnahmen verlagert. Angesichts dieser Entwicklungen ist es umso wichtiger, dass das Sicherheitsbedürfnis[130] gegenüber den Menschenrechten nicht ein übermächtiges Gewicht einnimmt.[131] Schliesslich stehen die gemäss Art. 2 BV aufgeführten Staatszwecke Freiheit und Sicherheit gleichwertig nebeneinander.[132]

---

125 Sigrist (Fn. 28), S. 254 f.
126 Vgl. dazu Rudin (Fn. 30), S. 434, wo die Registrierung von Prepaid-Karten genannt wird.
127 Sigrist (Fn. 28), S. 267.
128 Siehe oben Rn. 20; Max-Planck-Institut, Gutachten (Fn. 95), S. 6.
129 Vgl. dazu auch Epiney (Fn. 87), S. 1512 ff.
130 Es gilt jedoch zu beachten, dass gemäss Art. 5 EMRK auch ein Recht auf Sicherheit normiert wird.
131 Vgl. dazu Sigrist (Fn. 28), S. 1 ff.
132 Ebd. S. 253. Vgl. dazu auch Art. 5 EMRK.