Peyrot, Schlegel & Györffy
Rechtsanwälte

Zürich, 15. Dezember 2016

Viktor Györffy
Rechtsanwalt
Beethovenstrasse 47
8002 Zürich
Telefon 044 240 20 55
Telefax 043 500 55 71
gyoerffy@psg-law.ch
www.psg-law.ch

Einschreiben
Bundesgericht
Mon Repos
1000 Lausanne 14

Sehr geehrte Frau Präsidentin, sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

In Sachen

,
,
Beschwerdeführer 1

,
,
Beschwerdeführer 2

,
,
Beschwerdeführer 3

,
,
Beschwerdeführer 4

,
,
Beschwerdeführer 5

,
,

Beschwerdeführer 6

gegen

Dienst Überwachung Post- und Fernmeldeverkehr,
Informatikservice Center ISC-EJPD,
Fellerstrasse 15, 3003 Bern,

Beschwerdegegner

sowie

Bundesverwaltungsgericht, Abteilung I,
Postfach, 9023 St. Gallen,

Vorinstanz

betreffend **Speicherung von Vorratsdaten der Fernmeldekommunikation**

erhebe ich hiermit

Beschwerde

gegen das Urteil des Bundesverwaltungsgerichts, Abteilung I, vom 9. November 2016 mit folgenden

Anträgen:

1. Das Urteil der Vorinstanz vom 9. November 2016 sei aufzuheben.

2. Die Swisscom (Schweiz) AG (in Bezug auf Beschwerdeführer 1, Beschwerdeführer 2, Beschwerdeführer 3 und Beschwerdeführer 5) bzw. die Sunrise Communications AG (in Bezug auf Beschwerdeführer 4 und Beschwerdeführer 6) seien anzuweisen, die gemäss Art. 15 Abs. 3 BÜPF gespeicherten Verkehrs- und Rechnungsdaten der Beschwerdeführer zu löschen und deren Speicherung in Zukunft zu unterlassen, soweit die betroffenen Daten nicht für die Erbringung der vertraglichen Leistungen gegenüber den Beschwerdeführern zwingend erforderlich sind.

3. Die Swisscom (Schweiz) AG (in Bezug auf Beschwerdeführer 1, Beschwerdeführer 2, Beschwerdeführer 3 und Beschwerdeführer 5)

bzw. die Sunrise Communications AG (in Bezug auf Beschwerdeführer 4 und Beschwerdeführer 6) seien anzuweisen bzw. zu verpflichten, keine gemäss Art. 15 Abs. 3 BÜPF gespeicherten Verkehrs- und Rechnungsdaten der Beschwerdeführer an den Dienst ÜPF oder an andere Behörden oder an Gerichte herauszugeben.

4. Eventualiter sei die Sache an die Vorinstanz oder an die Beschwerdegegnerin zurückzuweisen, damit sie im Sinne der Anträge verfahre;

unter Kosten- und Entschädigungsfolgen zu Lasten des Staates.

I. Formelles

1. Der unterzeichnende Rechtsanwalt ist zur Vertretung der Beschwerdeführer gehörig bevollmächtigt. Kopien der entsprechenden Vollmachten liegen dem Gesuch bei (s. **Beilagen 1 - 6**).

2. Die vorliegende Beschwerde erfolgt innert Frist (**s. Beilage 7**).

3. Wer ein schutzwürdiges Interesse hat, kann gemäss Art. 25a VwVG von der Behörde, die für Handlungen zuständig ist, welche sich auf öffentliches Recht des Bundes stützen und Rechte oder Pflichten berühren, verlangen, dass sie (a.) widerrechtliche Handlungen unterlässt, einstellt oder widerruft und (b.) die Folgen widerrechtlicher Handlungen beseitigt.

4. Die Speicherung der Daten beschlägt, wie nachstehend dargelegt wird, Grundrechte, welche durch die Europäische Menschenrechtskonvention (EMRK) geschützt sind. Damit muss – in Verbindung mit diesen Grundrechten – auch das Recht auf effektive Beschwerde gemäss Art. 13 EMRK gewahrt sein.

5. Gemäss Art. 15 Abs. 3 des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (nachfolgend: BÜPF) sind die Anbieterinnen von Fernmeldediensten verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten (nachfolgend: Metadaten) während sechs Monaten aufzubewahren.

6. Die Beschwerdeführer 1, Beschwerdeführer 2, Beschwerdeführer 3 und Beschwerdeführer 5 sind Kunden der Swisscom (Schweiz), die Beschwerdeführer 4 und Beschwerdeführer 6 Kunden der Sunrise

Communications AG (nachfolgend: Anbieterinnen). Die Anbieterinnen speichern demnach gestützt auf Art. 15 Abs. 3 BÜPF, d.h. gestützt auf öffentliches Recht des Bundes, während sechs Monaten die erwähnten Metadaten, die bei der Kommunikation der Beschwerdeführer anfallen.

7. Die Speicherung der Metadaten stellt einen erheblichen und unrechtmässigen Eingriff in die nachstehend (Ziff. II.C.) genannten Grundrechte dar.

8. Die Speicherung der Metadaten durch die Anbieterinnen berühren somit Grundrechte der Beschwerdeführer. Es handelt sich bei der Speicherung der Metadaten mithin um eine Handlung i.S.v. Art. 25a VwVG.

9. Das erforderliche schutzwürdige Interesse der Beschwerdeführer ergibt sich vorliegend ohne Weiteres aus dem vorstehend erwähnten schweren Eingriff in das durch die Bundesverfassung und die EMRK geschützte Fernmeldegeheimnis.

10. Die Beschwerdeführer haben am 20. Februar 2014 ein Gesuch an den Beschwerdegegner gestellt mit im Wesentlichen gleich lautenden Anträgen wie im anschliessenden Beschwerdeverfahren.

11. Welche Behörde für die zu beurteilenden Handlungen – und damit zur Behandlung des vorliegenden Gesuchs – zuständig ist, ergibt sich aus den anwendbaren Sach- und Organisationsgesetzen (vgl. ISABELLE HÄNER in: Praxiskommentar zum VwVG, Zürich 2009, Art. 25a, N 30). Vorliegend wird die Speicherung der Metadaten von der jeweiligen Anbieterin, d.h. von einer juristischen Person des Privatrechts, vorgenommen. Diese ist naturgemäss nicht zum Erlass einer Verfügung gemäss Art. 25a VwVG befugt. Zuständig zum Erlass einer Verfügung ist im Bereich der auf Private ausgelagerten Aufgaben vielmehr der Bund bzw. die zuständige Aufsichtsbehörde (vgl. HÄNER, a.a.O., Art. 25a, N 15). Aufsichtsbehörde ist im Fernmeldewesen gemäss Art. 58 des Fernmeldegesetzes vom 30. April 1997 (nachfolgend: FMG) grundsätzlich das Bundesamt für Kommunikation (BAKOM). Im Bereich der Überwachung des Post- und Fernmeldeverkehrs ist jedoch davon auszugehen, dass die Zuständigkeit beim Beschwerdegegner liegt, da diesem gemäss Art. 13 Abs. 1 BÜPF insbesondere die Aufgabe zukommt, Überwachungen anzuordnen und diese bei Wegfall der Rechtmässigkeit einzustellen.

    Der Beschwerdegegner hat das Gesuch grundsätzlich materiell behandelt, und die Vorinstanz hat die dagegen erhobene Beschwerde richtigerweise materiell behandelt.

12. Gestützt auf Art. 82 ff. BGG und nachdem kein Unzulässigkeitsgrund vorliegt, sind die Beschwerdeführer zur Beschwerde gegen das Urteil der Vorinstanz legitimiert. Die Beschwerdeführer machen geltend, dass die Speicherung der Metadaten durch ihre Anbieterinnen sie wie nachstehend dargelegt schwer wiegend in ihren Grundrechten verletzt. Diese

Grundrechtsverletzung dauert an, da nach der Ablehnung der Beschwerde nach wie vor sie betreffende Metadaten gespeichert werden. Die verletzten Grundrechte sind wie nachstehend dargelegt durch die BV, die EMRK, den UNO-Pakt II sowie die Konvention Nr. 108 des Europarates geschützt. Tangiert sind namentlich das Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung, die Freiheit der Meinungsäusserung, die Meinungs- und Informationssowie die Medienfreiheit, die persönliche Freiheit und die Bewegungsfreiheit, die Unschuldsvermutung sowie in Bezug auf Beschwerdeführer 4 und Beschwerdeführer 5, welche als Journalisten tätig sind, auch die Medienfreiheit und der Quellenschutz. Die Vorinstanz anerkennt, dass die Speicherung der Metadaten – wie von den Beschwerdeführern geltend gemacht – einen schweren Eingriff in die Grundrechte bedeuten. Als Beschwerdegrund machen die Beschwerdeführer in diesem Sinne die Verletzung von Bundesrecht, die Verletzung ihrer durch die BV und die EMRK garantierten verfassungsmässigen Rechte bzw. Grundrechte und Völkerrecht geltend (Art. 95 BGG). Da u.a. die Verletzung von Völkerrecht, namentlich die Verletzung der EMRK, geltend gemacht wird, ist den Beschwerdeführern die Möglichkeit einzuräumen, gegen das Urteil der Vorinstanz Beschwerde ans Bundesgericht zu erheben und im Beschwerdeverfahren vor dem Bundesgericht eine uneingeschränkte Überprüfung zu erhalten, ob sie in ihren Grundrechten verletzt sind. Dabei sind die gesamthaften Auswirkungen der Grundrechtsverletzung zu überprüfen. Da weiterhin Vorratsdaten betreffend die Beschwerdeführer gespeichert werden und verwendet werden könnten, dauert die geltend gemachte Verletzung ihrer verfassungsmässigen Rechte bzw. ihrer Grundrechte an. Damit sind sie durch das angefochtene Urteil beschwert. Die Beschwerdeführer sind mit der Geltendmachung der nachstehend angeführten Grundrechte und nachdem die Beschwerde erforderlich ist, um einen grundrechtskonformen Zustand herzustellen, zur Beschwerde legitimiert

13. Wie schon der Beschwerdegegner ist die Vorinstanz auf den Antrag der Beschwerdeführer, es seien die Anbieterinnen zu verpflichten, keine Randdaten an die Vorinstanz oder an andere Behörden oder Gerichte herauszugeben, nicht eingetreten. Zum Einen erblickt die Vorinstanz im erneut gestellten Antrag eine unzulässige Ausweitung des Streitgegenstandes (E 4.3). Zum Andern führt die Vorinstanz die Trennung der verwaltungsrechtlichen von den strafprozessualen Aspekte der Überwachung an und daran anschliessend die sachliche Zuständigkeit und Überprüfungsbefugnis von Staatsanwaltschaft bzw. Genehmigungsbehörde und des Beschwerdegegners. Die materielle Überprüfungsbefugnis der Vorinstanz beschränke sich auf die verwaltungsrechtlichen Aspekte der Überwachung. Dazu räumt die Vorinstanz immerhin auch ein, dass der Wortlaut von Art. 13 Abs. 1 Bst. a BÜPF, welcher die Überprüfungsbefugnis des Beschwerdeführers bezüglich

der strafprozessualen Aspekte regle und einschränke, eine (umfassende) Überprüfungsbefugnis in verwaltungsrechtlicher Hinsicht nicht von vornherein ausschliesse. Eine Herausgabe von Randdaten durch die Anbieterinnen direkt an andere Behörden oder an Gerichte sei gesetzlich nicht vorgesehen. Die Randdaten seien gegebenenfalls dem Beschwerdegegner zuzuleiten. Das Zuleiten von gespeicherten Randdaten betreffe die strafprozessualen Aspekte der Überwachung des Fernmeldeverkehrs. Aus diesem Grund ist und sei der Beschwerdegegner zum Entscheid über Antrag Ziff. 2 der Beschwerdeführer sachlich nicht zuständig und sei somit mangels Vorliegens einer erforderlichen Sachentscheidvoraussetzung auf die betreffenden Anträge zu Recht nicht eingetreten. Daran ändere – für sich alleine – nichts, dass der beschuldigten Person im Rahmen einer konkreten Überwachung erst nachträglich die Möglichkeit geboten werde, Beschwerde gegen eine Überwachungsanordnung zu erheben (E 8.).

14. Richtigerweise wäre das Gesuch vom Beschwerdegegner und von der Vorinstanz gesamthaft materiell zu behandeln. Auch Begehren 2 wäre zu behandeln und gutzuheissen gewesen. Nachdem die Speicherung der Daten grundrechswidrig ist, wäre die Nutzung der gespeicherten Daten gleichermassen grundrechtswidrig. Damit ist in Form einer entsprechenden Anweisung an den Provider sicherzustellen, dass gespeicherte Daten nicht verwendet werden. Der Beschwerdegegner hat in Bezug auf Begehren 1 eine Verfügung erlassen. Das Bundesverwaltungsgericht hat die Beschwerde gegen diese Verfügung materiell behandelt und mit dem angefochtenen Urteil entschieden. Ebenso wie im Verfahren vor dem Beschwerdegegner wäre auch das entsprechende Begehren 2 von der Vorinstanz zu entscheiden gewesen. Sofern die Vorinstanz der Auffassung ist, sie habe aufgrund des vorangegangenen Nichteintretensentscheids hierüber nicht materiel entscheiden können, hätte sie die Verfügung des Beschwerdegegners auch insoweit aufheben und eine Rückweisung an diese zur materiellen Behandlung anordnen können. Indem sie weder das eine noch das andere getan hat, hat sie den gebotenen Schutz der Grundrechte der Beschwerdeführer vereitelt und damit ihre Grundrechte verletzt. Der Entscheid der Vorinstanz ist auch insoweit aufzuheben, und der diesbezügliche Antrag ist gutzuheissen oder die Sache ist zur Gutheissung an die Vorinstanz oder an den Beschwerdeführer zurückzuweisen.

15. Die Beschwerdeführer haben im vorangegangenen Verfahren zur Prüfung der vorliegenden Beschwerde bzw. zur Beurteilung der mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe im konkreten Fall beantragt, die die Beschwerdeführer betreffenden Vorratsdaten der Anbieterin beizuziehen. Die Vorinstanz hat dies in vorwegnehmender Beweiswürdigung abgewiesen, da sie sinngemäss davon ausgeht, dieser Antrag beinhalte keine Aspekte, die über das das bereits Ausgeführte hinaus für die vorliegende Streitsache von Bedeutung sei (E 14.).

16. Dies trifft nicht zu. Die Vorinstanz kann nicht wissen, was für Vorratsdaten konkret bezüglich der Beschwerdeführer gespeichert sind. Mangels dieses Wissens erscheint es als willkürlich, feststellen zu wollen, dass die mit der Speicherung und allfälligen weiteren Nutzung der Daten verbundenen Grundrechtseingriffe nicht derart ins Gewicht fallen, dass sie die angeführten öffentlichen Interessen überwiegen. Der angefochtene Entscheid ist insoweit wegen Willkür aufzuheben und aufgrund des Umstandes, dass entscheidwesentliche Sachverhaltsfeststellungen nicht getroffen worden sind, denn die Vorinstanz trifft keine konkreten Feststellungen über die die Beschwerdeführer betreffenden Vorratsdaten und die damit verbundenen Auswirkungen. Die Vorinstanz hätte die Überprüfung der Grundrechtskonformität zur Gewährleistung eines effektiven Rechtsschutzes (Art. 29 Abs. 2 BV, Art. 13 EMRK) unter Heranziehung der konkret gespeicherten Vorratsdaten vornehmen müssen. Der Entscheid ist aufgrund der Verletzung dieser Bestimmungen aufzuheben.

17. Die Beschwerdeführer haben in ihrer Beschwerde die Effektivität der Vorratsdatenspeicherung für die Aufklärung von Straftaten in Frage gestellt. Die Vorinstanz weist dies zurück. Der Verfahrensantrag der Beschwerdeführer, es sei die Praxis im Zusammenhang mit der Anordnung von Massnahmen zur rückwirkenden Überwachung des Fernmeldeverkehrs sowie deren richterlicher Überprüfung zu evaluieren, ist gemäss Vorinstanz in vorwegnehmender Beweiswürdigung abzuweisen, sofern er sich überhaupt als zulässig erweise (E 12.5). Die Vorinstanz übergeht dabei, dass – wie nachstehend dargelegt – die Notwendigkeit der mit der Vorratsdatenspeicherung verbundenen Grundrechtseinschränkungen vom Staat zu belegen ist. Fehlen solche Belege, kann demzufolge die Notwendigkeit nicht einfach unterstellt werden. Die beantragte Evaluation ist somit nachzuholen. Fehlt eine solche Evaluation oder vermag eine vorliegende Evaluation die Annahmen der Vorinstanz nicht zu stützen, so ist die Effektivität ist mangels eines entsprechenden Belegs im Ergebnis zu verneinen.

II. Begründung

A. Einleitung

1. Die Vorinstanz und der Beschwerdegegner anerkennen, dass die Vorratsdatenspeicherung einen schweren Eingriff in die Grundrechte bedeutet. Es sei davon auszugehen, dass die Speicherung und Aufbewahrung von Randdaten der Telekommunikation i.S.v. Art. 15 Abs. 3 BÜPF einen schweren Eingriff in das Recht der Beschwerdeführer auf Achtung ihres Fernmeldeverkehrs (Art. 13 Abs. 1 BV und Art. 8 Ziff. 1 EMRK) und ihres Rechts auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV und Art. 8 Ziff. 1 EMRK) darstelle, umso mehr als beide Garantien auch für die Meinungs- und Versammlungsfreiheit von grundlegender Bedeutung seien. Dieses Ergebnis werde durch die

Datenschutzkonvention bekräftigt. Bei ihrer Beurteilung hebt die Vorinstanz folgend Umstände hervor: Die Verpflichtung der Anbieterin zu einer systematischen Speicherung und Aufbewahrung von Randdaten der Telekommunikation, wovon personenbezogene Daten von grossem Umfang betroffen seien, aus denen über einen längeren Zeitraum hervorgehe, mit wem, wann, wie lange und von wo aus die Beschwerdeführer kommuniziert haben; die Möglichkeit, diese Angaben zu Persönlichkeitsprofilen über die Kommunikation der Beschwerdeführer bzw. über deren äussere Umstände zu verzichten; Rückschlüsse aus den Randdaten in ihrer Gesamtheit auf die persönlichen Lebensverhältnisse und das persönliche Umfeld; Speicherung und Aufbewahrung der Randdaten ohne konkreten Anlass, insbesondere ohne dass erforderlich wäre, dass gegen die betroffene Person bereits ein Vorverfahren eingeleitet worden ist; Einschränkung der Herrschaft der Beschwerdeführer über ihre personenbezogenen Daten und somit ihres Rechts auf informationelle Selbstbestimmung und Vertraulichkeit ihrer Kommunikation; Aufrechterhaltung und zusätzliche Verschärfung des Eingriffs mit der Aufbewahrung der Randdaten im Hinblick auf eine allfällige Verwendung. Die Vorinstanz hebt auch hervor, dass es nicht darauf ankomme, dass die Speicherung und Aufbewahrung von Randdaten nicht heimlich erfolge und im Zeitpunkt der Speicherung der Randdaten unsicher und in den allermeisten Fällen gar unwahrscheinlich sei, dass diese je den Strafverfolgungsbehörden bekannt gegeben werden müssen bzw. je verwendet würden. Bereits die Speicherung und Aufbewahrung für sich stelle einen Eingriff in die geschützte Privatsphäre bzw. das Recht auf informationelle Selbstbestimmung dar. Die Vorinstanz hebt sodann hervor, dass die Strafverfolgungsbehörde die Randdaten schon zu einem Zeitpunkt erhält, in dem eine Genehmigung der rückwirkenden Überwachungsanordnung durch das Zwangsmassnahmengericht in der Regel noch nicht vorliege und in dem Betroffenen noch kein Rechtsmittel gegen die Überwachungsanordnung offen stehe (E 9.4).

2. Den Ausführungen der Vorinstanz ist grundsätzlich beizupflichten. Wie in der vorliegenden Beschwerde dargelegt blendet die Vorinstanz allerdings einige Aspekte, die zur Schwere der Grundrechtseingriffe beitragen, aus bzw. unterschätzt diese.

3. Die Vorinstanz hat auch erkannt, dass die Vereinbarkeit der zu überprüfenden gesetzlichen Regelung mit der BV insoweit überprüft werden kann, als eine verfassungskonforme Auslegung derselben vorzunehmen ist, und dass die gesetzliche Regelung auf ihre Vereinbarkeit mit der EMRK hin zu überprüfen ist (E 6.).

4. Weiter führt die Vorinstanz aus, unter welchen Gesichtspunkten der EGMR prüft, inwieweit (geheime) staatliche Überwachungsmassnahmen mit den Garantien der EMRK, insb. mit Art. 8 EMRK, vereinbar sind. Der EGMR geht davon aus, dass bereits die blosse Existenz von Gesetzen, die eine

geheime Überwachung etwa des Fernmeldeverkehrs ermöglichen, für alle möglicherweise von dem Gesetz Betroffenen ein Überwachungsrisiko beinhalte, die Vertraulichkeit der Kommunikation beeintächtige und aus diesem Grund einen Eingriff in die gemäss Art. 8 Ziff. 1 EMRK garantierten Rechte darstelle. Der EGMR lasse grundsätzlich eine potentielle Verletzung der garantierten Rechte genügen und prüfe die betreffenden Erlasse abstrakt, ohne dass eine tatsächliche Beeinträchtigung nachgewiesen sein müsste. Demnach genüge die blosse Existenz geheimer Überwachungsmassnahmen bzw. entsprechender gesetzlicher Bestimmungen für eine Verletzung der konventionsrechtlichen Garantien, wenn die Beschwerde führende Person von der Massnahme zumindest möglicherweise betroffen ist, etwa weil die Massnahme alle Nutzer einer Kommunikationsdienstleistung betrifft; der EGMR spricht von einem virtuellen Eingriff in die konventionsrechtlichen Garantien. Zudem bezieht der EGMR die Möglichkeit innerstaatlicher Rechtsmittel, die gegen die Überwachungsmassnahme erhoben werden können, mit in seine Betrachtung ein. Ein wichtiges Kriterium hierbei seien die Erwartungen einer Person im Hinblick auf ihr Privatleben wie auch im Hinblick auf die Vertraulichkeit ihrer Kommunikation. Darüber hinaus seien nebst den Umständen der Speicherung insbesondere die Art der Aufzeichnung, die Art einer allfälligen Verwendung, die Art der Verarbeitung, die Ergebnisse, die erlangt werden können, sowie der Charakter der Daten zu berücksichtigen (E 9.2.2 des angefochtenen Urteils).

5. Die Vorinstanz schränkt ihre Überprüfung der Grundrechtkonformität ausgehend von der Aufgabe des Beschwerdegegners ein und blendet die strafprozessualen Aspekte der Vorratsdatenspeicherung in der Folge weitgehend aus (E 8.5). Sie übersieht damit allerdings, dass die Vereinbarkeit der Vorratsdatenspeicherung mit der EMRK so den zitierten Anforderungen des EGMR nicht zu genügen vermag. Der Eingriff in die Grundrechte liegt – wie die Vorinstanz zutreffend erkennt – zunächst in der mit der anlasslosen Speicherung der Vorratsdaten an sich verbundenen Überwachung. Der Eingriff geht aber darüber hinaus, indem er die spätere Nutzung der Vorratsdaten in einem allfälligen Strafverfahren erlaubt. Eben auch darin liegt der mit der Vorratsdatenspeicherung verbundene virtuelle Eingriff in die konventionsrechtlichen Garantien. Bei der Beurteilung der Konformität der Vorratsdatenspeicherung sind die allfällige spätere Verwendung, die Art der Verarbeitung und die Ergebnisse, die erlangt werden können, zwingend zu berücksichtigen, denn diese Aspekte sind Bestandteil der mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe. Die gesetzliche Ordnung, welche die Nutzung der Vorratsdaten in der StPO regelt, und die dort vorgesehenen Zuständigkeiten namentlich der Staatsanwaltschaft und der Gerichte, ändern daran nichts.

6. Die Vorinstanz thematisiert mehrfach die Unterscheidung zwischen Randdaten und Bestandesdaten (insb. E 4.2.2, E 4.2.3). Sie führt aus, die Erteilung von Auskünften über Bestandesdaten sei nicht Streitgegenstand.

Dies ist insoweit zutreffend, als sich die Beschwerde gegen die systematische Speicherung der Vorratsdaten wendet. Nicht übergangen werden darf aber der Aspekt, dass bei der Beurteilung einer allfälligen Verwendung, der Art der Verarbeitung, der Ergebnisse, die erlangt werden können, sowie des Charakters der Daten auch die Bestandesdaten ins Gewicht fallen, weil diese sich in einem Strafverfahren zusammen mit Randdaten verwenden lassen. Der gesamte Charakter der Daten und ihre Verwendungsmöglichkeiten haben eine gänzlich andere Qualität als wenn nur Bestandesdaten allein vorhanden wären, und die mögliche Kombination mit Bestandesdaten weitet die Anwendungsmöglichkeiten und die Reichweite der Randdaten weiter aus. Insoweit sind die Bestandesdaten bei der Beurteilung der Grundrechtskonformität der Vorratsdatenspeicherung mit einzubeziehen, da sich diese mit allen Aspekten der damit verbundenen Grundrechtseingriffe befassen muss.

7. Die Vorinstanz geht davon aus, dass die Vorratsdaten nach sechs Monaten gelöscht werden müssen und eine Bearbeitung der Daten danach grundsätzlich widerrechtlich wäre (E 12.7.4) und dass ein Einsichtsrecht in die über einen selbst gespeicherten Vorratsdaten besteht (E 12.7.2 und E 12.7.4). Die Beschwerdeführer sind durchaus der Auffassung, dass dies von Rechtes wegen so sein müsste, es entspricht aber – wie in dieser Beschwerde dargelegt – nicht der Realität bzw. der derzeit geltenden Rechtspraxis. Der von der Voinstanz postulierte, faktisch aber nicht gegebene Rechtszustand demnach nicht als Argument für die Rechtfertigung der mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe angeführt werden.

B. Regelung und Praxis der Vorratsdatenspeicherung, gespeicherte Daten

1. Art. 273 StPO sowie die im BÜPF und der entsprechenden Ausführungsgesetzgebung enthaltene Regelung verpflichten verschiedene Anbieter von Kommunikationsdienstleistungen, Daten im Zusammenhang mit den erbrachten Dienstleistungen während 6 Monaten zu speichern (Vorratsdatenspeicherung). Unter den in Art. 273 StPO genannten Voraussetzungen sind diese Daten an die Strafverfolgungsbehörden herauszugeben. Gemäss Praxis des Bundesgerichts sind die Daten u.U. auch dann herauszugeben, wenn sie länger als sechs Monate aufbewahrt worden sind (BGE 139 IV 98 [1B_481/2012]). Die Vorinstanz ist demgegenüber der Auffassung, die Speicherung bzw. Aufbewahrung von Randdaten über die gesetzlich vorgesehene Dauer von sechs Monaten hinaus sei grundsätzlich unverhältnismässig und aus diesem Grund sowie mit Blick auf Art. 80 FDV zudem unrechtmässig, sofern sie sich nicht aus einem anderen Grund rechtfertigen lasse. Die Randdaten der Telekommunikation dürften somit gestützt auf Art. 15 Abs. 3 BÜPF nur während sechs Monaten aufbewahrt werden und seien nach Ablauf dieser Aufbewahrungsfrist zu löschen (Art. 4 Abs. 1 DSG e contrario). Andernfalls sei – vorbehältlich eines Rechtfertigungsgrundes für eine längere Aufbewahrung etwa i.S.v. Art. 80 FDV – grundsätzlich von einer widerrechtlichen Bearbeitung von

Personendaten auszugehen. Die Vorinstanz gründet ihren Schluss, wonach die Vorratsdatenspeicherung grundrechtskonform sei, die datenschutzrechtlichen Grundsätze einhalte und genügend Schutz vor Missbrauch der Daten bestehe, u.a. auf diese Auffassung. Dies erschiene allerdings nur dann als zulässig, wenn es effektiv etablierte Praxis wäre, dass die Daten nach sechs Monaten zu löschen sind, eine darüber hinausgehende Bearbeitung als widerrechtlich erachtet würde und damit die Herausgabe und anschliessende Verwendung von Vorratsdaten, die länger als sechs Monate aufbewahrt worden sind, in Strafverfahren ausgeschlossen wäre. Dies ist nach derzeitigem Stand der Bundesgerichtspraxis aber gerade nicht der Fall. Zu beachten ist auch die effektive Informatikpraxis, in der – auf Grund der geringeren, technischen Regelkomplexität – Datensicherungen (Backups) oftmals unterschiedslos von allen Daten auch für längere Zeit angelegt werden (zumal um Systeme im Störungsvall vollständig wiederherstellen zu können und dies auch für längere Zeit als bloss sechs Monate zurück). Anschaulich erscheint dazu der Fall, in dem aus zwei Rechenzentren der Swisscom in Bern mehrere Kassetten mit riesigen Mengen an teilweise sehr alten Daten verschwanden (http://www.nzz.ch/schweiz/entwendete-baender-bringen-die-swisscom-in-noete-1.18151998).

2. Erfasst werden Daten im Zusammenhang mit schriftlicher und mündlicher Kommunikation, in erster Linie bei der Kommunikation in elektronischer Form, aber auch im herkömmlichen Verkehr via Post. Erfasst werden insbesondere Daten, die aus der Kommunikation via Telefon, Mail, Internet und in Briefpostsendungen anfallen.

3. Welche Daten von welchen Anbietern zu speichern sind, erschliesst sich nicht ohne Weiteres. Auf Gesetzesstufe (Gesetz im formellen Sinn) sind die Regelungen in der StPO und im BÜPF festgelegt. Aus dem Studium der entsprechenden Gesetzesartikel wird aber nicht klar, welche Daten von welchen Providern genau erfasst werden müssen. Weitere Regelungen finden sich in der VÜPF, also auf Verordnungsstufe. Die dort enthaltenen Vorschriften machen allerdings auch nicht hinreichend deutlich, was zu erfassen ist. Zudem sind die gesetzlichen Regelungen, einschliesslich jener auf Verordnungsstufe, insgesamt bereits derart abstrakt, dass sich für den Laien nicht erschliesst, was diese im Einzelnen bedeuten. Details sind in Richtlinien geregelt, die im Wesentlichen den ETSI-Standard Lawful Interception umsetzen (vgl. Art. 17 und Art. 25 VÜPF; https://www.li.admin.ch/de/documentation/downloads/trts_oar.html). Diese Richtlinien sind in ihren technischen Details nur für Spezialisten, die entsprechend technisch bewandert sind verständlich, für Laien hingegen nicht. Dazu kommt, dass in der Praxis nicht möglich ist, unter Berufung auf die Auskunftspflicht gemäss Datenschutzgesetz von der Anbieterin entsprechende detaillierte Auskünfte zu erhalten. Den Rechtsunterworfenen ist damit in ganz wesentlichen Aspekten nicht klar, welche Daten überhaupt erfasst werden.

4. Erfasst werden offenbar insbesondere folgende Daten:

a) Grunddaten des betreffenden Kunden:

- Name, Adresse
- Geburtsdatum
- Ausweis/Ausweisnummer
- Beruf
- Telefonnummer(n)
- Mail-Adresse(n)
- Bei Firmen: Firma, Firmennummer (Zefix)
- Kontaktperson
- Kunde seit bzw. von/bis

b) Telefon:

- Telefonnummer
- Telefonnummer der Gegenseite
- Telefon-Anbieter
- Telefon-Abo
- Dauer des Abos
- Art des Anschlusses
- Angaben zum Anschlussinhaber, einschliesslich Adresse(n)/ Mail-Adresse(n)
- Details zu Zahlungen für den Anschluss (Art der Zahlung, Inhaber, Bank, Kontonummern)
- Details zu Kosten/Zahlung des Gesprächs
- in den Richtlinien wird darauf verwiesen, dass gewisse zusätzliche Informationen, die nicht Bestandteil der Vorratsdatenspeicherung sind, über die strafprozessuale Editionspflicht erhältlich gemacht werden können, insb. weitere Zahlungsinformationen und gewählte Extensions während des Telefongesprächs (DTMF)
- Zeiten, insb. Beginn und Ende Anruf
- Art der Verbindung/Kommunikation
- Allfällig Umleitungen/Weiterleitungen bei der Kommunikation

zusätzlich bei Anrufen via Festnetz:
- Adresse des Anschlusses
- verwendetes Gerät

zusätzlich bei Anrufen via Mobiltelefon:
- IMSI (auf SIM gespeicherte, eindeutige Nummer)
- IMEI (eindeutige Nummer des Telefongerätes)
- pUK- und pUK2-Code (PIN-Unlock-Keys [Codes zum Entsperren der SIM])
- Zeiten, insb. Beginn und Ende der Verbindung zu den im Gespräch genutzten Antennen

- benutzte Antennen einschliesslich Adresse, Nummer und Koordinaten der Antenne, Hauptstrahlrichtung

zusätzlich bei SMS oder MMS:

- Angaben zu Art, Status, Übertragung der SMS bzw. MMS
- Mail-Adresse bei Übertragung via Mail-Gateway

c) Mail:

- Mail-Adressen, inkl. Aliases
- Mail-Konto-Inhaber, einschliesslich Adresse und Mail
- Dauer des Mail-Kontos
- Details zu Zahlungen für das Mail-Konto (Art der Zahlung, Inhaber, Bank, Kontonummern)
- Mail-Adresse Absender
- Mail-Adresse Empfänger
- Zeitangaben zur Übertragung des Mails
- Übertragungsprotokoll, Übertragungsart des Mails (POP, IMAP, Webmail)
- Übertragungsstatus des Mails
- IP-Adressen der kommunizierenden Stellen (z.B. Absender und Mailserver)
- Message ID
- Verbindungsaufnahmen zum Mail-Server

d) Internet:

- Provider
- Internet-Abo
- IP-Adresse
- MAC-Adresse (eindeutige Nummer des Gerätes), Lokalisation, Art und weitere Eigenschaften des Modems bzw. Routers und der Einwahl
- Angaben zum Kunden, einschliesslich Adresse(n)/Mail-Adresse(n)
- Details zu Zahlungen für das Internet-Abo (Art der Zahlung, Inhaber, Bank, Kontonummern)
- zusätzlich bei Internet-Verbindungen über Mobilfunk: benutzte Antennen einschliesslich Adresse, Nummer und Koordinaten der Antenne, Hauptstrahlrichtung, benutzter Port

e) Multimedia (Voice over IP [VoIP]-Telefonie, Videotelefonie, etc.):

- Provider der Multimedia-Kommunikation
- Telefonnummer, SIP-URI (sofern vorhanden)
- IMSI (sofern vorhanden)
- Multimedia-Service-Typ
- Beginn, Ende und Dauer der Kommunikation

- Rolle in der Kommunikation
- Adresse
- Details zu Zahlungen (Art der Zahlung, Inhaber, Bank, Kontonummern)
- IP-Adresse, ausgehender Port, Port auf der Gegenseite (auch bei Kommunikation über Mobilfunknetz)

f) Brief- und Paketpost:

- Angaben zu Absender und Empfänger von Postsendungen (soweit vorhanden)

Soweit die Vorinstanz in Frage stellt, ob es sich bei den genannten Daten effektiv um Randdaten handelt, bzw. vorbringt, es handle sich um Bestandesdaten (insb. E 9.3), kommt dem keine entscheidende Tragweite zu. Wie dargelegt ist die Grundrechtskonformität gesamthaft unter Berücksichtigung aller Aspekten der mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe zu beurteilen. Insofern ist nicht entscheidend, ob einzelne der gemäss ETSI-Richtlinien zu erfassende Daten Bestandesdaten darstellen. Die Zuordnung zu diesen beiden Kategorien, welche die Vorinstanz vornimmt, ist im Übrigen teilweise unzutreffend bzw. unscharf. So werden etwa IP-Adressen i.d.R. dynamisch vergeben und gehören jedenfalls insoweit nicht zu den Bestandesdaten.

5. Illustrativ hierzu (und zur nicht eben klaren Reichweite des BÜPF) ist eine im 23. Tätigkeitsbericht des EDÖB erwähnte Empfehlung an die SBB, welche im Rahmen ihres WLAN-Angebots «SBB-free» mit Blick auf die Verpflichtungen gemäss BÜPF u.a. «Ziel IP Adresse» und «Ziel Port» speichert. Der EDÖB ist der Auffassung, dass diese Daten nicht unter das BÜPF fallen und empfahl deswegen, diese nicht mehr zu erheben. Weiter wurde empfohlen, die Nutzungs- und Randdaten nur so lange wie im Gesetz vorgesehen, nämlich sechs und nicht neun Monate. Der ersten Empfehlung kam die SBB nicht nach, da der Dienst ÜPF dringend geraten habe, diese Daten für die Strafverfolgungsbehörden weiterhin zu speichern (https://www.bundespublikationen.admin.ch/cshop_mimes_bbl/8C/8CDCD4590EE41ED68FD028E08D8A361F.PDF).

6. Anschaulich zur Reichweite der Vorratsdatenspeicherung ist sodann die Stellungnahme des Chaos Computer Clubs (Deutschland) zur Vorratsdatenspeicherung vom 9. Juni 2009 (https://www.ccc.de/de/vds/VDSfinal18.pdf).

7. In den vorstehend dargelegten Bereichen werden systematisch Daten darüber gespeichert, wer mit wem wann kommuniziert, wo sich die in die Kommunikation involvierten Personen aufhalten, teilweise werden auch inhaltliche Daten der Kommunikation erfasst. Je nach Kommunikationsart bzw. -kanal werden aus Anlass eines Kommunikationsvorgangs zahlreiche

Daten gleichzeitig erfasst, etwa bei der Nutzung des Internets mit Hilfe eines Mobiltelefons.

8. Sehr viel Kommunikation spielt sich über Kanäle ab, die von der Vorratsdatenspeicherung tangiert sind. Zudem fallen ständig Daten an, die Aufschluss über den Aufenthalt einer Person erlauben. Damit wird von der Vorratsdatenspeicherung sehr viel und viel Aussagekräftiges erfasst, auch wenn dabei kein oder kaum Kommunikationsinhalt gespeichert wird.

C. Tangierte Grundrechte

1. Die Vorratsdatenspeicherung greift in verschiedene Grundrechte ein. Die Vorratsdatenspeicherung ist damit nur rechtmässig, wenn sie sich über eine genügende gesetzliche Grundlage verfügt, sich auf ein öffentliches Interesse stützen kann und verhältnismässig ist, sie muss also geeignet und erforderlich sein, um den beabsichtigten Zweck zu erreichen, und das öffentliche Interesse muss gegenüber den Interessen der betroffenen Person überwiegen (Art. 36 BV). Die Rechtfertigung eines Eingriffs in Art. 8 EMRK setzt voraus, dass der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

2. Die Vorratsdatenspeicherung tangiert das Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]). Diese Normen verleihen jeder Person das Recht, frei von staatlicher Überwachung mit anderen Personen zu kommunizieren. Dies betrifft jede Form von Kommunikation, unabhängig davon, wo und mit welchen Mitteln die Kommunikation geführt wird. Geschützt ist sowohl der Inhalt der Kommunikation als auch die Tatsache an sich, dass die Kommunikation stattfindet, namentlich Ort und Zeit der Kommunikation sowie die Identität der daran teilnehmenden Personen. Diese Grundrechte sind damit immer dann tangiert, wenn der Staat Daten im Zusammenhang mit der Kommunikation von Personen erfasst und speichert, und zwar sowohl, wenn der Inhalt der Daten gespeichert wird, als auch bei der Speicherung sogenannter Metadaten. Der schwere Eingriff liegt bereits in der Speicherung der Daten und der damit verbundenen Überwachung an sich (vgl. JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, S. 203 ff.,).

3. Die Vorratsdatenspeicherung tangiert weiter die Freiheit der Meinungsäusserung, die Meinungs- und Informations- sowie die Medienfreiheit (Art. 16 BV, Art. 10 EMRK) und die Versammlungsfreiheit (Art. 22 BV, Art. 11 EMRK). Diese Normen verleihen jeder Person das Recht, ihre Meinung frei von staatlichen Eingriffen zu bilden und zu äussern, Medien und weitere Informationsquellen selbst und frei von staatlichen Eingriffen zu konsultieren, ihre Meinung mit anderen Menschen auszutauschen und sich friedlich mit anderen Personen zu versammeln (vgl. MÜLLER/SCHEFER, a.a.O., S. 347 ff., S. 437 ff., S. 517 ff., S. 571 ff.).

4. Sodann sind die persönliche Freiheit und die Bewegungsfreiheit garantiert (Art. 10 Abs. 2 BV, Art. 8 EMRK). Diese Grundrechte schützen das Recht, die Persönlichkeit frei von staatlichen Eingriffen zu entfalten, die wesentlichen Aspekte seines Lebens selber zu gestalten, persönliche Beziehungen zu knüpfen, allein gelassen zu werden und sich frei zu bewegen (vgl. MÜLLER/SCHEFER, a.a.O., S., 139 ff., S. 83 ff.).

5. Schliesslich ist Unschuldsvermutung tangiert (Art. 6 EMRK, Art. 32 BV). Jeder Mensch gilt als unschuldig, so lange er nicht in einem rechtmässig geführten Verfahren für schuldig befunden wurde, einen gesetzlich umschriebenen Tatbestand erfüllt zu haben. Eine angeschuldigte Person hat das Recht auf Aussageverweigerung, sie muss sich nicht selbst belasten (nemo-tenetur-Grundsatz). Die Unschuldsvermutung ist auch im Rahmen des Datenschutzes zu beachten (vgl. MÜLLER/SCHEFER, a.a.O., S. 981 ff.).

6. Die Beschwerdeführer 4 und 5 sind als Journalisten tätig und deshalb von der Vorratsdatenspeicherung speziell betroffen. Sie sind für die Ausübung ihres Berufes verstärkt darauf angewiesen, frei von Überwachung und unter Wahrung des Quellenschutzes recherchieren und andere Personen kontaktieren zu können. Mit den gespeicherten Vorratsdaten wird bei der Anbieterin eine Datenspur gelegt, aus der Rückschlüsse auf ihre beruflichen Aktivitäten, ihre Recherchen und ihre Kontakte zu Drittpersonen gezogen werden können. Namentlich sind mit den gespeicherten Daten Schlüsse auf Kontakte mit journalistischen Quellen möglich. Die vorstehend dargelegten Grundrechtseingriffe wirken damit beim Journalisten noch verstärkt. Dies gilt namentlich auch für die Rechtsunsicherheit und Intransparenz, die aus der ungenügenden gesetzlichen Grundlage der Vorratsdatenspeicherung resultiert (dazu MÜLLER/SCHEFER, a.a.O., S. 377). Art. 17 BV garantiert die Medienfreiheit. Gestützt auf Art. 17 Abs. 3 BV und Art. 10 EMRK anerkennen der EGMR und das Bundesgericht den Schutz journalistischer Quellen als eine der Grundbedingungen der Medienfreiheit. Eine Pflicht zur Preisgabe der anvertrauten Informationen könnte die Informanten abschrecken Die Praxis des EGMR stützt sich dabei auf die Freiheit der Meinungsäusserung, die Praxis des Bundesgerichts überdies auf das Redaktionsgeheimnis. Geschützt ist namentlich die Identität des Autors sowie Inhalt und Quelle der Information. Medienschaffende können ihre Aufgabe als Informationsvermittler und Wächter nur erfüllen, wenn sie die

erforderliche Information von Dritten erhalten, insbesondere Hinweise auf Vorkommnisse von gesellschaftlichem Interesse, die sonst verborgen bleiben würden. Dies wiederum setzt voraus, dass die Informationsgeber darauf vertrauen können, dass ihr Name nicht preisgegeben wird. Eine Pflicht zur Preisgabe der anvertrauten Informationen könnte Informanten abschrecken («chilling effect»). Unter Schutz steht damit insbesondere die Identität der Quelle. Gemäss Strassburger Praxis vermögen nur zwingende Gründe des öffentlichen Interesses die Aufhebung des Redaktionsgeheimnisses zu rechtfertigen. Es ist jedenfalls ein überwiegendes öffentliches Interesse erforderlich. Nach der Praxis des Bundesgerichts bedarf die Offenbarungspflicht ausserordentlicher Umstände (MÜLLER/SCHEFER [mit FRANZ ZELLER], a.a.O., S. 472; FROWEIN/PEUKERT, EMRK-Kommentar, 3. Aufl., Kehl am Rhein 2009, Art. 10 Rn. 17; JENS MEYER-LADEWIG, Handkommentar EMRK, 3. Aufl., Baden-Baden 2011, Art. 10 Rn. 39; Basler-Komm/ZELLER, Art. 172 StPO, N 2, N 7 f.; DONATSCH, in: Kommentar zur Schweizerischen Strafprozessordnung, DONATSCH/HANSJAKOB/LIEBER (Hrsg.), 2. Aufl., Zürich/Basel/Genf 2014, Art. 172 N 2 und N 4; Basler-Komm/BOMMER/GOLDSCHMID, Art. 264 StPO, N 15; VIKTOR GYÖRFFY, Quellenschutz im Strafprozess, in: medialex 6/16 sowie medialex Jahrbuch 2016, S. 79 ff., Rz. 2 f.; EGMR, 27.3.1996, Goodwin v. The United Kingdom (GC), 17488/90; EGMR, 22.11.2007, Voskuil v. The Netherlands, 64752/01; BGE 132 I 184; BGE 140 IV 108).

7. Insgesamt liegt wie an anderer Stelle dargelegt ein schwerer Eingriff in die Grundrechte der Beschwerdeführer vor. Auch der Beschwerdegegner und die Vorinstanz haben dies grundsätzlich erkannt (Verfügung des Beschwerdegegners, Ziff. 8., 9. und 10., Urteil der Vorinstanz, E 9.4).

8. Ein Aspekt des Grundrechtseingriffs liegt darin, dass die Vorratsdatenspeicherung einen «chilling effect» auf das Kommunikations- und Informationsverhalten hat (dazu im Einzelnen II.H.21.).

D. Gesetzliche Grundlage

1. Die Vorratsdatenspeicherung stützt sich auf eine gesetzliche Grundlage, welche sich über mehrere Bundesgesetze und Verordnungen verteilen (vgl. im Einzelnen vorstehend II.B. sowie die diesbezüglichen Darlegungen der Vorinstanz).

2. Die Beschwerdeführer machen geltend, die gesetzliche Grundlage sei zu wenig klar, formell ungenügend, und die gesetzliche Grundlage gebe die effektive Praxis nur rudimentär wieder. Da die Vorratsdatenspeicherung einen schweren Eingriff in Grundrechte bewirkt, müsse die Regelung der Vorratsdatenspeicherung präzise in einem Gesetz im formellen Sinn festgelegt sein. Da dies nicht der Fall ist, erachten die Beschwerdeführer die bestehende gesetzliche Grundlage als ungenügend.

3. Die Vorinstanz ist anderer Auffassung. Sie führt aus, es sei nach bundesgerichtlicher Rechtsprechung mit hinreichender Bestimmtheit im Gesetz selbst zu umschreiben, unter welchen Voraussetzungen, zu welchem Zweck und in welchem Ausmass persönliche Daten welcher Personen bearbeitet werden dürfen, wem derartige Informationen bekanntgegeben werden dürfen und wann bzw. unter welchen Voraussetzungen die Daten wieder gelöscht werden müssten. Zudem seien wirksame Verfahren vorzusehen, die einen Missbrauch persönlicher Daten verhindern. So müsse jede Überwachungsanordnung unverzüglich durch eine richterliche Behörde genehmigt werden, es seien Grund, Art und Dauer der Überwachungsmassnahme jedenfalls im Nachhinein der überwachten Person mitzuteilen. Gemäss EGMR müsse das innerstaatliche Recht die Personengruppen festlegen, deren Kommunikation durch gerichtliche Anordnung überwacht werden darf und es sei die Natur der Straftaten zu bestimmen, die zur Anordnung solcher Massnahmen führen können. Nach der EGMR-Rechtsprechung sei eine zeitliche Begrenzung der Massnahmen vorzusehen, das Verfahren für die Auswertung, Verwendung und Speicherung der erlangten Daten sei zu umschreiben und die Löschung der gespeicherten Daten zu regeln. Die Vorinstanz führt weiter aus, dass es gemäss EGMR auch bei klarer Formulierung der gesetzlichen Bestimmungen stets ein Element richterlicher Interpretation gibt. Die EMRK verbiete die allmähliche Präzisierung durch gerichtliche Auslegung nicht. Es soll erkennbar sein, unter welchen Umständen und unter welchen Bedingungen der Staat ermächtigt ist, in die garantierten Rechte einzugreifen.

4. Die Vorinstanz führt aus, dass die Begriffe «Teilnehmeridentifikation» und «Verkehrs- und Rechnungsdaten» technischer Natur seien. Dabei sei nicht allein auf den Wortlaut der betreffenden Bestimmung abzustellen. Vielmehr sei das Bestimmtheitserfordernis mit Blick auf die Umschreibung der umstrittenen Massnahme an Ziel und Zweck des Regelungsgegenstands zu messen und es sei nach der Bedeutung zu fragen, die der Bestimmung im Kontext mit anderen Bestimmungen zukommt. Das BÜPF lege den Zweck, die beteiligten Organe und das Ausmass der Datenbearbeitung jedenfalls in den Grundzügen selbst fest. Die Vorinstanz führt aus, dass die verwendeten Begriffe zwar weniger bestimmt gehalten seien, sich die Grundzüge der Regelung jedoch erkennen lassen. Die Verpflichtung sei damit und mit Blick auf den Regelungsgegenstand in sachlicher wie auch in zeitlicher Hinsicht hinreichend bestimmt umschrieben und eingegrenzt; es würden keine wesentlichen Wertungen der Gesetzesanwendung überlassen. Die Vorinstanz führt ferner aus, dass vorhersehbar sei, dass die Anbieterinnen systematisch äussere Daten ihrer Kommunikation speichern und aufbewahren. Es sei nicht notwendig im Einzelnen zu wissen, welche Daten gespeichert werden, sofern sich wie vorliegend das Ausmass der Datenbearbeitung in den Grundzügen aus dem Gesetz selbst ergibt. Die Vorinstanz nimmt an, dass die Anbieterinnen nicht Daten speichern und der Vorinstanz zuleiten, die nicht von Art. 15 Abs. 3 BÜPF erfasst sind. Die

Bestimmungen von Art. 16 Bst. d und Art. 24d VÜPF gingen hinsichtlich der Daten, deren Übermittlung angeordnet werden kann, nicht über Art. 15 Abs. 3 BÜPF hinaus. Dies gelte auch für Daten wie etwa den Standort und die Hauptstrahlrichtung der Antenne. Die Vorinstanz schliesst, dass sich die Rüge der ungenügenden Bestimmtheit von Art. 15 Abs. 3 BÜPF als unbegründet erweist.

5. Die Beschwerdeführer halten daran fest, dass die gesetzliche Grundlage ungenügend ist. Auch wenn im Gesetz ersichtlich ist, dass Telekommunikationsranddaten gespeichert werden und in einem Strafverfahren verwendet werden können, ist die Regelung doch zu wenig konkret und auch nicht allen wesentlichen Punkten in einem Gesetz im formellen Sinn verankert. Infolgedessen kann sich die rechtsunterworfene kein zureichendes Bild davon machen, welche Vorratsdaten über sie gespeichert werden, welches im Einzelnen die Verwendungsmöglichkeiten dieser Daten sind und wie sich dies auf ihre Grundrechte auswirkt.

6. Betrachtet man, welche Daten effektiv gespeichert werden bzw. praxisgemäss gespeichert werden dürfen und was mit Hilfe dieser Daten an Informationen über die betroffenen Personen gesammelt werden kann, so muss man feststellen, dass die gesetzliche Regelung die Praxis nur rudimentär wiedergibt. Das Ganze ist überdies sehr technisch. Die eigentliche Praxis ist kaum fassbar, zumal die betroffene Person von den Behörden und den involvierten Kommunikationsanbietern keine erschöpfenden und anschaulichen Informationen darüber erhalten kann, welche Daten über sie gespeichert werden und welche Informationen im Einzelnen durch diese Daten gewonnen werden können. So weit ersichtlich weigern sich alle Anbieterinnen, Einsicht alle im Rahmen der Vorratsdatenspeicherung erfassten Daten eines Kunden zu gewähren. Die Anbieterinnen der Beschwerdeführer sind nicht bereit, die gespeicherten Vorratsdaten der Beschwerdeführer gesamthaft herauszugeben, so dass die Beschwerdeführe bis dato nicht im Einzelnen wissen, was für Daten über sie gespeichert sind und was sich aus diesen Daten im Einzelnen für Informationen gewinnen lassen (vgl. dazu nachstehend Ziff. II.G.8.). Die technische Komplexität wird namentlich aus den technischen Richtlinien zur Vorratsdatenspeicherung (ETSI-Standard Lawful Interception) deutlich (vgl. vorstehend Ziff. II.A.3. ff.). Mit durchschnittlichen Kenntnissen ist es einer Person nicht ansatzweise möglich, die technischen Richtlinien zu verstehen. Nur wer über sehr gute fachliche Kenntnisse verfügt, kann ermessen, was alles gespeichert wird und welche Erkenntnisse die Behörden mit den gespeicherten Daten gewinnen können. Das ist bei Providern bzw. deren Angestellten und weiteren beruflich mit dieser Materie betrauten Personen der Fall. Die eigentlich Betroffenen, deren Daten gespeichert und allenfalls verwendet werden, können sich hingegen nicht zureichend erfassen, was die bestehende Regelung in Bezug auf sie bewirkt.

7. Die Vorratsdatenspeicherung u.a. deshalb einen schweren Eingriff in die Grundrechte dar, weil sie sich nicht auf Daten beschränkt, welche notwendigerweise mit der Kommunikationsdienstleistung verbunden sind, wie etwa die Aufzeichnung der Zeitdauer eines Telefongesprächs zum Zwecke der Rechnungsstellung (MÜLLER/SCHEFER, a.a.O., S. 204 m.w.H.). Im Rahmen der bestehenden Praxis werden weit mehr Daten gespeichert (vgl. vorstehend Ziff. II. B.3.ff.). Bei einem Anruf mit einem Mobiltelefon werden beispielsweise nebst der Gesprächsdauer und der Telefonnummer der angerufenen Person zahlreiche weitere Daten gespeichert wie die IMEI des verwendeten Telefongeräts, Angaben zu den benutzten Antennen (und damit der ungefähre Standort des Anrufers) sowie die benutzte IP-Adresse. Bei Versand eines Mails müsste rein für die Rechnungsstellung in aller Regel nichts gespeichert werden, nachdem die Nutzung hier nicht pro Mail, sondern pauschal verrechnet wird. Dennoch ist bei jedem Versand eines Mails eine ganze Reihe von Daten zu speichern. Der Umfang und die Tragweite der Vorratsdatenspeicherung liegt damit, wie an anderer Stelle dargelegt, in ganz anderen Dimensionen als der Umfang der Daten, welche für die Rechnungsstellung vom Provider gespeichert werden müsste.

   Unter diesen Umständen müsste die Regelung der Vorratsdatenspeicherung präzise in einem Gesetz im formellen Sinn festgelegt sein. Voraussetzungen und Umfang der Überwachung müssten für den Einzelnen klar aus dem Gesetz ersichtlich sein (MÜLLER/SCHEFER, a.a.O., S. 210). Auf Gesetzesstufe findet sich aber nur eine rudimentäre Regelung. Aus dem Gesetz selbst wird nicht hinreichend klar, welche Daten erfasst werden und welche Informationen sich daraus insgesamt gewinnen lassen.

8. Die bisherige Gerichtspraxis hat u.a. markante Ausweitungen der Vorratsdatenspeicherung auf Verordnungsstufe zugelassen (beispielsweise die Rasterfahndung in gespeicherten Antennenstandorten samt Hauptstrahlrichtung von Mobiltelefonen, dazu II.D.10.) sowie die Verwertung von gespeicherten Daten nach Ablauf von sechs Monaten, wenn diese beim Anbieter vorhanden sind (dazu vorstehend Ziff. II.B.1.). Auch in diesen Aspekte wird deutlich, dass das Erfordernis, die Vorratsdatenspeicherung auf eine hinreichend klare und nachvollziehbare, in einem Gesetz im formellen Sinn enthaltene gesetzliche Grundlage zu stellen, nicht erfüllt ist.

9. Zu beachten ist in diesem Zusammenhang, dass gerade aus einer vagen gesetzlichen Grundlage ein «chilling effect» resultieren kann, da für die rechtsanwendenden Behörden ein grosser Spielraum bleibt und die Tragweite der Regelung für die Rechtsunterworfenen kaum erkennbar ist. Dies daraus resultierende Tendenz, sich bei der Äusserung von Meinungen zurückzuhalten, beeinträchtigt die Meinungsfreiheit. An die Bestimmtheit der gesetzlichen Grundlage sind insoweit aus dem Gedanken des grundrechtlichen Schutzes freier Kommunikation und der Gefahr unerwünschter

«chilling effects» besonders strenge Anforderungen zu stellen (MÜLLER/SCHEFER, a.a.O., S. 375 ff.)

10. Als Beispiel dafür, dass die Tragweite der gespeicherten Daten für die betroffenen Personen kaum zu ermessen ist, kann die Rasterfahndung in gespeicherten Antennenstandorten erwähnt werden (sog. Antennensuchlauf, vgl. 1B_376/2011 sowie SIMON SCHLAURI, Fernmeldeüberwachung à discrétion?, in: sic! 2012, S. 238, S. 240 f.). Eine Person mag sich allenfalls bewusst sein, dass jedes Mal, wenn sie ihr Mobiltelefon verwendet (bzw. das Mobiltelefon für gewisse, vom Benutzer u.U. nicht einmal wahrgenommene Funktionen aktiviert wird), der Antennenstandort samt Hauptstrahlrichtung gespeichert wird, und dass ihr effektiver Standort damit sehr genau, u.U. auf wenige Meter genau, erfasst wird. Sie wird sich aber kaum darüber im Klaren sein, dass diese Daten dafür verwendet werden können, sie in eine Rasterfahndung einzubeziehen, wenn die Strafverfolgungsbehörde im Rahmen einer entsprechenden Strafuntersuchung wissen möchte, wer sich in den letzten sechs Monaten in einem bestimmten Zeitpunkt an einem bestimmten Ort aufgehalten hat. Die Rasterfahndung in gespeicherten Antennenstandorten vermag sich zudem nur auf eine Verordnungsbestimmung zu stützen (Art. 16 lit. e VÜPF). Ein Gesetz im formellen Sinn, das diese Massnahme im Einzelnen regeln würde, besteht nicht. Sie verfügt damit nicht über eine genügende gesetzliche Grundlage, zumal sie einen schweren Eingriff in die Grundrechte darstellt. Hinzu kommt, dass die meisten Personen, deren Daten in eine solche Rasterfahndung einbezogen werden, hernach nicht über die Verwendung ihrer Daten benachrichtigt werden.

11. Insgesamt ist damit zu konstatieren, dass zwar eine gesetzliche Grundlage für die Vorratsdatenspeicherung existiert, diese aber als ungenügend zu erachten ist. Wesentliche Details der Praxis erschliessen sich aus keinem Gesetz im formellen Sinn, sondern sind nur auf Verordnungsstufe (VÜPF) bzw. gar nur in den ETSI-Standards Lawful Interception festgehalten. Zum Einen kann die betroffene Person effektiv nicht ermessen, was alles über sie gespeichert wird und welche Informationen damit gewonnen werden können. Zum Anderen begrenzt die gesetzliche Regelung nur ungenügend, welche Informationen zu welchem Zweck gesammelt werden dürfen.

E. Öffentliches Interesse

1. Als öffentliches Interesse für die Vorratsdatenspeicherung kann insbesondere das Interesse an der Aufklärung von Verbrechen, Vergehen und Übertretungen nach Artikel 179^{septies} StGB (Missbrauch einer Fernmeldeanlage) sowie die Aufklärung irgendwelcher Straftat über das Internet begangener Straftaten (Art. 14 Abs. 4 BÜPF) angeführt werden. Unter den in Art. 273 StPO genannten Voraussetzungen kann die Staatsanwaltschaft gespeicherte Vorratsdaten herausverlangen und als Beweismittel in der entsprechenden Strafuntersuchung verwenden. Art. 273 StPO verweist

sodann auf die Voraussetzungen von Art. 269 Abs. 1 lit. b (genügende Schwere der Straftat) und lit. c (Subsidiarität: Erfolglosigkeit der bisherigen Ermittlungen, Aussichtslosigkeit oder unverhältnismässige Erschwerung der Ermittlungen) StPO. Hervorzuheben ist dazu, dass nicht etwa ein Katalog von Delikten besteht, der die Nutzung der gespeicherten Daten im Strafverfahren erlaubt, sondern dass grundsätzlich ein dringender Verdacht auf irgend ein Verbrechen oder Vergehen ausreicht, im Fall von Artikel 179^{septies} StGB sogar der Verdacht auf eine Übertretung. Die Verwendung von Vorratsdaten beschränkt sich also grundsätzlich nicht auf Fälle schwerer Kriminalität. Die in Art. 269 Abs. 1 lit. b. StPO aufgeführten Voraussetzungen sind sehr vage formuliert. Wie schwer eine Straftat konkret sein muss und was die Subsidiarität genau impliziert erschliesst sich nicht ohne Weiteres. Die Voraussetzungen von Art. 269 Abs. 1 lit. c schränken die Verwendung von Vorratsdaten ungenügend ein, indem sie die Verwendung von Vorratsdaten bereits zulassen, wenn alternativ eine der genannten Voraussetzungen vorliegt. Was die Schwere der Tat und die Güterabwägung betrifft, wirkt der Gesetzgeber präjudizierend, indem er grundsätzlich bereits Vergehen und in einer Konstellation sogar Übertretungen genügen lässt. Die Schwelle liegt damit insgesamt tief. Jedenfalls beschränkt sich die Nutzung der Vorratsdaten nach dem Wortlaut des Gesetzes keineswegs auf schwere oder gar schwerste Kriminalität. Die Voraussetzungen der genügenden Schwere der Tat und der Subsidiarität haben im Übrigen in der Praxis der Genehmigung der Verwendung von Vorratsdaten kaum eine Relevanz und bilden somit keine effektive Schwelle gegen entsprechende Anordnungen. Auch in der Praxis ist damit nicht sichergestellt, dass die Nutzung der Vorratsdaten-speicherung auf die Verfolgung schwerer Kriminalität beschränkt bleibt.

2. Es kann nicht nur die Herausgabe der Daten der verdächtigten Person verlangt werden, sondern auch jene eines Anschlussüberlassers i.S.v. Art. 270 lit. b Ziff. 1 StPO sowie gemäss eines Teils der Lehre die Daten eines Nachrichtenmittlers i.S.v. Art. 270 lit. b Ziff. 2 StPO (vgl. THOMAS HANSJAKOB, StPO-Kommentar, Zürich 2010, Art. 273 StPO N 11; NIKLAUS SCHMID, Praxiskommentar StPO, Zürich/St. Gallen 2009, Art. 273 N 6). Es müssen sich damit u.U. auch nicht verdächtigte Personen die Nutzung ihrer Vorratsdaten gefallen lassen.

3. Wird eine Straftat über das Internet begangen, so ist die Internet-Anbieterin gemäss Art. 14 Abs. 4 BÜPF verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen. Dies betrifft insbesondere (dynamische) IP-Adressen. Einer richterlichen Genehmigung bedarf es nicht, und die Auskunftspflicht ist nicht auf Daten der letzten sechs Monate beschränkt (vgl. THOMAS HANSJAKOB, Wichtige Entwicklungen der Bundesgerichtspraxis zu Überwachungen des Post- und Fernmeldeverkehrs, in: forumpoenale 3/2013, S. 176 f.; BGE 139 IV 98 [1B_481/2012]). Eine über das Internet begangene Straftat liegt vor, wenn irgend eine Tathandlung über das Internet abgewickelt wird, beispielsweise die Anstiftung. Eine

Beschränkung in Bezug auf die Art der Straftat besteht nicht (http://www.reko-inum.ch/de/display_file.php?fname=114010669724120&query=). Die Auskunftspflicht umfasst alle Angaben, die eine Identifikation des Urhebers ermöglichen, namentlich Auskunft darüber, wer eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt benutzt hat, nach Möglichkeit mit weiteren Daten zur entsprechenden Person, etwa der Telefonnummer. Die Auskunftspflicht greift auch, wenn es um die konkrete Zuordnung dynamischer IP-Adressen geht (THOMAS HANSJAKOB, Kommentar BÜPF/VÜPF, Art. 14 N 24 ff.).

4. Mit Inkrafttreten des Nachrichtendienstgesetzes (NDG), welches ebenfalls die Verwendung der Vorratsdaten vorsieht, werden künftig die Bekämpfung von Terrorismus, verbotenen Nachrichtendienst, Proliferation und Angriffen auf eine kritische Infrastruktur sowie die Wahrung weiterer wichtiger Landesinteressen als öffentliche Interessen hinzukommen (vgl. Art. 26 Abs. 1 lit. a NDG)

5. Ein öffentliches Interesse für die Speicherung und Nutzung der Vorratsdaten kann damit zwar angeführt werden, es ist dazu jedoch festzuhalten, dass die gesetzliche Regelung sich auf Interessen von höchst unterschiedlichem Gewicht bezieht, indem sich die Regelung der Vorratsdatenspeicherung nicht auf die Verfolgung von schwerer Kriminalität beschränkt, sondern auch auf leichtere Delikte zielt, in bestimmten Konstellationen sogar auf die Verfolgung von Übertretungen.

F. Eignung und Erforderlichkeit

1. Die Vorinstanz ist der Auffassung, die Vorratsdatenspeicherung sei geeignet und erforderlich mit Blick auf das angeführte öffentliche Interesse. In Bezug auf die Eignung prüft die Vorinstanz, ob die Aufbewahrung der Randdaten im Rahmen dessen bleibt, was in einer demokratischen Gesellschaft notwendig ist. Die Frage, ob die Voraussetzungen für eine Überwachung gegeben sind und damit auch, ob eine konkrete Überwachungsanordnung verhältnismässig ist, sei im Rahmen einer Strafuntersuchung nach strafprozessualen Gesichtspunkten zu beurteilen. Die Vorinstanz führt aus, dass nach der Rechtsprechung des Bundesgerichts das Resultat einer rückwirkenden Randdatenerhebung für die Aufklärung die rechtliche Qualifikation des untersuchten Delikts von wesentlicher Bedeutung sein könne. Danach könne eine rückwirkende Überwachung geeignet sein, das Tatmotiv eines Beschuldigten und die genauen Tatumstände zu eruieren. Weiter können Randdatenerhebungen und entsprechende Abgleichungen dem Zweck dienen, zu prüfen, ob sich die Beschuldigten zu den Zeitpunkten an den Tatorten weiterer einschlägiger Delikte untereinander oder mit anderen Personen telefonisch verabredet hatten. Auch könnten Verbindungsdaten der Abklärung dienen, ob mehrere Raubüberfälle zumindest teilweise von derselben Täterschaft ausgeführt wurden. Aus diesen Beispielen schliesst die

Vorinstanz, dass die Speicherung und Aufbewahrung von Randdaten und damit die rückwirkende Überwachung des Fernmeldeverkehrs geeignet ist, zur Aufklärung von Straftaten beizutragen. Die Vorinstanz führt weiter aus, dass der Verhältnismässigkeitsgrundsatz aus Sicht des Grundrechtsschutzes nicht verlangt, dass die Erhebung von Randdaten in jedem Fall von unmittelbarer Bedeutung für die Aufklärung einer Straftat sein muss. An das Subsidiaritätsprinzip, welches das Verhältnismässigkeitsprinzip konkretisiert, seien insbesondere beim Verdacht eines schweren Verbrechens grundsätzlich keine allzu hohen Anforderungen zu stellen. Es reiche vielmehr aus, wenn die Überwachungsmassnahme darauf abziele, eine unverhältnismässige Erschwerung komplexer Untersuchungen zu vermeiden. Weiter ermögliche die Speicherung und Aufbewahrung der Randdaten eine differenzierte rückwirkende Überwachung, indem den Strafverfolgungsbehörden ermöglicht wird, anhand verschiedener Targets einen bestimmten Fernmeldeverkehr zu überwachen. Die Vorinstanz weist den Verfahrensantrag ab, die Praxis im Zusammenhang mit der Anordnung von Massnahmen zur rückwirkenden Überwachung des Fernmeldeverkehrs sowie deren richterlicher Überprüfung zu evaluieren. An der Eignung ändere sich gemäss Vorinstanz nichts, dass das Max-Planck- Institut 2011 zu dem Ergebnis gekommen ist, es liessen sich keine Hinweise darauf finden, dass die in der Schweiz seit mehreren Jahren praktizierte Speicherung und Aufbewahrung von Randdaten zu einer systematisch höheren Aufklärung von Straftaten geführt hätte.

2. Die Vorinstanz erwägt in Bezug auf die Erforderlichkeit, dass die Massnahme des sog. quick freeze nicht gleich effektiv erscheine und damit nicht gleich wie die anlasslose Speicherung und (zeitlich beschränkte) Aufbewahrung von Randdaten i.S.v. Art. 15 Abs. 3 BÜPF geeignet sei, zur Strafverfolgung beizutragen. Sie käme vielmehr einer Echtzeit-Überwachung nahe. Eine rückwirkende Überwachung werde praktisch verunmöglicht, da Randdaten erst nach Aufkommen eines begründeten dringenden Verdachts erhältlich gemacht werden könnten. Weiter sei es der vom Gesetzgeber geschaffenen und gewollten Möglichkeit der rückwirkenden Überwachung immanent, dass (Rand-)Daten anlasslos gespeichert und (zeitlich begrenzt) aufbewahrt werden. Mit der von den Beschwerdeführern vorgeschlagenen Massnahme würde der Zugang zu Informationen über den in der Vergangenheit geführten Fernmeldeverkehr und damit eine Sicherung entsprechender Beweise verunmöglicht. Die Vorinstanz fügt an, dass die streitbetroffene Verpflichtung i.S.v. Art. 15 Abs. 3 BÜPF in personeller und auch in zeitlicher Hinsicht somit nicht über das hinaus geht, was zur Zielerreichung notwendig ist. Eine gewisse Aufbewahrungsdauer sei zum Zweck der Strafverfolgung vielmehr notwendig. Es sei nicht ersichtlich, dass die zu speichernden und aufzubewahrenden Randdaten in sachlicher Hinsicht über das hinausgehen, was zur Erreichung des Zwecks notwendig ist.

3. Die Beschwerdeführer halten am Standpunkt fest, dass der Vorratsdatenspeicherung die Eignung und Erforderlichkeit nicht attestiert werden kann. Sie rufen in Erinnerung, dass die Notwendigkeit der damit verbundenen Grundrechtseinschränkungen vom Staat zu belegen ist (dazu nachstehend II.H.32.)

4. Die Effektivität der Vorratsdatenspeicherung wäre empirisch zu untermauern. Die Anführung einzelner Fälle aus der Rechtsprechung vermag dies nicht zu ersetzen, da solche Fälle keine eine gesamthafte Abschätzung der Effektivität erlauben, und zudem regelmässig offen bleiben wird, in wie weit die Vorratsdaten für die Aufklärung eines Deliktes effektiv unerlässlich waren bzw. welchen entscheidenden Beitrag sie geleistet haben. Vorratsdaten werden kaum das einzige vorhandene Beweismittel sein, und es stellt sich im Einzelfall zudem die Frage, welche anderen Ermittlungsansätze aufgrund der Möglichkeit, Vorratsdaten heranzuziehen, in den Hintergrund gerückt sind oder gar nicht verfolgt wurden.

5. Empirisch lässt sich die Effektivität der Vorratsdatenspeicherung kaum belegen, und diese relativiert das Gewicht des angeführten öffentlichen Interesses stark. Empirische Untersuchungen dazu zeigen keinen signifikanten Einfluss auf die Aufklärungsrate, eine abschreckende Wirkung durch ein höheres Nachweisrisiko ist ebenfalls nicht nachweisbar. Aufschlussreich sind hier insbesondere die diesbezüglichen Gutachten und Untersuchungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Nachdem die Vorratsdatenspeicherung in Deutschland eingeführt und später aufgrund eines Urteils des Bundesverfassungsgerichts wieder ausser Kraft gesetzt wurde, wäre zu erwarten, dass sich signifikante Unterschiede zwischen der Zeit, in der Vorratsdatenspeicherung zur Verfügung stand, und der Zeit davor und danach zeigen würden. Auch ein Vergleich mit der Schweiz, die die Vorratsdatenspeicherung schon seit langem kennt, bietet sich an. Das Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht hat diese Zusammenhänge untersucht, stellte aber insgesamt kaum signifikante Veränderungen bzw. Unterschiede fest. In der Schweiz existieren offenbar keinerlei Statistiken und Untersuchungen zur Effektivität der Vorratsdatenspeicherung, obschon die Vorratsdatenspeicherung hierzulande schon seit 2002 zur Verfügung steht. (Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Freiburg i. Br., 2011, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? [http://www.mpicc.de/ww/de/pub/forschung/forschungsarbeit/kriminologie/vorratsdatenspeicherung.htm]). Dass das Max-Planck-Institut Unsicherheiten in der Datenlage hervorhebt, tut den Feststellungen im Gutachten keinen Abbruch, denn die Effektivität wäre am Staat, die Notwendigkeit der Grundrechtseinschränkungen zu belegen. Empirische Untersuchungen können nicht dadurch ersetzt werden, dass einzelne Fälle anekdotisch als Beleg für den Nutzen der Vorratsdatenspeicherung angeführt werden, zumal einzelne Beispiele

keinen allgemein bestehenden Effekt belegen können. Im Einzelnen wird regelmässig schwerlich festzustellen sein, ob die Vorratsdaten für die Aufklärung des Delikts unerlässlich waren, zumal diese nicht die einzigen Beweismittel sind und der tatsächliche Ursprung eines Tatverdachts zuweilen nicht klar zutage liegt. Nicht selten finden sich dazu keine oder nur nebulöse Hinweise in den Akten (*«Polizeiliche Ermittlungen haben ergeben…»*), und es ist offenbar insbesondere im Drogenbereich international gängige Praxis der Strafverfolgungsbehörden, den effektiven Ursprung des Tatverdachts zu verschleiern, etwa durch die Inszenierung von scheinbar zufälligen Polizeikontrollen (vgl. http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805, wo ein Beamter der amerikanischen Drug Enforcement Administration [DEA] zu diesem als *«parallel construction»* bezeichneten Ansatz wie folgt zitiert wird: *«Parallel construction is a law enforcement technique we use every day, It's decades old, a bedrock concept.»*).

6. Die Effektivität der Vorratsdatenspeicherung ist im Nationalrat u.a. im Rahmen der Fragestunde vom 16. März 2015 thematisiert worden. Der Bundesrat bestätigt in seiner Antwort auf die Frage der Nationalrätin Aline Trede, dass keine Statistiken über die Wirksamkeit von rückwirkend angeordneten Überwachungsmassnahmen erfasst werden. Die Anzahl verwertbarer Beweise aus rückwirkender Überwachung seien unbekannt. Auch konnte der Bundesrat die Anzahl notwendiger rückwirkender Überwachungsmassnahmen über sechs Monate hinaus weder effektiv noch schätzungsweise angeben. Ebenfalls ist dem Bundesrat nicht bekannt, innert welcher Frist nach Ermittlungsbeginn rückwirkende Überwachungen angeordnet werden (Fragestunde Nationalrat 15.5191, Cura Vista, http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20155191).

   Die Effektivität der Vorratsdatenspeicherung muss damit insgesamt stark angezweifelt werden. Es kann nicht davon ausgegangen werden, dass sich die Aufklärungsquote mit Hilfe der Vorratsdatenspeicherung markant steigern lässt.

7. Zur Verhältnismässigkeit, namentlich zur Erforderlichkeit, finden sich zwar die Bestimmungen von Art. 269 Abs. 1 lit. b und c StPO, welche aufgrund des Verweises gemäss Art. 273 Abs. 1 StPO auch bei der Vorratsdatenspeicherung zur Anwendung gelangen. Diese Voraussetzungen bilden in der Praxis aber keine effektive Schwelle gegen die Anordnung entsprechender Massnahmen (vgl. vorstehend Ziff. II.E.1.). Zu beachten ist zudem, dass sich dies nur auf die Verwendung der gespeicherten Daten im Strafverfahren bezieht, nicht auf die Speicherung an sich. Zu prüfen ist also vorab und in erster Linie einmal, ob die Speicherung an sich verhältnismässig ist.

8. Verlangt die Staatsanwaltschaft in einem konkreten Fall Auskunft über gespeicherte Daten, so können diese in der Strafuntersuchung als Beweis-

mittel verwendet werden, können also im Prinzip einen Beitrag zur Aufklärung der begangenen Straftat leisten. Die Vorratsdatenspeicherung ist damit grundsätzlich geeignet, das damit anvisierte öffentliche Interesse zu erfüllen.

9. Zu prüfen ist sodann, ob es für die Erreichung des Zwecks als notwendig erscheint, die Daten im vorgesehenen Umfang zu speichern. Über die vorgesehene Zeit hinweg fallen über die betroffene Person in grossem Umfang Daten an. Dies erscheint – jedenfalls in diesem Umfang, also für so viele Daten so vieler Personen über so lange Zeit – nicht als erforderlich. Nachdem die allermeisten der gesammelten Daten nie für eine Strafuntersuchung relevant werden, und nachdem die anfallenden Daten für die Aufklärung von Straftaten weitgehend ineffektiv sind, erscheint es als geboten, sich auf eine sehr viel weniger weit gehende Erfassung von Daten zu beschränken. So weit man die Auffassung vertreten will, dass Daten, die in Echtzeit nach Eröffnung des Strafverfahrens erfasst werden können, nicht genügen, kann – und muss – sich die Verwendung von Metadaten jedenfalls auf solche beschränken, die in engem zeitlichen und sachlichen Zusammenhang mit der zu untersuchenden Straftat angefallen sind. Es gibt verschiedene Prozeduren, die dies gewährleisten, etwa das in Deutschland als «quick freeze» bezeichnete Verfahren. Dabei werden vorhandene Metadaten sofort gesichert, sobald ein dringender Tatverdacht. Kurze Zeit später kann entschieden werden, in wie weit ein Anfangsverdacht Anlass gibt, die gesicherten Daten in einem konkreten Strafverfahren zu verwenden. Der grosse Unterschied ist hierbei, dass – wie bei anderen Zwangsmassnahmen auch – erst der dringende Tatverdacht überhaupt Anlass für den Grundrechtseingriff gibt. Dagegen erleiden bei der Vorratsdatenspeicherung alle an der Kommunikation mit Post und Fernmeldeverkehr teilnehmenden Personen einen Eingriff in die Grundrechte. Der Eingriff wird so, was die davon betroffenen Personen betrifft, flächendeckend. Dies erscheint nicht als notwendig. Die erhobenen Daten reichen auch nicht bis zu sechs Monate zurück, was einen kleineren Grundrechtseingriff darstellt und als ausreichend erscheint, zumal aus den vom Dienst ÜPF geführten Statistiken ersichtlich ist, dass die Strafverfolgungsbehörden in den meisten Fällen nur zeitnah angefallene Daten benötigen (vgl. Medienmitteilung der SwiNOG Federation vom 16. Juni 2013, https://www.digitale-gesellschaft.ch/2013/06/13/neue-statistiken-vorratsdatenspeicherung-ist-auch-hinsichtlich-der-vorhaltedauer-unverhaltnismassig/). Fest steht jedenfalls, dass mit der Vorratsdatenspeicherung flächendeckender Eingriff für alle betroffenen Personen verbunden ist, obschon die Daten der allermeisten Personen nie verwendet werden.

10. Das Interesse des Staats an der Vorratsdatenspeicherung verfügt insofern über kein grosses Gewicht, als die gespeicherten Daten die Aufklärung von Straftaten nicht oder nur unwesentlich zu verbessern vermögen. Im Arsenal der Untersuchungsmittel und Zwangsmassnahmen nimmt die Vorratsdatenspeicherung insgesamt nur einen bescheidenen Platz ein. Dagegen

fällt die permanente und weit reichende Überwachung der betroffenen Personen stark ins Gewicht.

G. Datenschutz und Datensicherheit

1. Die Rechtmässigkeit der Vorratsdatenspeicherung ist auch daran zu messen, in wie weit dabei datenschutzrechtliche Vorgaben eingehalten werden. Soweit datenschutzrechtliche Prinzipien wirksam sind, hat dies wiederum einen Einfluss auf die Beurteilung, ob die Vorratsdatenspeicherung als grundrechtskonform gelten kann.

2. Die Vorinstanz erkennt dies grundsätzlich. Es bezieht sich auf die Rechtsprechung des EGMR, welche festlegt, aus der Überwachung resultierende Eingriffe in grund- und konventionsrechtlich geschützte Positionen könnten nur dann als notwendig angesehen werden, wenn die gesetzliche Ordnung ausreichende Garantien zum Schutz vor Missbrauch vorsehe. Der EGMR verlange entsprechend, dass die Art der Daten, die aufgezeichnet werden können, die Umstände, unter denen Überwachungsmassnahmen angeordnet werden dürfen, die Vorsichtsmassnahmen im Umgang mit aufgezeichneten Daten, die Zeitdauer der Aufbewahrung und das Verfahren für die Auswertung, Verwendung und Speicherung einschliesslich der Kreis der zugriffsberechtigten Personen und der Löschung der Daten im Gesetz selbst umschrieben seien. Die Löschung bzw. Vernichtung der gespeicherten Daten müsse gemäss Rechtsprechung des EGMR und des Bundesgerichts verbindlich geregelt sein. Von einer Bearbeitung ihrer Daten betroffenen Personen müsse schliesslich ein Recht auf Auskunft und Einsicht in die betreffenden Daten zukommen (E 12.7.2 m. H.).

3. In Bezug auf die Vorratsdaten und deren Handhabung durch die Anbieterinnen stellt sich die Vorinstanz auf den Standpunkt, die massgeblichen Grundsätze seien eingehalten. Es führt dazu die in der VÜPF enthaltenen Bestimmungen sowie die VDSG und Bestimmungen des DSG an, die von den Anbieterinnen zu beachten seien. Die datenschutzrechtlichen Bestimmungen zur Datensicherheit würden auch für die Anbieterinnen gelten, soweit diese gestützt auf das BÜPF Randdaten der Telekommunikation und damit Personendaten speichern und aufbewahren. Diese Bestimmungen seien zudem hinreichend bestimmt umschrieben, wobei angesichts des Regelungsgegenstandes nicht zu beanstanden sei, dass sich der Gesetz- wie auch der Verordnungsgeber im Wesentlichen auf den Erlass finaler Bestimmungen bzw. das Festlegen von Zielen beschränkt hätten, anstatt detailliert die zu treffenden Massnahmen vorzuschreiben. Die gesetzliche Ordnung sei insofern und entgegen der Ansicht der Beschwerdeführer auch vor dem Hintergrund des Eingriffs in ihre Grundrechte nicht zu beanstanden, zumal nicht geltend gemacht werde, es sei mit der heutigen Technik und gemessen am Gefährdungspotential, das aus der Speicherung und

Aufbewahrung der Randdaten der Telekommunikation resultiert, eine sichere Datenbearbeitung nicht möglich (E 12.7.3).

4. Die von der Rechtsprechung geforderten weiteren Garantien zum Schutz vor Missbrauch bei der Bearbeitung von Personendaten durch die privaten Anbieterinnen ergeben sich nach Auffassung der Vorinstanz aus dem Fernmelderecht, insbesondere aus Art. 80 FDV und aus dem DSG. Über die Verhältnismässigkeit der Dauer der Aufbewahrung habe der Gesetzgeber mit der Festlegung der Aufbewahrungsdauer bereits generell-abstrakt entschieden. Nach Ablauf dieser Dauer seien sie zu löschen. Andernfalls sei grundsätzlich von einer widerrechtlichen Bearbeitung von Personendaten auszugehen. Die Vorinstanz geht davon aus, dass den betroffenen Personen gestützt auf Art. 8 DSB das Einsichtsrecht in die sie betreffenden Vorratsdaten zusteht sowie die Ansprüche nach Art. 25 DSG. Das (eingeschränkte) Auskunftsrecht gemäss Art. 45 FMG i.V.m. Art. 80 f. FDV vermöge jenem gemäss Art. 8 DSG nicht grundsätzlich entgegenstehen. Das Auskunftsrecht unterstütze dergestalt die in der BV niedergelegten und auch vorliegenden interessierenden Grundrechte von Art. 13 BV und könne insofern als normverwirklichende Drittwirkung der Grundrechte bezeichnet werden (E 12.7.4).

5. Entgegen diesen Darlegungen können die notwendigen datenschutzrechtlichen Grundsätze nicht als verwirklicht gelten, und es bestehen keine zureichenden Garantien zum Schutz vor Missbrauch bei der Bearbeitung von Personendaten. Insbesondere sind, wie dargelegt, in der Praxis weder die Löschung der Daten nach sechs Monaten noch das Recht auf Einsicht in die eigenen Vorratsdaten gewährleistet.

6. Die Vorratsdatenspeicherung verletzt eine Reihe von datenschutzrechtlichen Grundsätzen, namentlich das Verbot des Datensammelns auf Vorrat, den Grundsatz der Zweckbindung der Daten und den Grundsatz der Verhältnismässigkeit der Datenbearbeitung (vgl. dazu Art. 4 ff. DSG; URS MAURER-LAMBROU/ANDREA STEINER, Balser Kommentar DSG, 2. Aufl., Basel 2006, Art. 4 N 9 ff.; ASTRID EPINEY, in: BELSER/EPINEY/WALDMANN, Datenschutzrecht, Bern 2011, § 9 N 23 ff.). Es werden sehr viele Daten aller betroffenen Personen auf Vorrat gesammelt. Die Daten entstehen als Nebenprodukt von Kommunikationsvorgängen und dienen eigentlich dazu, dass die gewünschte Kommunikation technisch stattfinden kann. Indem die Daten dabei systematisch aufgezeichnet und gespeichert werden, um allenfalls in einem späteren Strafverfahren verwendet werden zu können, ändern sie ihren Zweck grundlegend. Die Vorinstanz verneint eine Verletzung dieser Grundsätze und verweist insbesondere darauf, dass im BÜPF vorgesehen sei, dass die Randdaten der Telekommunikation insbesondere zum Zweck der Strafverfolgung gespeichert und aufbewahrt werden. Erstens ändert dies aber nichts daran, dass die Daten ursprünglich aus Kommunikationsvorgängen entstehen und zu diesem Zweck erstellt werden. Es geht auch nicht primär darum, die Daten im Rahmen eines zum Zeitpunkt ihres Entstehens laufenden Strafverfahrens zu erfassen, vielmehr

werden sie mit Blick auf ein allfälliges künftiges Strafverfahren systematisch gespeichert, um im Rahmen einer rückwirkenden Erhebung zu Handen der Strafakten zur Verfügung zu stehen. Zweitens ist die gesetzliche Grundlage wie dargelegt ungenügend. Für die betroffene Person, welche lediglich mit dem entsprechenden Kommunikationsmittel kommunizieren will, ist nicht in genügendem Mass erkennbar, welche Daten gesammelt werden und zu welchem Zweck sie verwendet werden können.

7. Es wäre erforderlich, dass die betroffene Person der Sammlung der Daten freiwillig zustimmt, nachdem sie angemessen informiert worden ist. Dies ist bei der Vorratsdatenspeicherung nicht der Fall. Als betroffene Person ist man nicht in der Lage, Inhalt und Tragweite der Vorratsdatenspeicherung zu erkennen, auch nicht, wenn man sich darum bemüht, die entsprechenden Informationen zu beschaffen. Die gesetzlichen Grundlagen und die technischen Details sind für Laien wie dargelegt unverständlich. Auch hat die betroffene Person nicht die Möglichkeit, der Sammlung und Verwendung der Daten zuzustimmen oder diese zu verhindern, indem sie ihre Zustimmung verweigert. Schliesslich gibt es nicht einmal griffige Bestimmungen, die sicherstellen würden, dass die Daten nach der gesetzlich vorgesehenen Frist von sechs Monaten gelöscht werden (wie dargelegt lässt das Bundesgericht die Verwendung der Daten auch nach Ablauf von sechs Monaten zu, vgl. vorstehend Ziff. II.B.1.). Die Verletzung datenschutzrechtliche Grundsätze durch einen Anbieter hat in aller Regel keine verwaltungsrechtlichen oder strafrechtlichen Folgen.

8. Eine Anfrage beim Provider oder beim Dienst ÜPF würde der betroffenen Person auch nicht zu einem befriedigenden Informationsstand verhelfen. Auf allgemeiner Ebene sind keine griffigen Informationen vorhanden, mittels derer sich ein Laie ein konkretes Bild über die gespeicherten Daten machen kann. Gesuche an den eigenen Anbieter, die über sich gespeicherten Daten zu erhalten, werden – so weit ersichtlich – von keinem Provider bewilligt. Die Anbieter sind höchstens bereit, einige allgemeine Angaben zur Kundenbeziehung herauszugeben sowie einige wenige Daten, die im Zusammenhang mit der Rechnungsstellung angefallen sind. Sie verweigern aber durchwegs die Einsicht in alle im Rahmen der Vorratsdatenspeicherung gespeicherten Daten (soweit bekannt hat bisher einzig der Beschwerdeführer 1 Einsicht in einen Teil der ihn betreffenden Vorratsdaten erhalten, vgl. Ziff. II.H.16.). Damit kann sich die betroffene Person kein Bild darüber machen, welche Daten von ihr gespeichert sind und wie gravierend der Eingriff in ihre Grundrechte konkret ist, welcher damit verbunden ist. Dieser Aspekt der Heimlichkeit der Vorratsdatenspeicherung verstärkt den damit verbundenen Eingriff zusätzlich.

9. Schliesslich ist nicht sichergestellt, dass die Daten nicht ins Ausland gelangen, etwa im Rahmen internationaler Rechtshilfe in Strafsachen, polizeilicher und geheimdienstlicher Zusammenarbeit, aber auch, weil ein Provider seine Daten im Ausland lagern lässt oder aufgrund von mangelnder Daten-

sicherheit. Offensichtlich verwalten betroffene Provider tatsächlich sensible Daten im Ausland, so namentlich Salt (vormals Orange). Dieser Provider hat den Betrieb und den Unterhalt des Mobilfunknetzes an Ericsson ausgelagert, was zur Folge hat, dass die Strafverfolgungsbehörden Vorratsdaten, welche von Salt zu liefern sind, im konkreten Fall teilweise in Rumänien einholen müssen (http://www.srf.ch/news/schweiz/orange-verwaltet-heikle-daten-in-rumaenien). Wenn die Daten ins Ausland gelangen ist die Einhaltung der in der Schweiz geltenden Garantien bezüglich Grundrechte, Datenschutz und Datensicherheit nicht gewährleistet. Diese Problematik kann nicht unter Verweis auf abstrakte Regelungen zum Datenschutz und zur Datensicherheit beseite gewischt werden, zumal die im Ausland gelegenen Daten auch dem dortigen Recht unterstehen und dies den zu gewährleistenden Schutz vor Missbrauch unterlaufen kann (anschaulich zu einer solchen Problematik der Entscheid des EuGH, mit dem das Safe-Harbor-Abkommen mit den USA gekippt worden ist: http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:62014CJ0362).

10. Auch der inländische Nachrichtendienst (NDB) kann auf gewisse Vorratsdaten zugreifen (Daten gemäss Art. 14 Abs. 1 lit. a BÜPF i.V.m. Art. 14 2bis BÜPF). Die Beschränkung des Zugangs auf diese Datenkategorie wird wegfallen: Das in Kraft tretende NDG ermöglicht sog. genehmigungspflichtige Beschaffungsmassnahmen, darunter die Nutzung der Vorratsdaten (Art. 26 Abs. 1 lit. a NDG). Bei der Nutzung der Vorratsdaten durch den Nachrichtendienst werden die strafprozessualen Garantien nicht gegeben sein. Es bedarf für die Nutzung in diesem Rahmen auch keines konkreten Tatverdachts. Voraussetzung ist, dass eine konkrete Bedrohung im Sinne von Artikel 19 Absatz 2 Buchstaben a–d NDG gegeben ist (Terrorismus, verbotener Nachrichtendienst, Proliferation oder Angriff auf eine kritische Infrastruktur) oder die Wahrung weiterer wichtiger Landesinteressen nach Artikel 3 NDG dies erfordert. Diese Voraussetzungen sind äusserst schwammig. Insbesondere wird, wenn der Nachrichtendienst solches behauptet, vom Gericht, das die Massnahme genehmigen muss, schlechterdings nicht zu überprüfen sein, ob die insinuierte Bedrohung und die Relevanz der von der Überwachung betroffenen Person diesbezüglich gegeben sind oder nicht. Das Gericht wird nur überprüfen können, ob der NDB Behauptungen aufstellt, die den gesetzlichen Anforderungen entsprechen. Die betroffene Person erfährt davon nichts und wird auch im Nachhinein regelmässig nicht über die Massnahme unterrichtet werden. Jede von der Vorratsdatenspeicherung betroffene Person läuft somit Gefahr, Ziel einer solchen genehmigungspflichtigen Massnahme zu werden, ohne dass ein Tatverdacht für eine strafbare Handlung besteht, und allfällige Vermutungen des NDB, welche die Person zum Ziel der Massnahme machen, müssen keineswegs zutreffend sein, so dass die betroffene Person u.U. Ziel der Massnahme wird, ohne konkret Anlass dazu gegeben zu haben. Nachdem der NDB überdies nach Art. 61 NDG Personendaten oder Listen von Personendaten ins Ausland bekannt geben kann, ist die

Einhaltung der Grundrechte bei Vorratsdaten, die dem NDB geliefert werden, erst recht nicht gewährleistet.

11. Die grosse Menge an Daten, die bei diversen Anbietern anfallen, werfen beträchtliche Probleme bezüglich der Datensicherheit auf. Die Daten werden nicht vom Dienst ÜPF oder von den Strafverfolgungsbehörden gesammelt, sondern müssen von den Anbietern gespeichert werden. Dies schützt zwar die Daten vor dem unmittelbaren staatlichen Zugriff, wirft aber dafür andere Probleme bezüglich Datenschutz und Datensicherheit auf: Die Daten müssen von den Anbietern vor unbefugten Zugriffen geschützt werden. Art. 9 VÜPF überträgt den Anbietern, für die Datensicherheit besorgt zu sein, und verweist zudem auf die VDSG, welche für die Anbieter ohnehin gelten würde, und die BinfV, welche inhaltlich nichts Wesentliches zum Problem beiträgt. Dies genügt nicht. Damit stellt der Staat nicht sicher, dass die Daten sicher gehandhabt werden. Es fehlen griffige Vorschriften zur Datensicherheit, und es fehlt an einer Durchsetzung und Kontrolle der Datensicherheit von staatlicher Seite. Der Dienst ÜPF selbst wird im Übrigen auch nicht zureichend kontrolliert. Zwar besteht u.a. eine parlamentarische Kontrolle der Tätigkeit des Dienstes ÜPF, diese kann aber nur von Zeit zu Zeit einzelne Aspekte der Tätigkeit des Dienstes ÜPF kontrollieren und erstreckt sich offenbar nicht auf die im ISC-EJPD angesiedelte Informatik, auf der die Praxis der Vorratsdatenspeicherung Seitens des Dienstes ÜPF beruht.

12. Effektiv ist die Datensicherheit offensichtlich nicht gewährleistet. Konkrete Vorfälle, die bekannt geworden sind, zeigen, dass dies kein hypothetisches Problem darstellt, sondern ein reales. Angestellte von Swisscom, Salt (vormals Orange) und Sunrise haben offenbar vertrauliche Daten verkauft (http://www.handelszeitung.ch/unternehmen/illegaler-datenverkauf-orange-und-sunrise-bestrafen-mitarbeiter; http://www.it-markt.ch/de-CH/News/2012/05/21/Verkauf-von-vertraulichen-Daten.aspx). Bei der Swisscom sind Daten, die geschreddert werden sollten, verschwunden. Dies ist bekannt geworden, nachdem entsprechende Datenträger der NZZ zugespielt worden sind. Darauf befinden sich offenbar 60 Millionen Datensätze, in denen sich Geheimnummern von 979 Prominenten sowie 14'500 interne Mails, Verträge, Projektbeschreibungen und Sitzungsprotokolle befinden. Die Swisscom hat keine Erklärung dafür, wie die Daten abhanden gekommen sein könnten. Bei einem Hackerangriff auf den Mobilfunkanbieter Vodafone in Deutschland sind die Daten von zwei Millionen Kunden – darunter Kontonummern – gestohlen worden (http://www.nzz.ch/aktuell/schweiz/entwendete-baender-bringen-die-swisscom-in-noete-1.18151998; http://www.nzz.ch/aktuell/schweiz/brisante-prominenten-liste-auf-gestohlenem-band-1.18208255). Hacker haben sich Zugang zur Datenbank des Schengen-Informationssystems SIS verschaffen und 1,2 Millionen Datensätze kopieren können. Der Angriff erfolgte auf einen IT-Systemdienstleister in Dänemark, der zu diesem Zeitpunkt unter anderem für Dänemarks Kopie der Schengen-Datenbank verantwortlich war.

(http://www.spiegel.de/netzwelt/netzpolitik/sis-hacker-kopierten-teile-der-schengen-datenbank-a-944059.html). Dass die genannten Anbieter, einschliesslich der Swisscom, die Datensicherheit nicht durchwegs gewährleisten können, weist darauf hin, dass hier ein grundsätzliches Problem besteht. Der Staat verlangt von privaten Anbietern, die Daten zu sammeln, ohne die Sicherheit der aufgezeichneten Daten zu gewährleisten. Darin liegt ein weiterer Aspekt, der den Eingriff in die Grundrechte als gravierend erscheinen lässt. Die betroffenen Grundrechte und namentlich auch das Fernmeldegeheimnis sind auf diese Weise nicht gewahrt (vgl. Entscheidung Nr. 1258 des rumänischen Verfassungsgerichtshofes).

13. Auf welcher Software und Hardware die Speicherung und Nutzung der Vorratsdaten seitens der Anbieter und seitens des Dienstes ÜPF beruht, ist nicht bekannt. Es kann ohne genauere Kenntnis diesbezüglich nicht angenommen werden, dass die gespeicherten Daten damit hinreichend geschützt sind. Angesichts der grossen Menge und der hohen Sensibilität der Daten müsste der Schutz der Daten auf technischer Seite sehr hohen Ansprüchen genügen. Das Risiko, dass ausländische staatliche Stellen oder nichtstaatliche Hacker versuchen, an diese Daten heranzukommen, ist nicht zu unterschätzen. Es sei hier auf die ungeheuren Aktivitäten der amerikanischen National Security Agency (NSA) und mit ihr verbundener Dienste verwiesen (vgl. nachstehend Ziff. II.C.28.). Es ist überdies stets damit zu rechnen, dass ein Anbieter von Soft- und Hardware für Belange der Vorratsdatenspeicherung mit der NSA oder anderen Diensten verknüpft ist, indem er auch der NSA oder anderen Diensten Soft- und Hardware liefert oder indem er sonstwie auf freiwilliger oder unfreiwilliger Basis mit den entsprechenden Diensten zusammenarbeitet, u.a., indem er ihm Kenntnisse über Sicherheitslücken weitergibt (dazu nachstehend). Im Zusammenhang mit der NSA sind einige derartige Vorkommnisse bekannt geworden. Dies kann aber genauso auch irgendwelche andere Software und irgendwelche andere Dienste der USA oder anderer Staaten betreffen. Unter diesen Umständen besteht die nicht unbeträchtliche Gefahr, dass in der verwendeten Soft- und Hardware Hintertüren versteckt sind, welche von der NSA oder von anderen Diensten, aber auch von nichtstaatlichen Hackern, genutzt werden können, um an die gespeicherten Daten heranzukommen. Der Bund lässt die Öffentlichkeit nicht wissen, wer die Lieferanten der vom Dienst ÜPF verwendeten Software sind. Den Medien ist zu entnehmen, dass es sich u.a. um Verint Systems handelt, eine amerikanische Firma mit israelischen Wurzeln, der enge Kontakte zum israelischen Geheimdienst und zur NSA nachgesagt werden (http://www.tagesanzeiger.ch/schweiz/standard/Abgehoerte-Leitungen-ein-Schweizer-Flop-und-die-Einheit-8200-/story/27811395; http://www.zeit.de/2013/48/deutsche-telekom-geheimdienste-nsa/komplettansicht).

14. Die mangelnde Datensicherheit und die fehlende Zweckbindung der Daten beinhalten ein weiteres Risiko: Wenn Daten gespeichert werden müssen, deren Datensicherheit aber nicht gewährleistet ist, kann dies auch dazu

führen, dass die Daten mit irgendwelchen anderen Absichten zweckentfremdet werden. Die Daten können u.a. auch dafür verwendet werden, betroffene Personen zu kompromittieren oder zu erpressen. Beispiele aus dem amerikanischen Geheimdienst zeigen, dass dies nicht nur ein theoretisches, sondern ein reales Risiko ist (vgl. http://www.thedailybeast.com/articles/2011/08/02/fbi-director-hoover-s-dirty-files-excerpt-from-ronald-kessler-s-the-secrets-of-the-fbi.html; https://www.aclu.org/blog/national-security-technology-and-liberty/prospect-blackmail-nsa).

15. Ein Schlaglicht auf die gesamte Problematik werfen die Vorgänge, die im Zusammenhang mit der NSA und anderen Diensten bekannt geworden sind (vgl. http://www.theguardian.com/world/edward-snowden). Die Tätigkeit der NSA geht so weit, dass sie die Integrität und Sicherheit des Datenverkehrs auf praktisch jeder Ebene nachhaltig untergraben hat. Die NSA lässt sich offenbar Daten von vielen grossen IT-Firmen liefern oder greift diese ohne deren Wissen oder Zustimmung ab. Die Sicherheit von Verschlüsselungstechnologien und dabei vergebenen Zertifikaten ist gezielt ausgehebelt worden. Die NSA und ihre in- und ausländischen Partnerdienste schaffen es so, verschlüsselte Kommunikation im Internet zu knacken. Die amerikanische Sicherheitsfirma RSA beispielsweise hat ihre Verschlüsselungs-Software offenbar mit einer NSA-Hintertüre ausgestattet. Werden solche Hintertüren und Schwächen eingebaut, besteht das Risiko, dass diese in der auch von (weiteren) Hackern ausgenützt werden (http://www.tagesanzeiger.ch/ausland/amerika/Auf-die-Spione-folgen-die-Kriminellen/story/17283716; http://www.tagesanzeiger.ch/ausland/amerika/Die-Zeche-fuer-die-globale-Spionage-der-NSA/story/19784722; http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security). Eine Zusammenarbeit zwischen NSA und IT-Firmen besteht offenbar auch insoweit, als IT-Firmen der NSA Informationen über Sicherheitslücken gibt, bevor diese geschlossen werden, so dass die NSA diese Lücken ausnützen kann (http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html). Die Enthüllungen über die NSA und ihre Partnerdienste machen klar, dass die Sicherheit der Kommunikation über Telefon, Internet und weitere elektronische Kanäle stark kompromittiert ist. Sie zeigen aber auch die Bedeutung Schwere der Auswertung gesammelter Daten und der Folgen für die Grundrechte der Betroffenen. Beides – die Datensicherheit und die Möglichkeiten der computergestützten Datenauswertung – betrifft auch die Vorratsdatenspeicherung.

16. Die Ausführungen der Vorinstanz zu den datenschutzrechtlichen Grundsätzen und zum Schutz vor Missbrauch der Daten vermögen die von den Beschwerdeführern dargelegten Bedenken nicht zu beseitigen. Die von der Vorinstanz angeführten abstrakten Bestimmungen reichen nicht aus. Die Vorgaben des EGMR, wonach die Art der Daten, die aufgezeichnet werden können, die Umstände, unter denen Überwachungsmassnahmen angeordnet werden dürfen, die Vorsichtsmassnahmen im Umgang mit aufgezeichneten Daten, die

Zeitdauer der Aufbewahrung und das Verfahren für die Auswertung, Verwendung und Speicherung einschliesslich der Kreis der zugriffsberechtigten Personen und der Löschung der Daten im Gesetz selbst umschrieben sein müssen, sind – wie sich aus den vorstehenden Ausführungen ergibt – nicht eingehalten. Es ist zudem sicherzustellen, dass die Einhaltung der erwähnten Grundsätze in der Praxis effektiv gewährleistet ist. Dies ist ebenfalls nicht der Fall.

H. Verhältnismässigkeit und Grundrechtskonformität

1. Die Vorinstanz stellt zutreffend fest, dass die Vorratsdatenspeicherung einen schweren Eingriff in die Grundrechte der Betroffenen darstellt. Dabei berücksichtigt sie allerdings nicht alle Aspekte; der Eingriff wiegt damit noch schwerer, als die Vorinstanz dies wertet.

2. Die Prüfung der Verhältnismässigkeit durch die Vorinstanz ist in zwei Aspekten klar ungenügend. Die Vorinstanz müsste die Vereinbarkeit mit der EMRK wie dargelegt umfassend prüfen und die Bundesverfassung zumindest insoweit beachten, als die bestehenden gesetzlichen Bestimmungen verfassungskonform auszulegen sind. Die Vorinstanz verweist indessen auf die bestehende gesetzliche Bestimmung und hält dafür, die Bearbeitung von Randdaten der Telekommunikation betreffend habe der Gesetzgeber über die Verhältnismässigkeit der Dauer der Aufbewahrung bereits generell-abstrakt entschieden, indem er einen Ausgleich zwischen den grundrechtlich geschützten Interessen Betroffener und dem öffentlichen Interesse an einer wirksamen Strafverfolgung gesucht und die Aufbewahrungsdauer auf sechs Monate beschränkt habe (E 12.7.4). Ob die gesetzgeberische Lösung effektiv verhältnismässig ist, kann jedoch nicht aus ihr selbst abgeleitet werden, sondern ist eben gerade zu überprüfen. Die Vorinstanz hat somit die Vorgaben von Art. 36 BV verkannt und bei ihrer Überprüfung die Voraussetzung der gesetzlichen Grundlage auf unzulässige Weise mit jener der Verhältnismässigkeit vermengt.

3. Die konkrete Güterabwägung sodann ist komplett ungenügend. Sie ist einseitig an den ins Feld geführten öffentlichen Interessen ausgerichtet und berücksichtigt die entgegenstehenden privaten Interessen der Beschwerdeführer teilweise gar nicht oder gewichtet sie völlig unzureichend. Zudem sind die datenschutzrechtlichen Garantien und der Schutz gegen Missbrauch wie dargelegt effektiv ungenügend. Die Vorinstanz führt das öffentliche und private Interesse an einer wirksamen Strafverfolgung an und meint, die Interessen der Beschwerdeführer hätten dahinter zurückzutreten (E 12.8). Die Vorinstanz wird so den effektiv zur Disposition stehenden Interessen nicht ansatzweise gerecht.

4. Die Vorinstanz führt an, das gesellschaftliche Bewusstsein im Umgang mit moderner Informationstechnologie habe sich offenkundig teilweise gewandelt (E 12.8). Sofern die Vorinstanz damit meint, moderne

Informationstechnologien würde heutzutage von zahlreichen Menschen genutzt, welche sich dabei keine grossen Gedanken um Datenschutz und informationelle Selbstbestimmung machen, so ist das kein Argument, das gegen die Beschwerdeführer ins Feld geführt werden könnte, ebenso wenig der Umstand, dass die breite Nutzung von modernen Informationstechnologien immer auch ein potenzielles Einfallstor für Überwachung ist – im Gegenteil. Erstens geht es hier nicht wie im hierzu angeführten Entscheid des Bundesgerichts betreffend Google Street View um einen Dienst, der Aufnahmen von öffentlich einsehbaren Bereichen anfertigt, sondern um der Privat- und Geheimsphäre zuzuordnende Daten, die durch das Fernmeldeheimnis und durch andere Grundrechte geschützt sind. Zweitens können nicht allgemeine gesellschaftliche Entwicklungen determinieren, in wie weit eine einzelne Person den Schutz ihrer Grundrechte in Anspruch nehmen darf und in Anspruch nehmen will. Selbst wenn ganz viele Menschen sehr sorglos mit ihren Daten umgehen würden, muss sich deswegen eine Person, die auf ihre Daten achtet, keine weitergehenden Eingriffe in ihre Grundrechte gefallen lassen. Die Güterabwägung ist letztlich aus Sicht der konkreten Betroffenheit der Beschwerdeführer zu beurteilen (dazu auch Ziff. II.K.). Drittens bliebe zu klären, was die gesellschaftliche Entwicklung in Bezug auf den Umgang mit modernen Informationstechnologien insgesamt beinhaltet. Ein allgemeiner Konsens, dass die Bedeutung der Privat- und Geheimsphäre durch die technische Entwicklung im Schwinden begriffen ist, besteht jedenfalls nicht. Aus Sicht der Beschwerdeführer führen die modernen Informationstechnologien dazu, dass die Überwachungsmöglichkeiten und die Überwachung durch die immer zahlreicher anfallenden Daten und ihre immer raffiniertere Auswertbarkeit tendenziell laufend zunimmt, womit auf der anderen Seite der Schutz der Grundrechte und die effektive Gewährleistung der damit verbundenen Garantien immer wichtiger wird. Damit stehen sie jedenfalls nicht alleine.

5. Die Vorinstanz führt das Gewicht einer wirksamen Strafverfolgung bei Tatvorwürfen wie etwa Tötung, sexuelle Handlungen mit Kindern oder Abhängigen, sexuelle Nötigung, Vergewaltigung, Pornographie, Körperverletzung, Verleumdung, Drohung, Freiheitsberaubung, Geiselnahme, Hausfriedensbruch, Diebstahl, Raub, Erpressung, Brandstiftung, Urkundenfälschung und Betäubungsmitteldelikten an. Die Vorinstanz übergeht dabei, dass sich die Nutzung der Vorratsdaten nicht auf schwere Kriminalität beschränkt, sondern weit darüber hinaus geht.

6. Verharmlosend erscheinen auch die Ausführungen zur Problematik, dass auch die Daten von Drittpersonen und nicht nur von Tatverdächtigen verwendet werden können (E 12.8). Das Risiko, als unbescholtene Drittperson Ziel von Überwachungsmassnahmen zu werden, trägt massgeblich zur Schwere des Eingriffs bei, der mit der Vorratsdatenspeicherung verbunden ist.

7. Unberücksichtigt bleibt auch, dass es eben nicht durchgehend so ist, dass Vorratsdaten ausschliesslich auf Basis eines bestehenden Tatverdachts gegen eine konkrete Person genutzt werden können. Beim rückwirkenden Antennensuchlauf wird im Rahmen einer Rasterfahndung in den entsprechenden Daten erst versucht, einen Tatverdacht gegen eine konkrete Person zu erzeugen, was bedeutet, dass man alleine aufgrund der gespeicherten Daten zum Ziel von Überwachungsmassnahmen und u.U. weiteren Untersuchungshandlungen werden kann (vgl. II.D.10.).

8. Nicht weiter erörtert wird bei der Verhältnismässigkeitsprüfung durch die Vorinstanz der zentrale Aspekt, dass die allermeisten Personen, deren Daten gespeichert werden, in keiner Art und Weise einen konkreten Anlass für die Speicherung ihrer Daten auf Vorrat geliefert haben. Dennoch erleiden sie einen Eingriff in ihre Grundrechte, indem ihre Daten unterschiedslos gespeichert werden. Die Anlasslosigkeit wird zwar erwähnt, aber nur den gesetzlich vorgesehenen Mechanismen zum Schutz vor Missbrauch gegenübergestellt, ohne dass eine eigentliche Gewichtung dieses Aspekts erfolgt. Die gesetzlich vorgesehenen Mechanismen vermögen am Grundproblem, dass hier ein anlassloser schwerer Eingriff in die Grundrechte vorliegt, nichts zu ändern.

9. Die Vorinstanz ist der Auffassung, es sei keine unverhältnismässige abschreckende Wirkung i.S. eines «chilling effect» auszumachen. Dies trifft, wie in der Beschwerde dargelegt, nicht zu. Die anlasslose Speicherung ist sehr wohl geeignet, das Kommunikationsverhalten zu beeinträchtigen, insbesondere aufgrund der Bedeutung der Kommunikationskanäle, die der Vorratsdatenspeicherung unterliegen.

10. Die Bedeutung der Kommunikation über Kanäle, die der Vorratsdatenspeicherung unterliegen, namentlich Telefon, Mail und Internet, ist sehr gross und nimmt in Zukunft noch zu. Die Daten, die bei der Vorratsdatenspeicherung anfallen, lassen weit reichende Schlüsse auf das Kommunikationsverhalten zu, auch auf den Inhalt, sei es, dass inhaltliche Daten erfasst werden, sei es, dass die erfassten Daten Rückschlüsse auf den Inhalt erlauben. Erfasst werden zudem weitere Daten, namentlich Standortdaten, Daten zur Person, insb. Adressen, Bankdaten, Daten zu den verwendeten Geräten und Daten mit Bezug auf den Provider. Bei der heute verbreiteten Nutzung namentlich von Mobiltelefonen fallen die entsprechenden Daten fast ständig an. Mobiltelefone führen praktisch zu ständiger «Kommunikation», auch wenn der Nutzer das Mobiltelefon nicht ständig aktiv nutzt, etwa in Form von eingehenden Push-Meldungen oder wenn Apps im Hintergrund Daten senden und empfangen. Mit jedem dieser Vorgänge fallen die entsprechenden Standortdaten in den Vorratdsaten an, was u.a. extrem detaillierte Bewegungsprofile erlaubt. Hinzu kommt, dass die im Rahmen der Vorratsdatenspeicherung erfassten Daten mit weiteren Daten kombiniert werden können, was zu noch tiefgreifenderen Grundrechtseingriffen führt.

11. Die Vorratsdatenspeicherung betrifft alle Personen gleichermassen, nicht nur Personen, die eine Straftat begangen haben oder der Begehung einer Straftat verdächtigt werden. Jede natürliche und juristische Person nutzt die von der Vorratsdatenspeicherung betroffenen Kommunikationsdienste und Kommunikationsnetze und ist damit Subjekt der damit verbundenen Überwachung. Die Unschuldsvermutung und die betroffenen Grundrechte sind unter diesen Umständen nicht gewährleistet (vgl. Entscheidung Nr. 1258 des rumänischen Verfassungsgerichtshofes, S. 12). Problematisch ist hierbei insbesondere, dass jede Person, deren Vorratsdaten aufgezeichnet werden, dem Risiko ausgesetzt wird, sich im Nachhinein rechtfertigen zu müssen, wenn aus den Metadaten ein Tatverdacht gegen sie erzeugt oder verstärkt wird. Sie muss sich für die angefallenen Daten erklären und dabei die Interpretation der Strafverfolgungsbehörden, die sie ihr als Beleg für den Tatverdacht entgegenhält, zu entkräften versuchen. Die Wahrscheinlichkeit, als unschuldige Person einer Tat verdächtigt zu werden und dadurch in ein Strafverfahren involviert zu werden – mit allen damit verbundenen privaten und beruflichen Nachteilen –, wird durch die Vorratsdatenspeicherung deutlich erhöht. Die Vorratsdatenspeicherung ist geeignet, den Kreis der Verdächtigen (letztendlich unendlich) zu vergrössern, weil die Zahl der auswertbaren Kommunikationsverbindungen grösser und umfassender wird (vgl. dazu den Antrag an den Verfassungsgerichtshof Österreich zur EU-Richtlinie 2006/24/EG, S. 32 f.).

12. Betrachtet man die gesetzliche Regelung und die Informationspraxis von Behörden und Providern zur Vorratsdatenspeicherung, so muss man feststellen, dass die mangelhafte Information der Betroffenen System hat. Ein gewisses Mass an Heimlichkeit gegenüber allen Personen, die die entsprechenden Kommunikationsformen nutzen, ist der Vorratsdatenspeicherung inhärent, und das entspricht durchaus der Absicht der involvierten Behörden und Provider. Auch dieser Aspekt trägt ganz wesentlich zum Schluss bei, dass der Staat mit der Vorratsdatenspeicherung jede Person als potenzielle Straftäter betrachtet, indem er von allen Personen Metadaten ihrer Kommunikation mitschneidet. Dies kollidiert mit der Unschuldsvermutung und mit den betroffenen Grundrechten.

13. Die Vorratsdatenspeicherung besteht aus der fortlaufenden Aufzeichnung von Daten, welche zu grossen Datensätzen kumuliert, systematisch durchsucht und verknüpft werden können (Stichworte: Data Warehousing, Data Mining und Big Data). Durch diese Akkumulation und Verknüpfbarkeit ändern die Daten ihren Charakter grundlegend. Die Daten können zu Profilen verknüpft werden. Mit dem Zusammenzug der Daten sind Rückschlüsse über das Kommunikationsverhalten möglich, die aus den einzelnen Daten für sich besehen nicht gewonnen werden können. Es können Bewegungsprofile angelegt werden, und es wird so sichtbar, wann sich eine Person wo aufgehalten hat. Die Daten können im Rahmen einer Rasterfahndung nach bestimmten Merkmalen durchsucht werden, etwa danach, ob sich eine Person zu einem bestimmten Zeitpunkt in einer bestimmten Gegend aufgehalten hat. Zwar werden im Wesentlichen

Metadaten gespeichert, welche sich aus der Kommunikation der betroffenen Person ergeben und kein Inhalt der Kommunikation. Die Daten sagen aber dennoch sehr viel über die betroffene Person aus, namentlich über ihr Kommunikationsverhalten und ihren Aufenthaltsort. Die Auswertung der vorhandenen Daten mittels spezieller Suchfunktionen und komplexer Algorithmen hebt deren Gehalt überdies auf eine andere Ebene. Die diesbezügliche Technologie hat sich in den letzten Jahren rasant entwickelt; ein Ende der Entwicklung ist nicht abzusehen. Einerseits erlauben derartige Auswertungen Aussagen über die Person, die weit über die einzelnen Datensätze hinausgehen. Das Ganze ist so besehen, was die Daten betrifft, weit mehr als alle einzelnen Teile. Andererseits sind die gewonnenen Aussagen bzw. die damit vorgenommenen Interpretationen von anderer Qualität als die herkömmliche Auswertung einzelner Daten. Es wird nach verborgenen Zusammenhängen in den Daten gesucht, wobei diese Zusammenhänge nicht unbedingt real bestehen, sondern letztlich nur eine mittels Datenverarbeitung gewonnene Interpretation der Daten darstellen. Daten, die für sich alleine betrachtet irrelevant erschienen und allenfalls auch gar nie ins Blickfeld kämen, können durch eine derartige Auswertung Relevanz gewinnen.

14. Problematisch ist dabei – nebst der Wucht und Raffinesse der Daten und ihrer Auswertung an sich –, dass die gespeicherten Daten genutzt werden können, um überhaupt einen Tatverdacht bzw. Korrelationen, die zu einem Tatverdacht führen können, zu erzeugen. Die Vorratsdaten können so dazu führen, dass eine Person aufgrund der gespeicherten Daten überhaupt erst in ein Strafverfahren verwickelt wird. Anschaulich ist dies insbesondere bei der Rasterfahndung in gespeicherten Antennendaten, mit der u.U. ein Tatverdacht generiert wird. Ein weiteres Beispiel dafür liefert ein Fall, in dem eine rückwirkende Erhebung der Randdaten von Mobiltelefonen angeordnet wurde, um zu eruieren, welches von vier potentiellen Familienmitgliedern eine schwere Verkehrsregelverletzung zu verantworten hatte. Das Erfordernis eines dringenden Tatverdachts und die Verhältnismässigkeit erscheinen hier als fraglich (1B_206/2016; vgl. den Kommentar dazu von KONRAD JEKER: http://www.strafprozess.ch/10488-2/). Die Daten der Vorratsdatenspeicherung können damit Grundlage für Zwangsmassnahmen bilden, denen kein hinreichender Tatverdacht vorausgeht, sondern bei denen die Zwangsmassnahmen dazu dienen, den Tatverdacht gegen konkrete Personen überhaupt zu generieren. Dies widerspricht dem rechtsstaatlichen Grundsatz, dass Zwangsmassnahmen nur ergriffen werden können, wenn ein hinreichender Tatverdacht vorliegt (vgl. NIKLAUS OBERHOLZER, Grundzüge des Strafprozessrechts, 3. Aufl., Bern 2012, S. 310, Rz. 848). In Art. 197 Abs. 1 lit. b StPO ist dies an sich festgelegt. Dieser Grundsatz ist aber im Rahmen der Nutzung der Daten aus der Vorratsdatenspeicherung nicht gewährleistet. Erschwerend kommt hinzu, dass nicht alle betroffenen Personen, deren Daten in Rasterfahndung einbezogen werden, danach darüber informiert werden. Die Vorratsdatenspeicherung ist auch insoweit grundrechtswidrig. Das

Beispiel der Rasterfahndung in Antennendaten zeigt deutlich, dass die Vorratsdatenspeicherung nicht mit der Unschuldsvermutung vereinbar ist. Es zeigt sich hier exemplarisch das Risiko, dass sich eine Person aufgrund aufgezeichneter Metadaten im Nachhinein rechtfertigen muss (vgl. Ziff. II.H.11.).

15. Die Daten können mit Daten anderer Personen verknüpft werden. Weiter ist eine Verknüpfung mit anderen Daten möglich, welche ausserhalb der Vorratsdatenspeicherung anfallen. Diese Daten können durch weitere Untersuchungshandlungen gewonnen werden, namentlich mit anderen strafprozessualen Zwangsmassnahmen, insb. Beschlagnahme oder Edition von Datenträgern bzw. Daten. Dies können weitere Daten sein zu den in der Vorratsdatenspeicherung gehaltenen Daten, namentlich inhaltliche Daten, etwa der Inhalt eines Mails, einer Voicemail-Nachricht, einer Chat-Nachricht. Diese Daten können auf einem verwendeten Gerät anfallen, namentlich auf einem Mobiltelefon, und von dort ausgelesen werden. Für die Kommunikation werden zunehmend Apps auf Computern, Mobiltelefonen und anderen Geräten verwendet. Die Verwendung dieser Apps generieren inhaltliche Daten und Metadaten, die auf den entsprechenden Geräten erzeugt werden und zumindest teilweise gespeichert bleiben. Gleichzeitig werden je nach genutztem Gerät und Kommunikationskanal auch Vorratsdaten generiert. Dies ist dann insbesondere dann der Fall, wenn für die Kommunikation der Datenkanal eines Mobilfunk-Anbieters genutzt wird. Da solche Apps insbesondere auf Mobiltelefonen sehr oft genutzt werden, fallen durch deren Verwendung mitunter enorme Datenspuren an. Andere Daten, die beigezogen werden können, können beispielsweise aus Hausdurchsuchungen, von der Festplatte eines beschlagnahmten Computers, aus einem Mobiletelefon oder aus Videoüberwachungen stammen. Möglich sind auch Editionsbegehren an Dritte, etwa Anbietern von Internet-Diensten, Arbeitgeber, Behörden, Ladenketten, Banken, Kreditkartenunternehmen oder Online-Shops. Gewonnen werden können so etwa Facebook-, Twitter- oder Google+-Einträge, Chat-Beiträge, Mails, Daten zu Einkäufen und Zahlungen.

16. Anschaulich wird die Aussagekraft von Vorratsdaten aus den Vorratsdaten des Beschwerdeführers 1. Er hat Einsicht in einen Teil der ihn betreffenden Vorratsdaten erhalten und hat diese veröffentlicht. Die Daten sind aufbereitet, visualisiert und mit weiteren Daten kombiniert worden. Aus den entsprechenden Präsentationen erhält man einen Eindruck, was für eine Aussagekraft Vorratsdaten gewinnen können. Es lässt sich ein detailliertes Bewegungsprofil erstellen. Es wird sichtbar, wann er mit welchen Personen über welche Kanäle kommuniziert hat. Die Daten lassen sich mit weiteren Daten verknüpfen, etwa mit Facebook- und Twitter-Einträgen. Aus den gewonnenen Daten lassen sich auch Rückschlüsse auf den Inhalt der Kommunikation und auf den (privaten oder politischen) Zweck der Aktivitäten des Beschwerdeführers 1 ziehen (http://www.watson.ch/!533090301; http://www.schweizamsonntag.ch/ressort/nachrichten/der_glaeserne_nati

onalrat/; https://www.digitale-gesellschaft.ch/vds.html; https://opendatacity.de/project/vorratsspeicherung-in-der-schweiz/).

17. Nachdem die heutigen Möglichkeiten der computergestützten Verarbeitung kumulierter Daten und die damit verbundene komplexe Auswertungen den Charakter der verwendeten Daten grundlegend ändern und auf eine andere Stufe heben, ist eine solche Bearbeitung von Personendaten mit dem Grundsatz der Zweckbindung grundsätzlich nicht vereinbar. Für die betroffene Person kann in der Regel nicht ersichtlich sein, zu welchen Zwecken die neu kreierten Daten verwendet werden können (vgl. zum Ganzen: EPINEY, a.a.O., § 9 N 34; ROLF H. WEBER, in: Jusletter IT, 11. Dezember 2013, Big Data: Sprengkörper des Datenschutzrechts?).

18. Gerade durch das Element der Heimlichkeit verstösst die Vorratsdatenspeicherung auch gegen den Nemo-tenetur-Grundsatz. Spuren, die jede Person durch alltägliche Formen der Kommunikation selbst gesetzt hat, werden ihrem ursprünglichen Zweck, der im Zusammenhang mit eben dieser Kommunikation steht, entrissen, und mutieren zum belastenden Element in einem Strafverfahren.

19. Die Anordnung von Überwachungsmassnahmen bedarf der Genehmigung durch das Zwangsmassnahmengericht (Art. 274 StPO). Zwischen der Anordnung der Massnahme und dem Entscheid können aber gemäss Gesetz bis zu sechs Tagen verstreichen. Dies kann zur Situation führen, dass die Staatsanwaltschaft nach der Anordnung der Massnahme Vorratsdaten erhält (Art. 273 StPO), das Zwangsmassnahmengericht die Massnahme dann aber nicht genehmigt. Ergebnisse aus nicht genehmigten Massnahmen sind sofort zu vernichten und die daraus gewonnenen Ergebnisse sind nicht verwertbar (Art. 277 StPO). Dies ergibt aber keinen zureichenden Schutz vor ungerechtfertigten Massnahmen, da die erlangten Ergebnisse den Fortgang des Verfahrens beeinflussen können, bevor die Nichtgenehmigung der Massnahme feststeht, und da das damit gewonnene Wissen in den Köpfen der Strafverfolgungsbehörden bleibt, auch wenn die entsprechenden Dokumente und Datenträger vernichtet werden. Diese Regelung verletzt insbesondere den Schutz der Berufsgeheimnisse, namentlich das Anwaltsgeheimnis und das Arztgeheimnis, die Medienfreiheit und den Quellenschutz. Zudem ist die effektive Löschung bzw. Entfernung der betreffenden Daten wie dargelegt nicht zureichend gewährleistet.

20. Aus den gespeicherten Metadaten lassen sich Rückschlüsse auf das Kommunikationsverhalten der betroffenen Person ziehen, insbesondere darauf, mit wem eine Person kommuniziert, wie und wo. Im Rahmen der Vorratsdatenspeicherung werden damit sehr aussagekräftige Daten angehäuft. Aus den Metadaten können auch Schlüsse auf den Inhalt der Kommunikation gezogen werden, verstärkt noch, wenn sie mit anderen Daten kombiniert werden. Die Vorratsdatenspeicherung stellt insofern einen weit reichenden Eingriff in die Meinungsfreiheit dar.

21. Der Umstand, dass bei der Nutzung der von der Vorratsdatenspeicherung erfassten Kommunikationstechnologien in beträchtlichem Umfang Daten gespeichert werden, aus denen weit reichende Schlüsse auf die betreffende Person, ihr Verhalten und weitere Eigenschaften gezogen werden können, ist geeignet, das Kommunikationsverhalten der betroffenen Person nachhaltig zu beeinflussen und sie in ihrer Nutzung der betroffenen Kommunikationstechnologien zu beeinträchtigen. Die Vorratsdatenspeicherung ist geeignet, die betroffene Person von der Nutzung der betroffenen Technologien abzuhalten oder sie in ihrer Nutzung negativ zu beeinflussen. Wenn die betroffene Person weiss oder ahnt, dass Vorratsdaten aufgezeichnet werden, wird sie ihr Kommunikationsverhalten tendenziell dem anpassen und die entsprechenden Technologien nicht oder nicht unbefangen nutzen. Die Vorratsdatenspeicherung beinhaltet insofern einen «chilling effect», welcher wiederum einen Eingriff in die genannten Grundrechte darstellt (vgl. MÜLLER/SCHEFER, a.a.O., S. 375 ff.).

22. Es bestehen Studien, die einen «chilling effect» aufgrund der Erwartung, potenzielles Ziel von (Massen-)-Überwachung zu sein, nachweisen, insbesondere als Folge der Enthüllungen von Edward Snowden https://www.digitale-gesellschaft.ch/2016/05/18/update-mai-2016-nachrichtendienstgesetz-buepf-selbstzensur-podiumsdiskussion/).

23. Mit der Vorratsdatenspeicherung ist eine Überwachung der Kommunikationsvorgänge praktisch aller natürlichen und juristischen Personen verbunden. Was dies bedeutet und welche Informationen aus diesen Daten gewonnen werden können, ist einlässlich dargelegt worden. Die Vorratsdatenspeicherung beeinflusst tendenziell die Nutzung der davon betroffenen Kommunikationstechnologien und beeinträchtigt damit das Kommunikationsverhalten. Die betroffenen Personen wissen allenfalls der Spur nach, dass Vorratsdaten gespeichert werden. Den Umfang der Speicherung können sie aber kaum ermessen, ebenso wenig, was aus diesen Daten für Erkenntnisse gewonnen werden können und in welcher Situation sie sich wiederfinden kann, wenn sie aufgrund von Vorratsdaten in ein Strafverfahren verwickelt werden sollte. Dabei muss man sich vor Augen halten, dass die allermeisten Personen, deren Daten gespeichert werden, in keiner Art und Weise einen konkreten Anlass für die Speicherung ihrer Daten auf Vorrat geliefert haben.

24. Bei der Beurteilung der Verhältnismässigkeit sind auch die weiteren Überwachungen mit einzubeziehen, denen sich die Rechtsunterworfenen ausgesetzt sehen. Dazu gehören nebst den entsprechenden Massnahmen in der StPO und dem BWIS bzw. NDG insbesondere polizeiliche Massnahmen wie automatisierte Erkennung von Fahrzeugkennzeichen und verdeckte Fahndungen, etwa in Chatrooms, Videoüberwachungen, zunehmender Datenaustausch zwischen Behörden und auch zwischen Privaten und Behörden. In diesem Sinne ist die Verhältnismässigkeitsprüfung in eine Überwachungsgesamtrechnung

einzubetten (vgl. dazu https://digitalcourage.de/blog/2016/materialsammlung-ueberwachungsgesamtrechnung; https://www.digitale-gesellschaft.ch/2016/12/11/heat-bericht-zur-ueberwachungsgesamtrechnung-in-oesterreich/.)

25. Die EU-Richtlinie 2006/24/EG, welche den Mitgliedsländern die Vorratsdatenspeicherung vorschrieb, ist vom EuGH mit Urteil vom 8. April 2014 für ungültig erklärt worden (vgl. Simon SCHLAURI/DANIEL RONZANI, EUGH: Vorratsdatenspeicherungsrichtlinie 2006/24/EG für ungültig erklärt, in: sic! 9/2014, S. 570 ff.). Die Richtlinie verletze die Grundrechte der Achtung des Privat- und Familienlebens (Art. 7) und des Schutzes personenbezogener Daten (Art. 8) der Charta der Grundrechte der Europäischen Union (GRC). Mit Urteil vom 27. Juni 2014 erklärte der Verfassungsgerichtshof Österreich (welcher u.a. die Sache dem EuGH mit Vorabentscheidungsgesuch vorgelegt hatte) in der Folge die Gesetze zur Vorratsdatenspeicherung in Österreich für verfassungswidrig. Der EuGH und der Verfassungsgerichtshof bemängelten dabei im Wesentlichen Folgendes:

Speicherungsmassnahmen hätten sich auf eine klare und präzise Regelung zu stützen und sich auf das absolut Notwendige zu beschränken. Es müsse ein wirksamer Schutz vor Missbrauch bestehen.

Die Speicherung der Vorratsdaten führe zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung, dies, ohne dass sich die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Ausnahmen zum Schutz des Berufsgeheimnisses sind nicht vorgesehen.

Zwar soll die Richtlinie zur Bekämpfung schwerer Kriminalität beitragen, verlangt aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.

Ein objektives Kriterium, welches sicherstellt, dass der Zugang zu den Daten auf Straftaten beschränkt ist, die im Hinblick auf das Ausmass und die Schwere des Eingriffs in die in Art. 7 und Art. 8 GRC verankerten Grundrechte im Einzelfall als hinreichend schwer angesehen werden können, besteht nicht.

Der Zugang zu den gespeicherten Daten unterliegt gemäss der Richtlinie auch keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle. In der nationalen Regelung ist eine richterliche Genehmigung für die Nutzung der Vorratsdaten im Rahmen der StPO vorgesehen. Der Verfassungsgerichtshof Österreich hat diese Regelung gleichwohl als verfassungswidrig taxiert.

Die Speicherungsfrist ist gemäss Richtlinie zwischen sechs Monaten und 24 Monaten anzusetzen, ohne dass ihre Festlegung auf objektiven Kriterien beruhen muss, die gewährleisten, dass sie auf das absolut Notwendige beschränkt wird.

Die Richtlinie sehe keine klaren und präzisen Regeln zur Tragweite des Eingriffs in die GRC vor. Die Richtlinie beinhalte einen Eingriff in die Grundrechte, der von grossem Ausmass und von besonderer Schwere sei, ohne dass sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.

Es bestünden keine hinreichenden Garantien dafür, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung geschützt sind. Insbesondere sehe sie keine Pflicht der Mitgliedstaaten vor, die Daten nach Ablauf der Speicherfrist unwiderruflich zu löschen, sie im Unionsgebiet zu speichern und die Einhaltung der Datenschutzerfordernisse durch eine unabhängige Stelle überwachen zu lassen.

Bereits die Speicherung der Daten an sich wird als schwerer Eingriff in die Grundrechte taxiert. Es wird auf die Möglichkeit hingewiesen, die Daten, welche in unterschiedlichen Zusammenhängen ermittelt worden sind, zu verknüpfen und Rückschlüsse aus den Daten zu ziehen.

Das Urteil des EuGH stützt sich in seinem Entscheid, was die zu gewährleistenden Grundrechte betrifft, auf die GRC. Der Schutzgehalt der zitierten Bestimmungen der Charta entspricht im Wesentlichen den entsprechenden Grundrechten der EMRK. Jedenfalls ist der Schutzstandard der GRC diesbezüglich nicht höher als jener der EMRK (SCHLAURI/RONZANI, a.a.O., S. 575). Der Verfassungsgerichtshof Österreich nimmt in seinem Entscheid sowohl auf die GRC als auch auf die EMRK Bezug und erachtet die Vorratsdatenspeicherung im Ergebnis (auch) als EMRK-widrig (Urteil des Verfassungsgerichtshofs Österreich, E. 2.3.17.).

26. Es bestehen weitere Entscheide nationaler Verfassungsgerichte, welche die Grundrechtswidrigkeit der Vorratsdatenspeicherung feststellen, so insb. in Deutschland, Rumänien und Tschechien (vgl. SCHLAURI/RONZANI, a.a.O., S. 570 ff.). In Holland und und Bulgarien sind die dort bestehenden nationalen Erlasse zur Vorratsdatenspeicherung verfassungsgerichtlich

aufgehoben worden (http://www.heise.de/newsticker/meldung/Bulgarien-Verfassungsgericht-untersagt-Vorratsdatenspeicherung-2574103.html).

27. Die holländische Regelung der Vorratsdatenspeicherung ist von einem Gericht in Den Haag am 11. März 2015 für unzulässig erklärt worden. Von den massgebenden Aspekten sind insbesondere zwei auch für die Schweiz relevant. Das Gericht befand, dass das Gesetz klare, objektive Kriterien für die Regelung von rückwirkenden Überwachungsmassnahmen vorsehen muss. Gemäss holländischem Recht war die Schwelle zur zulässigen Anordnung von rückwirkenden Überwachungsmassnahmen mit der Zulässigkeit der Anordnung von Untersuchungshaft gekoppelt. Dies betrifft Delikte, die mit mindestens vier Jahren Freiheitsentzug bestraft werden können. Das Gericht kam zum Schluss, dass eine solche Regelung Konventionsrecht verletze. Es brauche eine präzise Gesetzesgrundlage, die ausschliesse, dass weniger schwere Delikte miterfasst werden. Weiter kam das Gericht zum Schluss, dass auch mit einer fallweisen Beurteilung über die Zulässigkeit der Anordnung (innerhalb des Deliktkatalogs) zu rückwirkenden Überwachungsmassnahmen dem Schutzgehalt von Art. 7 und 8 EMRK nicht genüge getan werde. Alleine die potentielle Möglichkeit zum Zugriff reiche für eine Konventionsverletzung aus, wobei Sicherheitsvorkehrungen und Abgrenzungen auf Gesetzesstufe unerlässlich seien (Uitspraak, Rechtbank den haag, http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498, Ziff. 3.10.). Weiter war eine fehlende innerterritoriale Speicherung der Daten ausschlaggebend für die Unzulässigkeitserklärung der Regelung. Das Gericht erkannte in Übereinstimmung mit EU-Recht, dass ein territorialer Speicherort ein unerlässlicher Faktor zu einem effektiven Datenschutz darstellt. Allein das Fehlen einer gesetzlichen Regelung, die eine territoriale Speicherung zwingend vorschreibt, verletzt somit Konventionsrecht (UITSPRAAK, RECHTBANK DEN HAAG, Ziff. 3.9.). Der Deliktskatalog, welcher die Nutzung von Vorratsdaten in der Schweiz erlaubt, ist noch weiter gefasst als jener in Holland. Auch in der Schweiz ist eine innerstaatliche Speicherung der Daten nicht gewährleistet, wie es überhaupt an einem effektiven Datenschutz gebricht.

28. In der Folge zum erwähnten Urteils des EuGH sind Vorabentscheidungsersuchen an den EuGH hängig, bei denen es um die Frage der Konformität nationaler Gesetze mit EU-Recht, die Telekommunikationsanbieter zur Speicherung von Verkehrsdaten verpflichten, geht. In seinen Schlussanträgen vom 19. Juni 2016 (http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=DE) gelangt der Generalanwalt zur Auffassung, dass eine generelle Verpflichtung zur Vorratsspeicherung mit den im Unionsrecht verankerten Grundrechten vereinbar sein kann, sofern sie durch eine Reihe von Garantien eng eingegrenzt ist:

- Begrenzung auf genau abgegrenzte schwere Straftaten;

- Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle;
- Berücksichtigung der Grundrechte, insb. Berufsgeheimnisse und Quellenschutz;
- wirksame Kontrolle über den Zugang zu den Vorratsdaten;
- Regelung in Rechtsvorschriften, die zugänglich und vorhersehbar sind und einen geeigneten Schutz gegen Willkür bieten;
- Wahrung der Charta der Grundrechte;
- Verwendung nur bei absoluter Notwendigkeit zur Bekämpfung schwerer Straftaten, was bedeutet, dass keine andere Massnahme oder Kombination von Massnahmen bei der Bekämpfung schwerer Kriminalität genauso wirksam sein könnte und zugleich die in der Richtlinie 2002/58 und in den Art. 7 und 8 der Charta der Grundrechte verankerten Rechte weniger beeinträchtigen würde;
- Einhaltung der im vorstehenden EuGH-Urteil benannten Garantien, die den Zugang zu den Daten, die Dauer der Vorratsspeicherung sowie den Schutz und die Sicherheit der Daten betreffen;
- die Verpflichtung muss in einem in einer demokratischen Gesellschaft angemessenen Verhältnis zur Bekämpfung schwerer Kriminalität stehen, was bedeutet, dass die schwerwiegenden Gefahren, die von dieser Verpflichtung in einer demokratischen Gesellschaft ausgehen, nicht außer Verhältnis zu den Vorteilen stehen dürfen, die sich aus ihr bei der Bekämpfung schwerer Kriminalität ergeben.

Der Generalanwalt fügte bezüglich der Kontrolle an, dass keiner der drei von einem Antrag auf Zugang betroffenen Beteiligten praktisch in der Lage sei, eine wirksame Kontrolle über den Zugang zu den auf Vorrat gespeicherten Daten auszuüben. Die zuständigen Strafverfolgungsbehörden sind daran interessiert, einen möglichst weitgehenden Zugang zu diesen Daten zu beantragen. Die Betreiber, die die Ermittlungsakte nicht kennen, könnten nicht prüfen, ob der Antrag auf Zugang auf das absolut Notwendige beschränkt sei. Die Personen, deren Daten abgefragt werden, könnten nicht wissen, dass sie Gegenstand einer solchen Untersuchungsmassnahme sind, und zwar auch im Fall einer missbräuchlichen oder unrechtmässigen Nutzung. Diese Konstellation widerstreitender Interessen verlange das Tätigwerden einer unabhängigen Stelle, bevor die auf Vorrat gespeicherten Daten abgefragt werden, um die Personen, deren Daten auf Vorrat gespeichert sind, vor jedem Missbrauch durch die zuständigen Behörden zu schützen.

29. Der Menschenrechtskommissar des Europarats hat sich ebenfalls mit der Vorratsdatenspeicherung befasst. Er hat in seinem Bericht vom 8. Dezember 2014 die Rechtmässigkeit der Europäischen Vorratsdatenspeicherung beurteilt (Commissioner for Human Rights, The rule of law on the Internet and in the wider digital world, Issue paper published by the Council of Europe Commissioner for Human Rights, S. 117, https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&Instran

etImage=2654047&SecMode=1&DocId=2216804&Usage=2). Darin stützt er das Urteil des Europäischen Gerichtshofes vom 8. April 2014, indem er die Datenspeicherung mit den Grundsätzen der Rechtsstaatlichkeit als nicht vereinbar erklärt (Commissioner for Human Rights, S. 115). Die Regelung stehe im fundamentalen Widerspruch zu den grundlegendsten Datenschutzgrundsätzen und zum Grundsatz der Datensparsamkeit. Gemäss dem Bericht sei die Speicherung zudem als nicht effektiv zu bezeichnen, da keine signifikant positiven Effekte auf die Aufklärungsrate von Delikten zu verzeichnen seien (u.a. mit Verweis auf Hans Jörg Albrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, Max Planck Institute for Comparative and International Criminal Law, 2nd enlarged report, prepared for the German Federal Ministry of Justice, July 2011, at www.bmj.de/SharedDocs/Downloads/ DE/pdfs/20120127_MPI_ Gutachten_VDS_Langfassung.pdf?__blob=publicationFile).

Der Menschenrechtskommissar hält die nationalen europäischen Gerichte ausdrücklich dazu an, die innerstaatlichen Gesetze über die Datenspeicherung auf ihre Effektivität und Effizienz zu überprüfen. Im Rahmen der Erforderlichkeit müsse sichergestellt werden, dass nur jene Bereiche der Datenspeicherung unterworfen werden, die eine solche Massnahme rechtfertigen (COMMISSIONER FOR HUMAN RIGHTS, S. 24). Dies betrifft die Schweiz als Mitglied des Europarats direkt.

Der Menschenrechtskommissar hält ausdrücklich fest, dass die Daten nicht im Ausland gespeichert werden dürfen. Einzig aufgrund einer klaren, eindeutigen und hinreichend detaillierten internationalen Rechtsgrundlage, die den Anforderungen des Datenschutzes und anderen Menschenrechtsstandards genügt, könnte eine ausländische Speicherung rechtmässig erfolgen. Gleichzusetzen mit einer ausländischen Speicherung sei auch die Verbringung der Daten zum Speicherort über internationale Kabelwege (COMMISSIONER FOR HUMAN RIGHTS, S. 21).

30. Die Beurteilung der EU-Richtlinie durch den EuGH sowie der entsprechenden nationalen Regelung durch den Verfassungsgerichtshof Österreich und weitere Verfassungsgerichte sind in weiten Teilen auf die Schweizer Regelung der Vorratsdatenspeicherung übertragbar. Zwar ist in der Schweiz vorgesehen, dass der Beizug der Vorratsdaten in einem Strafverfahren gerichtlich überprüft wird. Dies war aber in der nationalen Regelung in Österreich auch der Fall. Die Überprüfung erweist sich zudem nicht als effektiv. Weiter bestehen materielle Voraussetzungen für die Nutzung der Vorratsdaten. Damit wird aber weder die Speicherung an sich noch die Nutzung der anfallenden Daten auf das absolut Notwendige beschränkt. Insbesondere beschränkt sich die Speicherung und Nutzung der Vorratsdaten nicht auf Fälle schwerer Kriminalität. Die Situation auch insoweit mit der gesetzlichen Regelung in Österreich vergleichbar, welche ebenfalls materielle Voraussetzungen für den Beizug von Vorratsdaten im

Strafverfahren kennt. Diese sind jedoch vom Verfassungsgerichtshof als ungenügend eingestuft worden.

31. Der Vorinstanz ist eine Kopie der Eingabe von Müller Müller Rössner ans Bundesverfassungsgericht vom 6. November 2015 eingereicht worden (vgl. die Dokumentation auf http://www.mueller-roessner.net). Diese beinhaltet die Verfassungsbeschwerde gegen die Wiedereinführung der Vorratsdatenspeicherung in Deutschland. In dieser Eingabe ist eine Reihe von Punkte moniert worden, welche auf die Regelung in der Schweiz übertragbar sind:

31.1. Nichterfüllung von Vorgaben des Entscheids des Bundesverfassungsgerichts vom 2. März 2010:

a) Technisch bedingt werden bei der Vorratsdatenspeicherung in Bezug auf SMS auch die Inhalte der SMS abgespeichert (vgl. Eingabe S. 23 f.).

b) Der Richtervorbehalt in Deutschland erfüllt seine Wächterfunktion nicht, die richterliche Überprüfung erweist sich also als nicht effektiv, namentlich, weil die vorhandenen statistischen Erfassungen zeigen, dass die beantragten Überwachungen allesamt genehmigt wurden. Der Richtervorbehalt ist damit als Kontrollinstrument nicht wirksam (vgl. Eingabe S. 26 f.).

c) Die Datensicherheit ist nicht gewährleistet, insbesondere auch vor dem Hintergrund der Erkenntnisse über die Ausspähung von Datenbeständen durch ausländische Nachrichtendienste sowie nichtstaatliche Hacker. Dies begründet Zweifel, ob die durch die Vorratsdatenspeicherung anfallende riesige Menge von Daten wirksam vor unbefugten Zugriffen geschützt werden kann (vgl. Eingabe S. 28).

31.2 Nichterfüllung der Vorgaben des Entscheids des EuGH vom 8. April 2014:

a) Die Vorratsdatenspeicherung beschränkt sich nicht auf das absolut Notwendige, wenn ausnahmslos, anlasslos und zusammenhangslos gespeichert wird (vgl. Eingabe S. 32 f.).

b) Die nationale Regelung der Speicherpflicht ist insbesondere aufgrund der enthüllten Überwachungstätigkeit von Edward Snowden nicht mit der – den Grundrechten der EMRK entsprechenden – Grundrechten der Grundrechte-Charta der EU vereinbar. Die notwendige Datensicherheit ist nicht gewährleistet (vgl. Eingabe S. 25).

c) Der Schutz von Berufsgeheimnisträger ist nicht gewährleistet (vgl. Eingabe S. 41 f.).

32. Die UNO hat sich ebenfalls mit der aktuellen Praxis der Massenüberwachung befasst, u.a. in zwei Berichten, die der Menschenrechtsrat der UNO zum Thema publiziert hat (Annual Report oft he UN High Commissioner for Human Rights, Navi Pillay, The right to privacy in the digital age, 30. Juni 2014 [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf] [wsEvents/Pages/DisplayNews.aspx?NewsID=14875&LangID=E]; Report of the Special Rapporteuron the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 7. April 2013 [http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf])

Im Bericht vom 30. Juni 2014 wird dargelegt, dass die blosse Existenz von Massenüberwachungsprogrammen einen Eingriff in die Privatsphäre darstellt. Es sei am Staat, zu belegen, dass diese Eingriffe weder willkürlich noch ungesetzlich seien. Die Zulässigkeit von Eingriffen setze voraus, dass diese gesetzlich vorgesehen seien, wobei die entsprechenden gesetzlichen Regelungen wiederum mit dem UNO-Pakt II vereinbar sein müssten. Nicht willkürlich bedeute, das zu garantieren sei, dass gesetzlich vorgesehene Eingriffe in Übereinklang mit den Bestimmungen, Zielen und Grundsätzen des UNO-Pakts II stünden.

Der Staat habe für die notwendige Transparenz bei der Überwachung und der dafür geltenden Regelungen zu sorgen. In vielen Ländern würde die justizielle Kontrolle die entsprechenden Massnahmen nur noch durchwinken, eine unabhängige Überwachung der Massnahmen, welche die Grundrechte effektiv schütze, fehle oft. Die Gesetze zur Überwachung müssten öffentlich zugänglich sein und garantieren, dass die Sammlung von Kommunikationsdaten, der Zugang dazu und deren Verwendung auf spezifische, legitime Zwecke zugeschnitten sind. Die Gesetze müssen ausreichenden präzise sein und effektiven Schutz gegen Missbrauch bieten. Massenüberwachungsprogramme seien als willkürlich einzustufen, selbst wenn sie einem legitimen Zweck dienen und auf Basis eines nachvollziehbaren Regelwerks eingeführt werden.

Eine allgemein vorgesehene Speicherung von Daten von Drittpersonen erscheine weder als notwendig noch als verhältnismässig. Jegliche Erfassung von Daten sei ein Eingriff in die Privatsphäre, und zudem führe das Sammeln und Speichern von Kommunikationsdaten unabhängig davon zu einem Eingriff in die Privatsphäre, ob diese Daten später beigezogen oder benützt werden oder nicht. Nur schon die blosse Möglichkeit, dass Kommunikatons-Informationen erfasst werden, erzeuge einen Eingriff in die Privatsphäre und einen potenziell abschreckenden Effekt («chilling effect») in Bezug auf die betroffenen Rechte, einschliesslich des Rechts auf freie Meinungsäusserung und der Vereinigungsfreiheit.

Der Bericht hebt – unter Verweis auf den EuGH-Entscheid – hervor, dass Metadaten sehr genaue Rückschlüsse auf das Privatleben der Person ermöglichen, deren Daten gespeichert worden sind. Vor diesem Hintergrund gelangt der Bericht zum Schluss, dass es nicht überzeuge, wenn gesagt werde, es stelle – im Gegensatz zur Sammlung von Daten zum Inhalt der Kommunikation – keinen Eingriff in die Privatsphäre dar, wenn Metadaten gesammelt werden.

Der Bericht vom 7. April 2013 analysiert die Situation ebenfalls. Er äussert sich kritisch zur Möglichkeit von Staaten, die Anonymität einzuschränken Er empfiehlt u.a. die Erleichterung privater, sicherer und anonymer Kommunikation. Staaten sollten davon absehen, die Identifikation von Nutzern zur Vorbedingung für den Zugang zu Kommunikation, einschliesslich Online-Services, Internet-Cafés und Mobiltelefonie, zu machen. Personen sollten frei sein, die Technologie ihrer Wahl zur Sicherung ihre Kommunikation zu nutzen. Staaten sollten bei der Nutzung von Verschlüsselungstechnologien nicht eingreifen und nicht die Herausgabe von Schlüsseln erzwingen. Staaten sollten nicht ausschliesslich für Überwachungszwecke Daten speichern oder deren Speicherung verlangen.

Am 9. Dezember 1998 hat die Generalversammlung der UNO die Resolution 'Erklärung über das Recht und die Verpflichtung von Einzelpersonen, Gruppen und Organen der Gesellschaft, die allgemein anerkannten Menschenrechte und Grundfreiheiten zu fördern und zu schützen' verabschiedet. In Art. 12 Abs. 2 wird festgehalten, die Staaten hätten alle notwendigen Maßnahmen zu ergreifen, um sicherzustellen, dass die zuständigen Behörden jeden, einzeln wie auch in Gemeinschaft mit anderen, vor jeder Gewalt, Bedrohung, Vergeltung, tatsächlichen oder rechtlichen Diskriminierung, jedem Druck sowie vor jeglichen anderen Willkürhandlungen schützen, die eine Folge seiner rechtmäßigen Ausübung der in dieser Erklärung genannten Rechte sind. Gefordert wird also u.a. ein aktiver Schutz von Human Rights Defenders (http://www.ohchr.org/Documents/Issues/Defenders/Declaration/DeklarationGerman.pdf).

Ein zentraler, im Rahmen der Prüfung der Grundrechtskonformität zu beachtender Aspekt der zitierten Berichte liegt darin, dass Menschenrechtseinschränkungen nur dann zulässig sein können, wenn der betreffende Staat die Notwendigkeit dieser Einschränkungen belegen kann. So hält der Bericht vom 30. Juni 2014 fest (S. 8):

> *«In its general comment No. 31 on the nature of the general legal obligation on States parties to the Covenant, for example, the Human Rights Committee provides that States parties must refrain from violation of the rights recognized by the Covenant, and that any restrictions on any of [those] rights must be permissible under the relevant*

provisions of the Covenant. Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights.»

33. Im Rahmen der Überprüfung der Verhältnismässigkeit und Notwendigkeit der mit der Vorratsdatenspeicherung verbundenen Grundrechtseinschränkungen kann nicht einfach die Regelung des Gesetzgebers quasi als abschliessender gesetzgeberischer Entscheid hingenommen werden. Ob die getroffene Regelung verhältnismässig ist, muss effektiv überprüft werden, und die Notwendigkeit derselben ist vom Staat zu belegen, andernfalls kann sie nicht als menschenrechtskonform taxiert werden.

34. Insgesamt führ die bestehende Regelung der Vorratsdatenspeicherung zu unverhältnismässigen Eingriffen in die Grundrechte. Die anlasslose Speicherung an sich erscheint weder als notwendig, noch besteht hierfür ein überwiegendes Interesse. Die Speicherung und Verwendung der Vorratsdaten gemäss geltender Praxis beschränkt sich nicht auf die Verfolgung (ausreichend) schwerer Kriminalität. Die dadurch bewirkten Grundrechtseingriffe erscheinen nicht als gerechtfertigt. Die bestehende Regelung erscheint auch nicht i.S.v. Art. 8 EMRK als in einer demokratischen Gesellschaft notwendig für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Sie geht weit über das in diesem Sinn Notwendige hinaus. Die in Art. 269 Abs. 1 lit. c formulierten Voraussetzungen schränken die Verwendung von Vorratsdaten ungenügend ein, indem sie die Verwendung von Vorratsdaten nicht bloss zulassen, wenn dies für die Verfolgung einer Straftat als notwendig erscheint, sondern alternativ eine der genannten Voraussetzungen genügt. Allein die Erfolglosigkeit der bisherigen Ermittlungen, die Aussichtslosigkeit oder die unverhältnismässige Erschwerung der Ermittlungen begründet (je) noch nicht die Notwendigkeit der Verwendung der Vorratsdaten. Auch wenn eine der hier aufgezählten Voraussetzungen gegeben ist, kann nicht ohne Weiteres bzw. in zahlreichen Fällen nicht davon gesprochen werden, dass die Verwendung der Vorratsdaten für die Aufklärung der Straftat notwendig ist. Es entspricht aber der Praxis der Gerichte, eine der Voraussetzungen genügen zu lassen bzw. keine einlässliche Prüfung der Notwendigkeit vorzunehmen. Es ist unverhältnismässig, dass eine Person Kommunikationskanäle, welche der Vorratsdatenspeicherung unterliegen, nicht nutzen kann, ohne dass ihre Daten gespeichert werden und allenfalls in einem Strafverfahren genutzt werden können, dass die Person also insoweit nicht kommunizieren kann, ohne schwer wiegende Eingriffe in ihre Grundrechte zu erleiden, und dies auch dann, wenn sie persönlich

keinen konkreten Anlass hierfür geboten hat. Die Vorratsdatenspeicherung verletzt somit das Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung, die Freiheit der Meinungsäusserung, die Meinungs- und Informations- sowie die Medienfreiheit, die persönliche Freiheit und die Bewegungsfreiheit sowie die Unschuldsvermutung.

I. Verhältnismässigkeit und Grundrechtskonformität in Bezug auf den Quellenschutz

1. Die Vorinstanz befasst sich nicht im Einzelnen mit der von Seiten der Beschwerdeführer monierten Verletzung des Quellenschutzes und der Medienfreiheit. Sie beschränkt sich auf die Feststellung, die entsprechenden Vorbringen seien in einem allfälligen Strafprozess zu erheben (E 13.). Der Quellenschutz und die Medienfreiheit werden aber bereits durch die Speicherung der Vorratsdaten selbst verletzt und eine Wahrung dieser Grundrechte ist im Strafprozess eben nicht gewährleistet. Soweit sich der Journalist überhaupt in einem Strafprozess wehren könnte, könnte er damit jedenfalls nicht bewirken, dass die Verletzung des Quellenschutzes ungeschehen gemacht wird. Die Ausführungen der Vorinstanz sind damit offenkundig unzulänglich, verletzen die Beschwerdeführer 4 und 5 in ihrem rechtlichen Gehör und in ihrem Anspruch auf eine effektive Beschwerde (Art. 29 Abs. 2 BV, Art. 13 EMRK).

2. Art 28a StGB und Art. 172 StPO verankern den Quellenschutz und postulieren grundsätzlich die Straflosigkeit und ein Verbot strafprozessualer Zwangsmassnahmen für den Fall, dass ein Journalist als Zeuge seine Quelle nicht offen legt. Der Schutz der Medienfreiheit und der Quellenschutz haben damit zwar grundsätzlich Eingang in die Strafprozessordnung gefunden. Dieser Schutz erweist sich aber in mehrerer Hinsicht als ungenügend. Ungeachtet des für Journalisten bestehenden Zeugnisverweigerungsrechts werden Metadaten, die von der Vorratsdatenspeicherung betroffen sind, auch im Verkehr zwischen Journalisten und ihren Kommunikationspartnern, einschliesslich ihrer Quellen, erfasst. Diese Metadaten können Hinweise auf die Quellen des Journalisten erlauben. Dies stellt einen Eingriff in die Medienfreiheit dar, da mit jeder Form von Kommunikation, die der Vorratsdatenspeicherung unterliegt, der Quellenschutz insoweit durchbrochen wird. Angesichts der eminenten Wichtigkeit des Quellenschutzes wiegt dieser Eingriff schwer.

3. Soweit das in Art. 28a StGB enthaltene Verbot von Zwangsmassnahmen greift, ist der Journalist zwar davor geschützt, dass die vorhandenen Metadaten durch Anordnung von Massnahmen gemäss Art. 273 StPO (Auskunft über Verkehr- und Rechnungsdaten Teilnehmeridentifikation) gegen den Journalisten an die Staatsanwaltschaft gelangen. Eine solche Mass-

nahme ist damit unzulässig, soweit sie nur zum Ziel hat, den Quellenschutz zu unterlaufen (HANSJAKOB, Kommentar BÜPF/VÜPF, Art. 4 N 31 ff). Dies ändert aber nichts daran, dass die entsprechenden Metadaten, die in der Kommunikation mit Quellen anfallen, im Rahmen der Vorratsdatenspeicherung erfasst werden.

4. Art. 271 StPO verankert den Schutz von Berufsgeheimnissen i.S.v. Art. 271 StPO bei Überwachungen. Richtet sich die Überwachung gegen eine Person, die einer Berufsgruppe gemäss Art. 170 - 173 angehört, so sind Informationen, die mit dem Gegenstand der Ermittlungen und dem Grund, aus dem diese Person überwacht wird, nicht in Zusammenhang stehen, unter der Leitung eines Gerichts auszusondern. Dabei dürfen der Strafverfolgungsbehörde keine Berufsgeheimnisse zur Kenntnis gelangen. Art. 271 Abs. 2 StPO schränkt die Zulässigkeit von Direktschaltungen ein in Fällen, in denen sich die Überwachung gegen Berufsgeheimnisträge richtet. Gemäss Art. 271 Abs. 3 sind bei der Überwachung anderer Personen Informationen, über welche eine in den Art. 170 - 173 genannte Person das Zeugnis verweigern könnte, aus den Verfahrensakten auszusondern und sofort zu vernichte; sie dürfen nicht verwendet werden.

5. Zwar bezieht sich Art. 271 StPO auch auf den Quellenschutz von Journalisten. Ein effektiver Schutz der Grundrechte des Journalisten in Bezug auf die Verwendung von Daten aus der Vorratsdatenspeicherung resultiert daraus nicht. Vom Wortlaut her ist nicht einmal klar, ob sich Art. 271 StPO auf die Auskunft über Vorratsdaten nach Art. 273 StPO bezieht. Abgesehen schützt Art. 271 StPO den Journalisten bzw. seine Grundrechte nicht zureichend. Gerade bei Vorratsdaten lässt sich nicht vermeiden, dass diese der Strafverfolgungsbehörde zur Kenntnis gelangen, bevor die Mechanismen, wie sie in Art. 271 StPO vorgesehen sind, greifen können.

6. Die gesetzlich vorgesehene Beschränkung der Zulässigkeit von Direktschaltungen lässt sich in der Praxis seit einigen Jahren nicht mehr durchsetzen, da es kurz gesagt technisch gesehen im aktuellen System nur noch Direktschaltungen gibt. Die Ermittlungsbehörden von Bund und Kantonen können jederzeit und unmittelbar auf die aufgezeichneten Gespräche etc. zugreifen. Die Bestimmung von Art. 274 Abs. 4 lit. b StPO, wonach sich das Zwangsmassnahmengericht zur Zulässigkeit von Direktschaltungen äussern muss, ist damit obsolet (NIKLAUS SCHMID, Handbuch des Schweizerischen Strafprozesses, Zürich/St. Gallen 2009, N 1146; HANSJAKOB, StPO-Kommentar, Art. 271 StPO N 11; BaslerKomm/JEAN-RICHARD-DIT-BRESSEL, Art. 269 StPO N 12, Art. 271 StPO N 10, Art. 274 StPO N 8).

7. Fatal für den Quellenschutz ist auch die Regelung, wonach die Staatsanwaltschaft die geheime Überwachung anordnet und das Zwangsmassnahmengericht erst nachträglich innert fünf Tagen über dessen Zulässigkeit entscheidet (Art. 274 StPO). Daten, die unmittelbar nach der Anordnung anfallen, sind für die Staatsanwaltschaft laufend

einsehbar und können von dieser ausgewertet werden. Die Strafverfolgungsbehörden können nicht gleichzeitig die in Echtzeit hereinkommenden Daten für das laufende Strafverfahren nutzen und dieselben Daten, soweit sie dem Quellenschutz unterliegen, nicht zur Kenntnis nehmen. Tangieren die anfallenden Daten den Quellenschutz, ist dieser damit bereits durchbrochen (GYÖRFFY, a.a.O., Rz. 19 f.). Dies gilt auch für anfallende Vorratsdaten.

8. Die Vorschrift, bei der Überwachung von Drittpersonen seien Informationen, die dem Zeugnisverweigerungsrecht unterliegen, aus den Akten zu nehmen, und die entsprechenden Informationen würden einem Verwertungsverbot unterliegen, genügt zum Schutz des Journalisten bzw. seiner Quelle nicht. Man hat versucht, den Quellenschutz zu gewährleisten, indem man den Journalisten denselben Vorschriften unterstellt hat wie andere Geheimnisträger. Dabei hat der Gesetzgeber übersehen, dass es hier entscheidende Unterschiede gibt. Anders als etwa bei Anwälten, Geistlichen und Ärzten geht es beim Quellenschutz nicht nur um das Gegenüber des Geheimnisträgers, sondern mindestens ebenso um den Geheimnisträge selbst. Während dem der Schutz des Anwaltsgeheimnisses dem Klienten dienen soll, bezieht sich der Quellenschutz als Teil der Medienfreiheit und des Redaktionsgeheimnisses (Art. 17 BV) primär auf den Journalisten.

9. Art. 271 StPO gewährt dem Journalisten keinen wirksamem Schutz seiner Grundrechte. Zum Einen liegt die entscheidende Information, nämlich dass, wo und über welchen Kanal ein Journalist mit einer anderen Person kommuniziert hat, in den eingeholten Vorratsdaten selbst. Soweit es sich beim Kommunikationspartner um eine geschützte Quelle handelt, liegt die entsprechende Information den Strafverfolgungsbehörden mit der Einholung der Auskunft über die Vorratsdaten unmittelbar vor. Die Strafverfolgungsbehörden erlangen damit ohne Weiteres über den Kontakt mit einer anderen Person Kenntnis. Ist diese andere Person eine Quelle des Journalisten, ist der Quellenschutz damit ausgehebelt. Zum Anderen ist der Journalist weniger umfassend geschützt als etwa der Anwalt. Beim Anwalt ist grundsätzlich die gesamte Kommunikation in seiner Berufssphäre durch das Anwaltsgeheimnis geschützt. Beim Journalisten hingegen bezieht sich der Schutz nur auf seine Quelle, nicht auf irgendwelche andere Kontakte, da er nur insoweit über ein Zeugnisverweigerungsrecht verfügt. Absurderweise würde damit die Durchsetzung der Aussonderung und Unverwertbarkeit nach Art. 271 Abs. 3 StPO beim Journalisten voraussetzen, dass der Behörde, welche die Aussonderung vornimmt und sich der Unverwertbarkeit bewusst sein soll, gerade davon Kenntnis hat, dass es sich um eine Quelle handelt. Anders kann sie das – eben nur selektiv auf Quellen bezogene – Zeugnisverweigerungsrecht im konkreten Fall gar nicht berücksichtigen. Wenn es nun aber der Strafverfolgungsbehörden von sich aus oder aufgrund von Angaben der Quelle oder des Journalisten klar wird, dass sich die Kommunikation auf eine geschützte Quelle des Journalisten bezieht, ist der Quellenschutz bereits ausgehebelt und das Zeugnisverwei-

gerungsrecht wertlos. Eine nachherige Entfernung der entsprechenden Daten ändert daran nichts, ebenso wenig ein Verwertungsverbot. Die entsprechenden Daten mögen danach nicht mehr in den Akten sein. Das Wissen, wer die Quelle des Journalisten ist, ist bereits in die Köpfe der damit befassten Strafverfolgungsbehörden gelangt. Gerade am Quellenschutz des Journalisten, bei dem es zentral darum geht, wer mit wem kommuniziert, zeigt sich, wie einschneidend es sein kann, wenn Vorratsdaten an die Strafverfolgungsbehörden gelangen. Anders als etwa beim Anwalt, wo es in der Regel zentral um den Inhalt der Kommunikation gehen wird – etwa zwischen Angeschuldigtem und Verteidiger –, ist es beim journalistischen Quellenschutz primär entscheidend, dass keine entsprechenden Metadaten bekannt werden, welche Rückschlüsse auf die Kommunikationspartner ermöglichen.

10. Hinzu kommt, dass eine selektive Löschung der dem Zeugnisverweigerungsrecht des Journalisten unterstehenden Daten mitunter gar nicht möglich ist. In der Praxis ist eine teilweise Entfernung von Daten nicht oder nur eingeschränkt möglich. Grundsätzlich ist die Datenintegrität zu wahren. Ein weiteres Problem besteht insoweit, als die überwachte Person ein Interesse haben kann, dass auch Kommunikationsdaten mit Geheimnisträgern Eingang in die Untersuchung finden. Werden solche Daten sofort ausgesondert und vernichtet, dann können sie nicht mehr ins Verfahren eingeführt werden, auch wenn dies die betreffende Person später beantragt. Schliesslich kommt es immer wieder vor, dass Kommunikation teilweise geschützte Geheimnisse betrifft, aber auch Passagen beinhaltet, die verwertbar sind. Die teilweise Löschung einzelner Kommunikationsvorgänge ist allerdings vom System her nicht möglich und wäre auch bedenklich aufgrund der damit verbundenen Missbrauchsgefahr. Es bedarf jedenfalls einer Anordnung durch die Staatsanwaltschaft, was wiederum voraussetzt, dass die Staatsanwaltschaft die entsprechenden Daten zuvor zur Kenntnis genommen hat (vgl. HANSJAKOB, StPO-Kommentar, Art. 271 StPO N 15 ff.).

11. Weil Überwachungsmassnahmen geheim sind, weiss der betroffene Journalist zunächst nichts von diesen, sondern wird allenfalls im Nachhinein darüber orientiert, was allerdings in der Praxis auch nicht in jeder Konstellation garantiert ist, insbesondere dann nicht, wenn der Journalist lediglich Verbindungspartner der überwachten Person. Werden Vorratsdaten aus einer Anordnung verwendet, bei der der Journalist selbst nicht Subjekt Massnahme ist, aber ihn betreffende Vorratsdaten herausgegeben werden, wird er nicht orientiert. Er hat nach h. L. nicht einmal ein Beschwerderecht, was der Praxis des EGMR widerspricht, gemäss der Gesprächspartner von überwachten Personen Anspruch auf eine wirksame Beschwerde nach Art. 13 EMRK haben. Wird die Aussonderung durch das Gericht vorgenommen, bevor die Betroffenen über die Massnahme orientiert sind, so ist der Journalist bei der Aussonderung nicht involviert, dies unabängig davon, ob ihn diese als überwachte Person oder sonstwie betrifft. In dieser Situation obliegt die

Gewährleistung des Quellenschutzes den übrigen Beteiligten, also der mit der Auswertung betrauten Behörde und dem mit der Leitung betrauten Gericht. Dabei kann es sich wegen der Relativität des den Journalisten betreffenden Zeugnisverweigerungsrechts ergeben, dass die anordnende Behörde von Tatsachen Kenntnis erhält, deren Schutz nach Art. 264 Abs. 1 StPO gerade bezweckt ist. Es ist für die involvierten Stellen auch nicht unbedingt ersichtlich, dass der Quellenschutz tangiert ist. Schliesslich besteht ein eigentlich unlösbares Problem, indem die involvierten Stellen einerseits zur Wahrung des Quellenschutzes realisieren müsste, dass dieser tangiert sein könnte. Hierfür müssten sie aber gewisse Kenntnis über die Daten haben, was beim Quellenschutz gerade zu dessen Verletzung führen kann (BaslerKomm, JEAN-RICHARD-DIT-BRESSEL, Art. 271 StPO N 10 f.; HANSJAKOB, StPO-Kommentar, Art. 271 N 8, N 14 f.; SCHMID, StPO Praxiskommentar, Art. 271 N 9; BaslerKomm/BOMMER/GOLDSCHMID, Art. 264 StPO, N 58 f.; GYÖRFFY, a.a.O., Rz. 24 ff.).

12. Anschaulich für die Probleme bei der Umsetzung des Quellenschutzes erscheint ein Fall, der Urs Paul Engeler in seiner journalistischen Tätigkeit betrifft (vgl. https://dominiquestrebel.wordpress.com; zum Quellenschutz im diesbezüglichen Strafverfahren auch BGE 140 IV 108).

13. Es bestehen damit keine wirksamen Schutzmechanismen gegen die mit der Vorratsdatenspeicherung verbundene Kompromittierung des Quellenschutzes. Der Journalist muss damit rechnen, dass Vorratsdaten, die durch die Kommunikation mit Quellen anfallen, in einem Strafverfahren beigezogen werden und so seine Quellen offen legen. Der Quellenschutz ist damit durch die Vorratsdatenspeicherung beeinträchtigt und kann nicht mehr garantiert werden, sobald der Journalist Kommunikationsmittel verwendet, die der Vorratsdatenspeicherung unterliegen. Die mit der Vorratsdatenspeicherung verbundenen Einschränkungen der Grundrechte wiegen damit für ihn besonders schwer, einschliesslich des darin enthaltenen «chilling effects». Die Vorratsdatenspeicherung beeinträchtigt damit seine Arbeit bzw. seine Arbeitsweise nachhaltig, zumal er als Journalist eigentlich essenziell auf Kommunikation und die Nutzung zeitgemässer Kommunikationskanäle angewiesen ist. Der Journalist steht vor der Wahl, sich bei der Kommunikation, die der Vorratsdatenspeicherung unterliegt, vom Quellenschutz zu verabschieden, oder aber, diese Kommunikationsformen nicht mehr zu nutzen. Der Anspruch auf Quellenschutz und auf Medienfreiheit ist damit verletzt.

14. Einen Eindruck für die Bedeutung des Quellenschutzes für einen Journalisten in der heutigen Zeit geben Fälle, die dessen konkrete Bedeutung aufzeigen, etwa bei der Publikation der Enthüllungen von Edward Snowden u.a. durch Laura Poitras und Glenn Greenwald bzw. nur schon die Tatsache, wie viele Daten und Kommunikationserbindungen bei der journalistischen Tätigkeit anfallen (https://de.wikipedia.org/wiki/Laura_Poitras; http://www.journalist.de/aktuelles/meldungen/aufgeflogen-daniel-

mossbruckers-experiment-zur-vorratsdatenspeicherung.html). In der Auseinandersetzung um die Wiedereinführung der Vorratsdatenspeicherung in Deutschland sind gewichtige ablehnende Voten abgegeben worden, welche auf die Unvereinbarkeit mit dem Quellenschutz hinweisen (GYÖRFFY, a.a.O., Rz. 39 m.w.H.; https://netzpolitik.org/wp-upload/2015-05-15_BMJV-Referentenentwurf-Vorratsdatenspeicherung.pdf; http://www.djv.de/fileadmin/user_upload/Infos_PDFs/Gemeinsame_PM_11_06_15.pdf).

K. Schlussfolgerungen

1. Von den vorstehenden Grundrechtsverletzungen durch die Vorratsdaten-speicherung sind die Beschwerdeführer als Kunden ihrer Anbieterinnen konkret betroffen. Die Anbieterinnen müssen die entsprechenden, sie betreffenden Daten während sechs Monaten aufbewahren. Dies ist, wie dargelegt, mit den Grundrechten der Beschwerdeführer nicht vereinbar. Es gibt hierfür insbesondere keine genügende gesetzliche Grundlage, und der Eingriff in die Grundrechte ist wie dargelegt unverhältnismässig. Er verletzt die Grundrechte der Beschwerdeführer, namentlich das Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung, die Freiheit der Meinungsäusserung, die Meinungs- und Informations- sowie die Medienfreiheit, die persönliche Freiheit und die Bewegungsfreiheit sowie die Unschuldsvermutung. In ihren konkreten Verhältnisse sind die Beschwerdeführer davon wie folgt betroffen:

2. Der Beschwerdeführer 1 ist Nationalrat und Fraktionspräsident der Grünen. Privat und politisch beschäftigt er sich mit Überwachung im öffentlichen und digitalen Raum und setzt sich für Meinungsfreiheit und den ungehinderten Zugang zu Informationen ein. Zudem engagiert er sich als Vorstandsmitglied des Vereins SPAZ (Sans-Papiers Anlaufstelle Zürich) und des Vereins Solidarité sans frontières u.a. für die Ausübung der Grundrechte von Sans-Papiers, Asylsuchender und anderer MigrantInnen.

   Der Beschwerdeführer 1 verkehrt in seiner Funktion als Nationalrat, aber auch aufgrund des Engagements in den genannten Fällen immer wieder mit AnwältInnen und Anwälten, um in einzelnen Sachfragen für sich und für Dritte kundigen Rechtsbeistand zu erhalten. Dabei wäre er eigentlich darauf angewiesen, vom Anwaltsgeheimnis profitieren zu können. Dies wird allerdings durch die Vorratsdatenspeicherung partiell untergraben.

   Als nationaler Parlamentarier erhält der Beschwerdeführer 1 immer wieder auch vertrauliche Informationen aus der Bevölkerung via Email und Telefon. Zur Klärung der Sachverhalte nimmt er im Gegenzug auch über die erwähnten Kanäle Kontakt mit den betreffenden Personen auf und vermittelt gegebenenfalls Kontakte zu Medienschaffenden oder

kontaktiert diese direkt. Die Vorratsdatenspeicherung untergräbt gerade in diesen sensiblen Fällen nicht nur den Schutz der Privatsphäre und das Brief-, Post- und Fernmeldegeheimnis beider Kommunikationspartner, sondern untergräbt in der Konsequenz auch den eigentlich gesetzlich gegebenen Quellenschutz.

Eine technisch mögliche, verschlüsselte und vor allem verschleierte Kommunikation, welche insbesondere keine auswertbaren Randdaten erzeugt z.B. setzt erhebliche technische Kenntnisse bei allen Kommunikationspartnern voraus. Gerade die üblichen Verschlüsselungstechnologien verschlüsseln zwar die Inhalte der Kommunikation, verschleiern aber nicht die Randdaten der Kommunikation. Trotz gewisser technischer Möglichkeiten fallen damit durch die Vorratsdatenspeicherung entsprechende Daten mit Bezug auf den Beschwerdeführer 1 an, und er ist in seinem Kommunikationsverhalten beeinträchtigt.

3. Der Beschwerdeführer 2 ist Aktivist des Chaos Computer Club Zürich CCCZH und ferner am Aufbau des Chaos Computer Club Schweiz CCC-CH beteiligt. Als Student der Universität Zürich ist er in diversen studentischen Organisationen aktiv, darunter dem Verband der Studierenden der Universität Zürich VSUZH, der linken studentischen Organisation kritische Politik kriPo sowie diversen Protestnetzwerken.

   Immer wieder hat er mit Personen zu tun, welche sich am äusseren linken Rand der Gesellschaft bewegen und in Projekten aktiv sind, welche sich in rechtlichen Grauzonen aufhalten, so etwa dem Autonomen Beauty Salon ABS oder der Autonomen Schule Zürich ASZ. Im Bereich der digitalen Gesellschaft ist Beschwerdeführer 2 oft in Kenntnis vieler Zusammenhänge, welche in Enthüllungen münden.

   Auf Grund seiner Aktivitäten an neuralgischen Punkten von Netz- als auch linker Politik geht er davon aus, in vielen Kommunikationsnetzwerken, wie diese aus der Vorratsdatenspeicherung einsehbar sind, in bedeutender Stellung zu sein.

   Der Beschwerdeführer hat seine Masterarbeit am Institut für Computerlinguistik an der Universität Zürich zum Thema «Computerlinguistik und Massenüberwachung» geschrieben (archive.org/details/MA_computerlinguistikmassenueberwachung).
   Während seines Studiums war er vom Einsatz des vorübergehend von der Universität eingesetzten «Pornografiefilters» betroffen (http://www.nzz.ch/digital/universitaet-zuerich-schaltet-pornofilter-vorerst-ab-1.18265443), und sein universitäres E-Mailkontos war von den Datenlieferungen an die Staatsanwaltschaft im Zuge der «Mörgeli-Affäre» erfasst, bei der dann auch Telefonkontakte über universitäre Anschlüsse ausgewertet wurden. Dabei ging es um Medienkontakte, wodurch der Beschwerdeführer 2 ins Visier geriet, weil (in ganz anderem

Zusammenhang) E-Mailverkehr «Tages-Anzeiger» geführt hatte (vgl. zur «Mörgeli-Affäre» und zum Fall Ritzmann 1B_26/2016 sowie GYÖRFFY, a.a.O., Rz. 28 ff.).

Gegeben seine Absicht, unterdrückten Minderheiten zu einer Stimme zu verhelfen, und der Gesellschaft insgesamt mehr Transparenz und demokratische Kontrolle über soziale Institutionen zu verschaffen, erachtet der Beschwerdeführer seine Aktivitäten als legitim und schützenswert.

Durch seine Kenntnis der Vorratsdatenspeicherung und insbesondere dem Bewusstsein darüber, dass auch immer wieder Dritte Gegenstand der durch die Vorratsdatenspeicherung möglichen «rückwirkenden Überwachung» werden können, sieht er sich zu oft mit der Situation konfrontiert, das Mobiltelefon bewusst nicht oder nur eingeschränkt zu verwenden, bewusst ein-, auszuschalten, bewusst zuhause zu lassen oder falsche Spuren zu legen.

Der Beschwerdeführer 2 versucht, sich nach Möglichkeit gegen die Überwachungsmassnahmen zu behelfen. Dies geht jedoch nur eingeschränkt und der Beschwerdeführer kann die mannigfaltigen Möglichkeiten der elektronischen Kommunikation aufgrund der Vorratsdatenspeicherung nur mit gewichtigen Beschränkungen nutzen. Insgesamt ist seine Kommunikation durch die Vorratsdatenspeicherung deutlich eingeschränkt.

Der Beschwerdeführer 2 weiss, dass dieser «Überwachungsdruck» nicht nur bei ihm, sondern auch bei vielen anderen Aktivisten mit Bewusstsein über die Vorratsdatenspeicherung dazu führt, dass sie sich in ihrer Meinungsäusserungs- als auch Versammlungsfreiheit beschränkt sehen, was insgesamt die demokratische Partizipation auf allen Kanälen stört.

Er ist überzeugt, dass Aufgabe einer progressiven Gesellschaft nicht sein kann, engagierte Menschen am Ausbau der freiheitlichen Strukturen derselben zu hindern: So steht der Beschwerdeführer 2 dafür ein, dass die Vorratsdatenspeicherung auch in der Schweiz abgeschafft gehört.

4. Der Beschwerdeführer 3 ist Informatiker und Telekommunikations-Spezialist. Privat beschäftigt er sich mit Überwachung im öffentlichen und digitalen Raum und setzt sich für Meinungsfreiheit und den ungehinderten Zugang zu Informationen ein.

Wie das Deutsche Bundesverfassungsgericht im Urteil zur Vorratsdaten-speicherung feststellt, ist die anlasslose Speicherung von Telekommunika-tionsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobach-tetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grund-rechte in vielen Bereichen beeinträchtigen kann.

Das Wissen um die Vorratsdatenspeicherung beeinflusst somit die persönliche Kommunikation und die Teilhabe am öffentlichen Leben. So surft der Beschwerdeführer denn schon seit längerem ausschliesslich über Proxy-Server, lässt das Handy öfters mal ausgeschaltet oder zuhause und besitzt anstatt einem modernen Smartphone ein nicht ganz so intelligentes.

Dies macht zwei mögliche Reaktionen sichtbar: Wer sich technisch zu helfen weiss (und entsprechende Ressourcen zur Verfügung hat), umgeht mögliche Überwachungsmassnahmen. Dies kann in einer weiteren Betrachtung dazu führen, dass durch eine flächendeckende und verdachtsunabhängige Vorratsdatenspeicherung gerade für die Aufdeckung schwerer Kriminalität schlussendlich weniger Informationen zur Verfügung stehen, da entsprechende Abwehrmassnahmen getroffen werden. Was in der Logik der Überwacher zu wohl noch tiefgreifenderen Massnahmen führen kann.

Wer nicht in der Lage ist, der Überwachung zu entgehen, wird eher sein Kommunikationsverhalten und seinen Bewegungsfreiraum einschränken. Freie Meinungsäusserung, Versammlungsfreiheit, schlussendlich Teilhabe an demokratischen Prozessen sind beeinträchtigt.

Genau diese Prinzipien muss eine freiheitliche, demokratischen Gesellschaft jedoch gewährleisten. Dafür stehen unsere verfassungsmässig garantieren Grundrechte ein. Die Vorratsdatenspeicherung kollidiert fundamental mit diesen Freiheitsrechten.

Der Beschwerdeführer 3 versucht, sich nach Möglichkeit gegen die Überwachungsmassnahmen zu behelfen. Dies geht jedoch nur eingeschränkt und der Beschwerdeführer kann die mannigfaltigen Möglichkeiten der elektronischen Kommunikation aufgrund der Vorratsdatenspeicherung nur mit gewichtigen Beschränkungen nutzen. Insgesamt ist seine Kommunikation durch die Vorratsdatenspeicherung deutlich eingeschränkt.

5. Der Beschwerdeführer 4 hat in seiner journalistischen Tätigkeit einen Schwerpunkt im Bereich Recherche. Er publiziert u.a. regelmässig kritische Artikel zur Justiz in der Schweiz. Er ist in seiner journalistischen Tätigkeit essenziell darauf angewiesen, dass der Schutz seiner journalistischen Quellen gewährleistet ist.

6. Der Beschwerdeführer 5 ist Journalist, Künstler und Politiker. Er ist Mitglied des Gemeinderats der Stadt St. Gallen und des Kantonsrats St. Gallen. In allen diesen Tätigkeiten ist es für ihn von eminenter Bedeutung, unüberwacht kommunizieren zu können. Als Parlamentarier ist der Beschwerdeführer 5 immer wieder in Kontakt mit der Bevölkerung, erhält verschiedenste Informatio¬nen und stellt Kontakte her. Die Vorratsdatenspeicherung untergräbt ge¬rade in diesen sensiblen Fällen den Schutz der Privatsphäre und das Brief-, Post- und Fernmeldegeheimnis

beider Kommunikationspartner. In seiner journalistischen Tätigkeit ist der Beschwerdeführer 5 essenziell darauf angewie¬sen, dass der Schutz seiner journalistischen Quellen gewährleistet ist.

7. Der Beschwerdeführer 6 beteiligt sich aus einer zivilgesellschaftlichen Perspektive aktiv am internationalen Diskurs zu Internet Governance Themen. Bei eini¬gen dieser Themen gibt es einen direkten Interessenkonflikt zwischen die¬ser zivilgesellschaftlichen Perspektive und den Partikulärinteressen von gewissen in den USA beheimateten Firmen. In den betreffenden politi¬schen Diskursen ist die Anzahl der Personen, die den US-Wirtschafts¬interessen gegenüber freundlich gesinnt sind, sehr gross, und die Koordi¬nation dieser Personen untereinander funktioniert in der Regel auch gut und ist effektiv. Umso wichtiger ist es für Vertreter von anderen zivilgesell¬schaftlichen Perspektiven, ebenfalls miteinander kommunizieren und Dokumente austauschen zu können, ohne dabei damit rechnen zu müssen, dabei möglicherweise bespitzelt zu werden. Aus der Perspektive des Beschwerdeführers 6 sind daher in seiner aktuellen persönlichen Situation die oben in Ziff. II.C.3 angeführten Grundrechte von ganz besonderer Wich¬tigkeit.

   Der Beschwerdeführer 6 nimmt regelmässig an internationalen Konferenzen wie dem Internet Governance Forum (IGF) der Vereinigten Nationen teil und verwendet dabei gelegentlich die Mobiltelefon-Dienstleistung der Anbie¬terin, um mit Personen zu kommunizieren, mit denen er auch Dokumente austauscht, die für politische Gegner von Interesse wären. Nun verfügt der Beschwerdeführer 6 über IT-Fachwissen, das ihm erlaubt, seine Computer relativ gut vor unauthorisiertem Zugriff zu schützen. Die Computer vieler Kommunikationspartner sind deutlich weniger gut geschützt.

   Die Vorratsdatenspeicherung ohne angemessene Vorkehrungen zum Schutz der Kommunikations-Randdaten vor unauthorisiertem Zugriff führt damit dazu, das ein Angreifer, der sich Zugriff auf diese Kommunikations-Randdaten verschafft, damit Kenntnis erlangt, in welche relativ schlecht geschützten Computer einzubrechen wäre, um inhaltlichen Zugriff auf die Kommunition des Abtragstellers zu erlangen.

   Darüber hinaus sind in diesen politischen Kontexten die Kommunikations-Randdaten selber, aus denen ja hervorgeht, wer mit wem kommuniziert, insofern in besonderer Weise schützenswert, als es extrem unfair ist und einen Machtfaktor bedeutet, wenn einseitig eine Seite in den politischen Auseinandersetzungen Einblick in die Kommunikationsgewohnheiten der anderen Seite hat.

   Der Beschwerdeführer 6 ist darauf angewiesen, dass angemessene besondere Vorkehrungen zum Schutz der Kommunikations-Randdaten vor unauthorisiertem Zugriff bestehen.

8. Die Speicherung der Vorratsdaten ist grundrechtswidrig. Der angefochtene Entscheid ist somit aufzuheben. Zur Wahrung der Grundrechte bzw. zur Wiederherstellung eines grundrechtskonformen Zustands sind die Anbieterinnen anzuweisen, die im Rahmen der Vorratsdatenspeicherung aufbewahrten Daten der Beschwerdeführer, die bei ihnen Kunden sind, zu löschen, und inskünftig keine Vorratsdaten zu speichern, soweit die betroffenen Daten nicht für die Erbringung der vertraglichen Leistungen gegenüber dem Beschwerdeführer zwingend erforderlich sind. Die Nutzung der bereits vorliegenden, grundrechtswidrig gespeicherten Daten wäre ebenfalls grundrechtswidrig. Aus diesem Grund sind die Anbieterinnen überdies anzuweisen bzw. zu verpflichten, keine entsprechenden Daten gestützt auf das BÜPF an den Dienst ÜPF oder an andere Behörden oder an Gerichte herauszugeben. Allenfalls ist die Angelegenheit hierfür an die Vorinstanz oder an den Beschwerdegegner zurückzuweisen, damit diese dem entsprechend verfahren.

Abschliessend ersuche ich Sie um Gutheissung der eingangs gestellten Anträge.

Mit freundlichen Grüssen

Viktor Györffy

Dreifach

Beilagen:
1. Vollmacht des Beschwerdeführers 1 in Kopie
2. Vollmacht des Beschwerdeführers 2 in Kopie
3. Vollmacht des Beschwerdeführers 3 in Kopie
4. Vollmacht des Beschwerdeführers 4 in Kopie
5. Vollmacht des Beschwerdeführers 5 in Kopie
6. Vollmacht des Beschwerdeführers 6 in Kopie
7. Angefochtenes Urteil in Kopie