

EuGH: Vorratsdatenspeicherungsrichtlinie 2006/24/EG für ungültig erklärt

Gedanken zum Urteil des EuGH vom 8. April 2014 in den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland Ltd. et al., mit einem Blick auf neue österreichische und schweizerische Entscheide

SIMON SCHLAURI* | DANIEL RONZANI**

Mit Urteil vom 8. April 2014 erklärte der EuGH die Europäische Vorratsdatenspeicherungsrichtlinie 2006/24/EG für ungültig. Damit beantwortete er zwei Vorabentscheidungsgesuche des High Court of Ireland (Rs. C-293/12) und des Verfassungsgerichtshofs Österreich (Rs. C-594/12). Er hielt fest, 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. Der Eingriff durch die Vorratsdatenspeicherungsrichtlinie in diese Grundrechte sei unverhältnismässig, weshalb die Richtlinie ungültig sei. In der Folge erklärte auch der Österreichische Verfassungsgerichtshof die Gesetze zur Vorratsdatenspeicherung in Österreich für verfassungswidrig. In der Schweiz wurden erste Gesuche um Einstellung der Vorratsdatenspeicherung demgegenüber kürzlich abgewiesen. Eine abweichende Beurteilung durch den Europäischen Gerichtshof für Menschenrechte bleibt jedoch möglich.

Par jugement du 8 avril 2014, la Cour de justice de l'Union européenne a déclaré invalide la directive euro-

péenne 2006/24 sur la conservation des données. Ce faisant, elle répondait à deux demandes de décisions préjudicielles provenant de la High Court of Ireland (Rs. C-293/12) et de la Cour constitutionnelle de la République d'Autriche (Rs. C-594/12). Selon la Cour, la directive violait le droit au respect de la vie privée et de la vie familiale (art. 7) ainsi que le droit à la protection des données à caractère personnel (art. 8) de la Charte des droits fondamentaux de l'Union européenne. L'atteinte à ces droits fondamentaux étant disproportionnée, la directive était invalide. Par la suite, la Cour constitutionnelle d'Autriche a déclaré contraires à la Constitution autrichienne les lois autrichiennes sur la conservation des données. En Suisse en revanche, les premières demandes concernant cette problématique ont récemment été rejetées. Une appréciation différente par la Cour européenne des droits de l'homme reste cependant possible.

- I. Sachverhalt und Vorlagefragen
- II. Die Erwägungen des Gerichtshofs
 1. Zu den anwendbaren Bestimmungen der Charta
 2. Eingriff in die Rechte gemäss Art. 7 und 8 der Charta
 3. Zur Rechtfertigung des Eingriffs
 4. Fazit
- III. Die Folgen des Entscheids
 1. Österreich
 2. Irland
- IV. Vergleich mit der schweizerischen Regelung
 1. Vorratsdatenspeicherung nach Schweizer Recht

2. Der Entscheid des Dienstes ÜPF vom 30. Juni 2014
3. Durch Vorratsdatenspeicherung tangierte Grundrechte
4. Öffentliches Interesse an der Vorratsdatenspeicherung
5. Verhältnismässigkeit
6. Konsequenzen
7. Ausblick

I. Sachverhalt und Vorlagefragen

Der vorliegend besprochene Entscheid des Europäischen Gerichtshofs (im Folgenden: EuGH oder Gerichtshof) betrifft die Rechtmässigkeit der Vorratsdatenspeicherung von Telekommunikationsranddaten in der Europäischen Union. Der irische High Court und der Österreichische Verfassungsgerichtshof hatten dem EuGH im Jahr 2012 je ein Vorabentscheidungsgesuch zur Klärung der Gültigkeit der Richtlinie 2006/24 eingereicht. Aufgrund der Ähnlichkeit der Rechtsfragen wurden beide Fälle vom EuGH verbunden.

Das Ersuchen des irischen High Court (Rechtssache C-293/12) erging in einem Rechtsstreit der Digital Rights Ireland Ltd (im Folgenden: Digital Rights) gegen Organe des irischen Staates und betraf die Rechtmässigkeit legislativer und administrativer Massnahmen zur Vorratsspeicherung von Daten elektronischer Kommunikationsvorgänge zum Zwecke der Strafverfolgung.

Das Ersuchen des Österreichischen Verfassungsgerichtshofs (Rechtssache C-594/12) bezog sich auf verfassungsrechtliche Verfahren, die vor diesem Gericht von der Kärntner Lan-

* PD Dr. iur., Rechtsanwalt, Zürich.

** Ph.D. in Information Systems, LL.M., M.A. HSG, Rechtsanwalt, Zürich.
Die Autoren bedanken sich bei Dr. iur. CAROLINE AEBERLI, lic. iur. VIKTOR GYÖRFFY, Rechtsanwalt, lic. iur. GUY KRAYENBÜHL, Staatsanwalt, und ERIK SCHÖNENBERGER für die kritische Durchsicht des Manuskripts.

desregierung sowie von Herrn Seitlinger, Herrn Tschohl und 11 128 weiteren Antragstellern zur Prüfung der Vereinbarkeit des Gesetzes zur Umsetzung der Richtlinie 2006/24 in österreichisches Recht mit dem Bundes-Verfassungsgesetz anhängig gemacht worden waren.

Die nationalen Gerichte ersuchten den EuGH um die Beantwortung einer Reihe von Vorlagefragen. Der Gerichtshof beschränkte sich am Ende auf die Beantwortung eines Teils dieser Fragen, weil sich die Beantwortung der restlichen Fragen erübrigte. Im Wesentlichen ging es am Ende um die Frage, ob die Vorratsdatenspeicherungsrichtlinie 2006/24 mit den Art. 7 (Achtung des Privat- und Familienlebens) und 8 (Schutz personenbezogener Daten) der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) vereinbar sei. Die ebenfalls aufgeworfene Frage nach einer Verletzung von Art. 11 der Charta (Meinungsäusserungsfreiheit) wurde nicht geprüft.

II. Die Erwägungen des Gerichtshofs

1. Zu den anwendbaren Bestimmungen der Charta

Nach einer Darstellung der Rechtsgrundlagen setzt sich der Gerichtshof mit den genannten Vorlagefragen auseinander. Dies in folgenden (teils gekürzten oder zur Kürzung oder Klärung umformulierten) Erwägungen. Die Ziffern beziehen sich auf den Entscheid des Gerichtshofs.

Rz. 24. Wie sich aus Art. 1 sowie den Erwägungsgründen 4, 5, 7 bis 11, 21 und 22 der Richtlinie 2006/24 ergibt, sollen mit der Richtlinie in erster Linie die Vorschriften der Mitgliedstaaten über die Vorratsspeicherung bestimmter von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes erzeugter oder verarbeiteter Da-

ten harmonisiert werden, um sicherzustellen, dass die Daten, unter Wahrung der in den Art. 7 und 8 der Charta verankerten Rechte, zwecks Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten wie organisierter Kriminalität und Terrorismus zur Verfügung stehen.

Rz. 25/26. Die in Art. 3 der Richtlinie 2006/24 vorgesehene Pflicht der Anbieter zur Vorratsdatenspeicherung (u. a. von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung sowie Endeinrichtung, Standort, Name, Anschrift, Rufnummern oder IP-Adressen von Teilnehmern) wirft Fragen hinsichtlich des in Art. 7 der Charta verankerten Schutzes sowohl des Privatlebens als auch der Kommunikation sowie hinsichtlich des von Art. 8 der Charta erfassten Schutzes personenbezogener Daten auf.

Rz. 27. Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.

2. Eingriff in die Rechte gemäss Art. 7 und 8 der Charta

Rz. 32/34. Durch die Verpflichtung zur Vorratsspeicherung weicht die Richtlinie in Bezug auf die Verarbeitung personenbezogener Daten im Bereich elektronischer Kommunikationsvorgänge von der durch die Richtlinien 95/46 (Datenschutzrichtlinie) und 2002/58 (Datenschutzrichtlinie für elektronische Kommunikation) geschaffenen Regelung zum Schutz des Rechts auf Achtung der Privatsphäre ab. Dies daher, weil diese Richtlinien die Vertraulichkeit der Kommunikation und der Verkehrsdaten vorsehen sowie die Pflicht, diese Daten zu löschen oder zu

anonymisieren, sobald sie für die Übertragung einer Nachricht und zur Rechnungsstellung nicht mehr benötigt werden. Die Pflicht der Anbieter zur Vorratsdatenspeicherung stellt daher einen Eingriff in die durch Art. 7 der Charta garantierten Rechte dar. Auch der Zugang der zuständigen nationalen Behörden zu den Daten stellt einen Eingriff in Art. 7 der Charta dar.

Rz. 36. Desgleichen greift die Richtlinie 2006/24 in das durch Art. 8 der Charta garantierte Grundrecht auf Schutz personenbezogener Daten ein, da sie eine Verarbeitung personenbezogener Daten vorsieht.

Rz. 37. Der mit der Richtlinie verbundene Eingriff in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte ist von grossem Ausmass und als besonders schwerwiegend anzusehen. Ausserdem ist der Umstand, dass die Vorratsspeicherung der Daten und ihre spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird, geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist.

3. Zur Rechtfertigung des Eingriffs

a) Voraussetzungen für einen Eingriff

Rz. 38. Nach Art. 52 Abs. 1 der Charta muss jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten; unter Wahrung des Grundsatzes der Verhältnismässigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

b) Eingriff in den Wesensgehalt

Rz. 40. Die Vorratsspeicherung von Daten ist nicht geeignet, den Wesensgehalt des in Art. 8 der Charta verankerten Grundrechts auf den Schutz personenbezogener Daten anzutasten, da die Richtlinie 2006/24 die Kenntnisnahme des Inhalts elektronischer Kommunikation nicht gestattet.

c) Dem Gemeinwohl dienende Zielsetzung der Union

Rz. 41/42. Materielles Ziel der Richtlinie ist es, zur Bekämpfung schwerer Kriminalität und somit letztlich zur öffentlichen Sicherheit beizutragen. Nach der Rechtsprechung des Gerichtshofs stellt dies eine dem Gemeinwohl dienende Zielsetzung der Union dar, wie sie für einen Grundrechtseingriff von Art. 52 Abs. 1 der Charta gefordert wird. Im Übrigen ist festzustellen, dass nach Art. 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat.

d) Eignung des Eingriffs zur Verfolgung der Zielsetzung

Rz. 45/46. Unter diesen Umständen ist die Verhältnismässigkeit des festgestellten Eingriffs zu prüfen. Der Grundsatz der Verhältnismässigkeit verlangt, dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und dass sie nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist.

Rz. 49. Zu der Frage, ob die Vorratsspeicherung der Daten zur Erreichung des mit der Richtlinie 2006/24 verfolgten Ziels geeignet ist, ist festzustellen, dass angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die nach dieser Richtlinie auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen na-

tionalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und insoweit daher ein nützliches Mittel für strafrechtliche Ermittlungen darstellen. Die Vorratsspeicherung solcher Daten kann somit als zur Erreichung des mit der Richtlinie verfolgten Ziels geeignet angesehen werden.

Rz. 50. Der Umstand, dass es mehrere elektronische Kommunikationsweisen gibt, die nicht in den Anwendungsbereich der Richtlinie fallen oder eine anonyme Kommunikation ermöglichen, vermag zwar die Eignung der in der Vorratsspeicherung der Daten bestehenden Massnahme zur Erreichung des verfolgten Ziels zu begrenzen, führt aber nicht zur Ungeeignetheit dieser Massnahme.

e) Beschränkung des Eingriffs auf das absolut Notwendige

Rz. 51/52. Die Bekämpfung schwerer Kriminalität ist zwar von grösster Bedeutung für die Gewährleistung der öffentlichen Sicherheit, und ihre Wirksamkeit kann in hohem Mass von der Nutzung moderner Ermittlungstechniken abhängen. Eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch für sich genommen die Erforderlichkeit einer Speichermassnahme – wie sie die Richtlinie 2006/24 vorsieht – für die Kriminalitätsbekämpfung nicht rechtfertigen, denn der Schutz des Grundrechts auf Achtung des Privatlebens verlangt jedenfalls, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken.

Rz. 54/55. Daher muss die fragliche Unionsregelung klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Massnahme vorsehen und Mindestanforderungen aufstellen, sodass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen,

die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen. Dies umso mehr, als Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs auf diese besteht.

Rz. 56. Zu der Frage, ob der mit der Richtlinie 2006/24 verbundene Eingriff auf das absolut Notwendige beschränkt ist, ist festzustellen, dass nach Art. 3 dieser Richtlinie in Verbindung mit ihrem Art. 5 Abs. 1 alle Verkehrsdaten betreffend Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie auf Vorrat zu speichern sind. Sie gilt somit für alle elektronischen Kommunikationsmittel, deren Nutzung stark verbreitet und im täglichen Leben jedes Einzelnen von wachsender Bedeutung ist. Ausserdem erfasst die Richtlinie nach ihrem Art. 3 alle Teilnehmer und registrierten Benutzer. Sie führt daher zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung.

Rz. 58. Die Richtlinie 2006/24 betrifft zum einen in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Zudem sieht sie keinerlei Ausnahme vor, sodass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.

Rz. 59. Die Richtlinie soll zum andern zwar 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.

Rz. 60. Im Weiteren sieht die Richtlinie 2006/24 kein objektives Kriterium vor, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten auf Straftaten zu beschränken, die im Hinblick auf das Ausmass und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können.

Rz. 61/62. Die Richtlinie enthält keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung. Insbesondere sieht die Richtlinie kein objektives Kriterium vor, das es erlaubt, die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späterer Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige zu beschränken. Der Zugang zu den gespeicherten Daten unterliegt auch keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht.

Rz. 64. Die Speicherungsfrist liegt zudem zwischen mindestens sechs Monaten und höchstens 24 Monaten, ohne dass ihre Festlegung auf objektiven Kriterien beruhen muss, die gewährleisten, dass sie auf das absolut Notwendige beschränkt wird.

4. Fazit

Rz. 65. Aus dem Vorstehenden folgt, dass die Richtlinie 2006/24 keine klaren und präzisen Regeln zur Tragweite des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte vorsieht. Somit ist festzustellen, dass die Richtlinie einen Eingriff in diese Grundrechte beinhaltet, der in der Rechtsordnung der Union von grossem Ausmass und von besonderer Schwere ist, ohne dass sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.

Rz. 66–68. Darüber hinaus ist festzustellen, dass die Richtlinie 2006/24 keine hinreichenden, den Anforderungen von Art. 8 der Charta entsprechenden Garantien dafür bietet, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung geschützt sind. Insbesondere sieht 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.

Rz. 69–71: Aus der Gesamtheit der vorstehenden Erwägungen ist zu schliessen, dass der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der Verhältnismässigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta einhalten musste. Infolgedessen ist die Richtlinie ungültig.

III. Die Folgen des Entscheids

1. Österreich

Mit Urteil vom 27. Juni 2014¹ erklärte der Verfassungsgerichtshof Österreich

¹ VfGH Österreich, Gesetze zur Vorratsdatenspeicherung in Österreich verfassungswidrig,

die Gesetze zur Vorratsdatenspeicherung in Österreich für verfassungswidrig. Eine Frist zur Reparatur wurde nicht gewährt.

Der Gerichtshof befand, die Vorratsdatenspeicherung sei ein gravierender Eingriff in die Grundrechte, der im Einklang mit dem Datenschutzgesetz und der Menschenrechtskonvention stehen müsse. Die angefochtenen Bestimmungen des Telekommunikationsgesetzes, der Strafprozessordnung und des Sicherheitspolizeigesetzes erfüllten die Bedingungen für die Speicherung, die Anforderungen an die Löschung sowie die Sicherungen beim Zugriff auf die vorratsgespeicherten Daten nicht. Die «Streubreite» der Vorratsdatenspeicherung überträfe die bisher in der Rechtsprechung des Verfassungsgerichtshofes zu beurteilenden Eingriffe in das Grundrecht auf Datenschutz (nahezu die gesamte Bevölkerung, Art der betroffenen Daten sowie Modalität der Datenverwendung).

Das Grundrecht auf Datenschutz sei in einer demokratischen Gesellschaft auf die Ermöglichung und Sicherung vertraulicher Kommunikation zwischen den Menschen gerichtet. Unter Berücksichtigung und Abwägung der neuen Kommunikationsmittel und deren Herausforderungen für die Kriminalitätsbekämpfung und das öffentliche Interesse seien der Einzelne und seine freie Persönlichkeitsentfaltung nicht nur auf die öffentliche Kommunikation in der Gemeinschaft angewiesen; die Freiheit als Anspruch des Individuums und als Zustand einer Gesellschaft werde bestimmt von der Qualität der Informationsbeziehungen, so der Verfassungsgerichtshof. Die Erweiterung der technischen Möglichkeiten

Presseinformation zur Verkündung der Entscheidung G47/2012 u. a. vom 27. Juni 2014, www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/presseinformation_verkuendung_vorratsdaten.pdf. Die Begründung war zum Zeitpunkt der Drucklegung noch nicht verfügbar.

fürte dazu, dass den Gefahren, die diese Erweiterung für die Freiheit des Menschen in sich birgt, in einer dieser Bedrohungen adäquater Weise entgegengetreten werden müsse. Die angefochtenen Bestimmungen über die Vorratsdatenspeicherung im Telekommunikationsgesetz, in der Strafprozessordnung und im Sicherheitspolizeigesetz bildeten jedoch in ihrem Zusammenhang einen unverhältnismässigen Eingriff und damit eine Verletzung des Grundrechts auf Datenschutz.

2. Irland

Zum Zeitpunkt der Drucklegung lag kein Urteil des High Court of Ireland vor.

IV. Vergleich mit der schweizerischen Regelung

1. Vorratsdatenspeicherung nach Schweizer Recht

Zur Aufklärung von Straftaten erhalten Schweizer Strafverfolgungsbehörden unter Umständen Zugriff auf Inhalte und Randdaten von Telekommunikation und Post. Dieser Zugriff ist in Art. 269 ff. StPO sowie im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und der zugehörigen Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) geregelt, wobei die StPO im Wesentlichen die Voraussetzungen der Überwachung durch die Untersuchungsbehörden regelt und das BÜPF die technische Umsetzung auf Providerseite sowie durch den Dienst des Bundes für die Überwachung des Post- und Fernmeldeverkehrs (im Folgenden: Dienst ÜPF)².

Die Regelung der StPO unterscheidet zwischen «rückwirkenden» Überwachungsmassnahmen (nachstehend in Anlehnung an die europäische Terminologie als Vorratsdatenspeicherung bezeichnet) und Echtzeitüberwachung³. Die Vorratsdatenspeicherung ist in Art. 273 StPO geregelt. Sie betrifft Informationen darüber, wann und mit welchen Personen oder Anschlüssen die überwachte Person über den Post- oder Fernmeldeverkehr Verbindung hat oder gehabt hat, sowie Verkehrs- und Rechnungsdaten. Die Art der aufzuzeichnenden Daten wird durch BÜPF und VÜPF und technische Ausführungsbestimmungen konkretisiert. Die Anbieterinnen sind nach geltendem Recht verpflichtet, die Daten während sechs Monaten aufzubewahren (Art. 15 Abs. 3 BÜPF)⁴.

Das BÜPF befindet sich derzeit in Revision. Die Botschaft des Bundesrates und der Entwurf (nachfolgend E-BÜPF) wurden am 27. Februar 2013 zuhanden des Parlaments verabschiedet⁵. Nachdem der Ständerat den Entwurf mehr oder weniger unverändert passieren liess, liegt die Vorlage zum Zeitpunkt der Drucklegung beim Nationalrat. Unter anderem soll der Kreis der Mitwirkungspflichtigen erweitert werden, namentlich um Anbieterinnen sogenannter abgeleiteter Kommunikationsdienste (d.h. von Diensten, die auf dem Internet aufbauen wie E-Mail, Internet-telefonie, Kurznachrichten, Hosting, Cloud-Dienste, Chat-Foren u.dgl.). Je nachdem sind dabei unterschiedliche Mitwirkungspflichten vorgesehen⁶. Nach Art. 27 Abs. 3 E-BÜPF sollen Anbieterinnen abgeleiteter Kommunikationsdienste, die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft an-

bieten, ebenfalls zur Vorratsdatenspeicherung verpflichtet werden können. Geplant ist zudem eine Verdoppelung der Aufbewahrungszeit der Vorratsdaten im Allgemeinen von sechs auf zwölf Monate (Art. 26 Abs. 5 E-BÜPF).

2. Der Entscheid des Dienstes ÜPF vom 30. Juni 2014

Am 20. Februar 2014 reichten sechs Mitglieder der Digitalen Gesellschaft Schweiz beim Dienst ÜPF Gesuche ein, ihre Fernmeldediensteanbieterinnen seien anzuweisen, von den Gesuchstellern keine Randdaten mehr zu speichern, vorhandene Daten zu löschen und künftig keine Daten mehr an Behörden herauszugeben⁷. Die Gesuche wurden mit Verfügung vom 30. Juni 2014 abgewiesen⁸.

Zur Begründung führte der Dienst ÜPF aus, mit dem BÜPF, der zugehörigen Verordnung VÜPF und der StPO bestünden genügende gesetzliche Grundlagen, um auch den (schweren) Eingriff in die Grundrechte zu rechtfertigen, den die Vorratsdatenspeicherung darstelle. Die geltende Gesetzgebung sehe die Speicherung von Randdaten vor, nicht von Gesprächsinhalten. Die Polizei und Staatsanwaltschaft hätten nicht unbeschränkten Zugriff auf diese Randdaten. Zudem dürfe in Straf- und Rechtshilfverfahren die Überwachung nur angeordnet werden, wenn ein dringender Tatverdacht auf ein Verbrechen oder Vergehen bestünde, die Schwere der Straftat die Überwachung rechtfertige, bisherige Untersuchungshandlungen erfolglos geblieben seien oder Er-

² Zum Ganzen T. HANSJAKOB, BÜPF/VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2. Aufl., St. Gallen 2006, Vb. BÜPF N 1 ff.

³ HANSJAKOB (Fn. 2), Vb. BÜPF N 15.

⁴ HANSJAKOB (Fn. 2), BÜPF 15 N 15.

⁵ Botschaft BÜPF, BBl 2013, 2683.

⁶ Art. 26 ff. E-BÜPF; Botschaft BÜPF, BBl 2013, 2694 f., 2705.

⁷ Vgl. KIRE/DIGITALE GESELLSCHAFT SCHWEIZ, Digitale Gesellschaft erhebt Beschwerde gegen Vorratsdatenspeicherung, www.digitale-gesellschaft.ch/2014/02/21/digitale-gesellschaft-erhebt-beschwerde-gegen-vorratsdatenspeicherung.

⁸ Dienst ÜPF, Verfügung vom 30. Juni 2014, abrufbar unter www.balthasar-glaetli.ch/2014/07/04/dienst-uepf-erachtet-ch-vorratsdatenspeicherung-als-rechtmaessig/.

mittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden. Schliesslich müssten für die Überwachung bei einer Notsuche dringende Anhaltspunkte für eine schwere Gefährdung von Gesundheit oder Leben der vermissten Person vorliegen. Der Grundrechtseingriff sei daher verhältnismässig.

3. Durch Vorratsdatenspeicherung tangierte Grundrechte

Aus der Gesamtheit der gesammelten Daten können nach Auffassung des EuGH sehr genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden, weshalb die Vorratsdatenspeicherung die durch Art. 7 der Charta garantierten Rechte (Schutz des Privatlebens) betrifft. Weil es sich bei den gespeicherten Daten um Personendaten handelt, ist auch das Recht auf Schutz personenbezogener Daten nach Art. 8 der Charta betroffen.

In der Schweiz hat nach Art. 13 Abs. 1 BV jede Person Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs. Art. 13 Abs. 1 BV schützt die Kommunikation unabhängig vom verwendeten Kommunikationsmedium, also auch über das Internet⁹. Jede Person hat zudem Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten (Art. 13 Abs. 2 BV). Auf Ebene der EMRK werden der Schutz der Privatsphäre und der Datenschutz in Art. 8 geregelt (Datenschutz nicht explizit, aber gestützt auf Rechtsprechung)¹⁰.

⁹ J.P. MÜLLER/M. SCHEFER, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, 203; vgl. auch die Verfügung des Dienstes ÜPF vom 30. Juni 2014 (Fn. 8), Ziff. 6 ff.

¹⁰ D. ROSENTHAL/Y. JÖHRI, Handkommentar zum Datenschutzgesetz, Zürich 2008, DSG 1 N 3; EGMR vom 26. März 1987, «Leander»/. S, Yearbook of the ECHR 87, 124 (125); J. MOLTHAGEN, Das Verhältnis der EU-Grundrechte zur EMRK, Hamburg 2003, 52.

Auch gemäss der bereits angeführten Entscheidung des Österreichischen Verfassungsgerichtshofs vom 27. Juni 2014 tangiert die Vorratsdatenspeicherung das Grundrecht auf Datenschutz sowie das Recht auf Privat- und Familienleben nach Art. 8 EMRK¹¹. Dasselbe Verständnis lässt sich auch in der erwähnten Verfügung des Dienstes ÜPF vom 30. Juni 2014 erkennen¹².

Auch aus dem Wortlaut und den Erläuterungen von EMRK und Charta lässt sich zudem nicht herleiten, dass der EU-Gesetzgeber mit Art. 7 der Charta einen höheren Schutzstandard hinsichtlich Privatsphäre hätte setzen wollen als er von Art. 8 EMRK vorgegeben ist¹³. Nachdem offensichtlich Personendaten betroffen sind, ist Art. 8 EMRK zudem auch in seiner Funktion als Datenschutznorm tangiert.

Damit dürfte der Auffassung des Gerichtshofs, die Artikel 7 und 8 der Charta seien betroffen, zumindest auch hinsichtlich von Art. 8 EMRK zu folgen sein, der in der Schweiz Anwendung findet. Unseres Erachtens spricht einer direkten Anwendung von Art. 13 Abs. 1 und 2 BV zudem nichts entgegen.

Nach Auffassung des EuGH handelt es sich ferner um einen schweren Eingriff, der jedoch den Wesens- bzw. Kerngehalt des Grundrechts nicht tangiert (Rz. 40). Dem folgt der Dienst ÜPF in seiner Verfügung vom 30. Juni 2014 zu Recht¹⁴.

4. Öffentliches Interesse an der Vorratsdatenspeicherung

Gemäss dem Entscheid des Gerichtshofs Rz. 42) liegt das materielle Ziel der Richtlinie in der Bekämpfung schwerer Kriminalität. Sie dient damit der öffentlichen Sicherheit, die auch nach Schwei-

¹¹ Entscheidung G 47/2012 vom 27. Juni 2014.

¹² Dienst ÜPF, Verfügung vom 30. Juni 2014 (Fn. 8), Ziff. 6 ff.

¹³ Vgl. MOLTHAGEN (Fn. 10), 33.

¹⁴ Dienst ÜPF, Verfügung vom 30. Juni 2014 (Fn. 8), Ziff. 10 f.

zer Rechtsauffassung als öffentliches Interesse anerkannt ist und einen Eingriff in Art. 13 BV rechtfertigen kann¹⁵.

5. Verhältnismässigkeit

a) Eignung

Der Grundsatz der Verhältnismässigkeit verlangt nach europäischem Verständnis, dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen (so der Gerichtshof in Rz. 45). Dem entspricht das Erfordernis der Eignung, das in der schweizerischen Rechtsprechung gestützt auf Art. 36 Abs. 3 BV Anwendung findet¹⁶.

Nach Auffassung des Gerichtshofs ist die Vorratsdatenspeicherung grundsätzlich geeignet, um das mit der Richtlinie verfolgte Ziel der Bekämpfung schwerer Kriminalität zu verfolgen (Rz. 49)¹⁷. Der Gerichtshof stützt sich bei seiner Argumentation darauf, dass die Vorratsdatenspeicherung den Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten würde. Er setzt sich jedoch nicht mit den zur Vorratsdatenspeicherung vorliegenden wissenschaftlichen Stimmen auseinander, die die Wirksamkeit der Vorratsdatenspeicherung hinsichtlich der Förderung der öffentlichen Sicherheit im Allgemeinen gestützt auf statistische Analysen infrage stellen.

So lautet eine Schlussfolgerung einer 2011 erschienenen Studie¹⁸ des Max-Planck-Institutes für ausländisches und internationales Strafrecht, dass sich der Wegfall der Vorratsdatenspei-

¹⁵ U. HÄFELIN/W. HALLER/H. KELLER, Schweizerisches Bundesstaatsrecht, 8. Aufl., Zürich 2012, N 315 ff.

¹⁶ HÄFELIN/HALLER/KELLER (Fn. 15), N 322.

¹⁷ So auch Dienst ÜPF, Verfügung vom 30. Juni 2014 (Fn. 8), Ziff. 24.

¹⁸ MAX-PLANCK-INSTITUT FÜR AUSLÄNDISCHES UND INTERNATIONALES STRAFRECHT, Schutzlücken durch Wegfall der Vorratsdatenspeicherung, 2. Fassung, Freiburg i.Br., Juli 2011, www.mpg.de/5000721/vorratsdatenspeicherung.pdf.

cherung (aufgrund eines Urteils des deutschen Bundesverfassungsgerichts vom 2. März 2010¹⁹ wurde die Vorratsdatenspeicherung in Deutschland gestoppt und seither nicht wieder eingeführt) nicht als Ursache für Bewegungen in der deliktsspezifischen Aufklärungsquote abbilden lässt. Eine andere Schlussfolgerung geht dahin, dass im Vergleich der Aufklärungsquoten, die in Deutschland und in der Schweiz im Jahr 2009 erzielt worden sind, sich keine Hinweise darauf ableiten lassen, dass die in der Schweiz seit etwa 10 Jahren praktizierte Vorratsdatenspeicherung zu einer systematisch höheren Aufklärung geführt hätte. Auch punktuelle Vergleiche zwischen Deutschland, Österreich und der Schweiz, also zwischen Ländern, die unterschiedliche rechtliche Grundlagen im Hinblick auf die Vorratsdatenspeicherung aufweisen, führen gemäss der Studie nicht zu dem Schluss, dass die systematische Sammlung und Speicherung von Verkehrsdaten bzw. deren Fehlen mit sichtbaren Unterschieden in der Sicherheitslage verbunden wären. Auch im Zusammenhang mit der Untersuchung von vier besonders interessanten Delikten, nämlich Enkeltrick, Tötungsdelikte, Kinderpornografie und Stalking, kommt die Studie nicht zum Schluss, dass der Wegfall der Vorratsdatenspeicherung Nachteile mit sich gebracht hätte. Es könne aber auch nicht ausgeschlossen werden, dass in komplexen Verfahren und bei Kapitaldelikten Verkehrsdaten wichtige Indizien repräsentierten oder zusätzliche Ermittlungsansätze schaffen würden. Derartige Fälle würden sich aber auf die Gesamttrends nicht auswirken, sofern sie überhaupt zweifelsfrei identifiziert werden könnten²⁰. Die Studie gesteht ferner zu, dass vorderhand erst unsichere Datengrundlagen bestehen, dass systematische empirische Un-

tersuchungen weitgehend fehlen und sich die befragten Praktiker teils widersprechen.

Grundsätzlich wäre u.E. aber die Eignung der Vorratsdatenspeicherung zur Erreichung des Ziels der Kriminalitätsbekämpfung als solche durchaus zu problematisieren gewesen.

Bemerkenswert ist ferner die Aussage des Gerichtshofs in Rz. 50, wonach der Umstand, dass es Kommunikationsmittel gebe, die nicht überwacht werden könnten, die Eignung der Vorratsdatenspeicherung zwar beschränken, aber nicht zu ihrer Ungeeignetheit führen. Immerhin ist zu erwarten, dass Delinquenten zu einem grossen Teil auf ebensolche Kommunikationsmittel ausweichen würden, sodass die Überwachungsmassnahmen ohnehin ins Leere liefen.

b) Notwendigkeit

Der Gerichtshof gesteht der Bekämpfung der schweren Kriminalität zwar höchste Bedeutung für die Gewährleistung der öffentlichen Sicherheit zu, und er anerkennt, dass die Wirksamkeit der Massnahmen in hohem Mass von der Nutzung moderner Ermittlungstechniken abhängt. Eine solche dem Gemeinwohl dienende Zielsetzung könne jedoch für sich genommen die Erforderlichkeit der Massnahme für die Kriminalitätsbekämpfung nicht rechtfertigen. Es sei weiterhin nötig, die Einschränkungen der betroffenen Grundrechte *auf das absolut Notwendige zu beschränken*.

Entsprechend müsse die fragliche Regelung klare und präzise Regeln vorsehen und Mindestanforderungen aufstellen. Die Richtlinie betreffe jedoch alle Verkehrsdaten des Telefonfestnetzes, des Mobilfunks, des Internetzugangs, von E-Mail und Internet-Telefonie und gelte damit für alle stark verbreiteten Kommunikationsmittel. Ausserdem sei fast die gesamte europäische Bevölkerung betroffen. Auch dif-

ferenziere die Richtlinie nicht zwischen Personen, die sich in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte, und anderen, und sie sehe zudem für Berufsgeheimnisträger keine Ausnahmen vor.

Diese Argumente zur Verhältnismässigkeitsabwägung können für die Beurteilung der Situation in der Schweiz ebenfalls Gültigkeit beanspruchen: Die Überwachung betrifft eine vergleichbar breite Palette von Kommunikationsmitteln (erst recht nach der geplanten Revision des Gesetzes, die auch abgeleitete Kommunikationsdienste mit einbeziehen will), und sie betrifft fast die gesamte schweizerische Bevölkerung. Eine Differenzierung nach Lage der Personen, die Anlass zur Strafverfolgung geben könnte, findet ebenfalls nicht statt, genauso wenig sind Berufsgeheimnisträger von der Speicherung ausgenommen.

Der Gerichtshof führt im Weiteren aus, die Richtlinie verlange keinen Zusammenhang zwischen den zu speichernden Daten und einer Bedrohung der öffentlichen Sicherheit und schränke die Überwachung nicht auf bestimmte Zeiträume, geografische Gebiete oder möglicherweise in schwere Straftaten verwickelte oder anderweitig für die Strafverfolgung interessante Personenkreise ein.

Auch in dieser Hinsicht findet in der Schweiz, weder nach geltendem Recht noch gemäss dem Entwurf, eine Einschränkung statt, sodass die Lage hierzulande mit der im EuGH-Entscheid beurteilten Situation vergleichbar ist.

Im Weiteren bemängelt der Gerichtshof, dass die Richtlinie keine materiell- oder verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung enthalte. Die Zahl der späteren Nutzer sei nicht beschränkt, und es sei keine unabhängige Kontrolle vorgesehen.

Hier weicht das – als nationales Recht naturgemäss weiter konkre-

¹⁹ Urteil des deutschen BVerfG vom 2. März 2010, 1 BvR 256/08.

²⁰ MAX-PLANCK-INSTITUT (Fn. 18), 219 ff.

sierte – Recht der Schweiz teilweise von der Richtlinie ab: Art. 273 Abs. 2 StPO sieht insbesondere eine Genehmigung des Zugriffs auf Vorratsdaten durch das zuständige Zwangsmassnahmengericht vor²¹. Zudem wird vorausgesetzt, dass die Schwere der Straftat die Überwachung rechtfertigt und dass die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden (Art. 273 Abs. 1 i.V.m. Art. 269 Abs. 1 lit. b und c StPO). Die Notwendigkeit des Zugriffs auf die Daten für die Ermittlungen wird damit zumindest für den Einzelfall schon von Gesetzes wegen vorausgesetzt. Indessen kennt auch die Schweiz bezüglich der Datenspeicherung im Allgemeinen keine Einschränkung, wie sie der EuGH genau besehen fordert; sämtliche Nutzer und Randdaten der überwachten Telekommunikationsdienste werden gespeichert.

Ferner besteht in der Schweiz eine allgemeine materielle Beschränkung auf Verbrechen und Vergehen sowie eine Übertretung (Missbrauch von Fernmeldeanlagen), während die Richtlinie den Entscheid über den Katalog der Delikte, bei denen ein Zugriff auf Vorratsdaten zulässig wäre, den Mitgliedstaaten überlässt (Rz. 60). Jedoch ist anzumerken, dass die Überwachung in der Schweiz nach dem Gesagten keineswegs auf «schwere Kriminalität» beschränkt ist, sondern auch bei sämtlichen Verbrechen und Vergehen und – im Einzelfall des Missbrauchs von Telefonanlagen – sogar bei einer Übertretung möglich ist (Art. 273 Abs. 1 StPO).

Das Schweizer Gesetz sieht zudem ebenfalls keine Beschränkung des Kreises der zugriffsberechtigten Personen vor; die Situation ist hier insofern gleich wie in der EU, als die Verantwortung für eine

solche Beschränkung auf die Mitgliedstaaten bzw. Kantone übertragen wird, diesen aber kein Rahmen gesetzt wird.

Im Weiteren bemängelt der EuGH, dass die Richtlinie eine Speicherfrist von 6 bis 24 Monaten vorsieht, ohne dass ihre Festlegung auf objektiven Kriterien beruhen müsse, die gewährleisten, dass sie auf das absolut Notwendige beschränkt würde. Das Schweizer Gesetz sieht derzeit eine Beschränkung auf 6 Monate vor, eine Verdoppelung der Frist auf 12 Monate ist im Entwurf angedacht. Eine Differenzierung findet ebenfalls nicht statt.

Darüber hinaus – so der Gerichtshof – enthalte die Richtlinie keine Garantien dafür, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauch sowie vor unberechtigtem Zugang geschützt würden, und insbesondere nach Ablauf der Speicherfrist nicht vernichtet würden. Sie schreibe auch nicht vor, dass die Daten im Unionsgebiet zu speichern seien, sodass die Einhaltung der Erfordernisse des Datenschutzes nicht durch eine unabhängige Stelle sichergestellt werden könne. Dies betrifft insbesondere ausländische Anbieter, die ihre Daten in Ländern speichern, deren Geheimdienste den Zugriff auf die Daten durchsetzen können.

In der Schweiz werden Datenschutz und -sicherheit bereits nach geltendem Recht geregelt (Art. 9 VÜPF); der Gesetzesentwurf sieht in Art. 12 eine rudimentäre Regelung auf Gesetzesstufe vor. Eine Vernichtung der Daten ist nicht vorgesehen. Eine entsprechende Verpflichtung der Provider ergibt sich jedoch u.E. bereits aus dem allgemeinen Datenschutzrecht (nach Ablauf der Aufbewahrungsfrist entfällt ein überwiegendes Interesse an der Speicherung nach Art. 13 DSG), eine Regelung wäre jedoch nur schon aus Gründen der Rechtssicherheit zu begrüssen gewesen. Eine Pflicht zur Speicherung auf dem Gebiet der Schweiz ist ebenfalls nicht vorgesehen.

c) Verhältnismässigkeit im engeren Sinn und Fazit

Entgegen der schweizerischen Gerichtspraxis²² verzichtet der EuGH in vorliegenden Entscheid, einer allgemeinen Tendenz folgend²³, auf eine formell gesonderte Prüfung einer Verhältnismässigkeit im engeren Sinn («Angemessenheit»). Die Angemessenheit ist in Art. 5 Abs. 4 Unterabsatz 1 AEUV und Art. 52 Abs. 1 der Charta nicht explizit erwähnt. Der Gerichtshof bringt den Gedanken der Angemessenheit jedoch wie üblich²⁴ implizit in die Prüfung der Eignung und der Notwendigkeit ein.

Abschliessend hält der Gerichtshof fest, aus dem Vorstehenden folge, dass die Richtlinie 2006/24 keine klaren und präzisen Regeln zur Tragweite des Eingriffs in die in Art. 7 und 8 der Charta verankerten Grundrechte vorsehe. Obgleich der Eingriff von grossem Ausmass und besonderer Schwere sei, enthalte die Richtlinie keine Bestimmungen, die eine Beschränkung auf das absolut Notwendige gewährleisten könnten. Aus der Gesamtheit der vorstehenden Erwägungen sei zu schliessen, dass der Unionsgesetzgeber beim Erlass der Richtlinie die Grenzen der Verhältnismässigkeit überschritten habe, womit die Richtlinie ungültig sei.

6. Konsequenzen

Der Gerichtshof zieht den Schluss der Ungültigkeit damit nicht aus einzelnen Mängeln der Richtlinie, sondern aus dem Zusammenspiel einer Vielzahl von zu abstrakt formulierten Normen. Dies lässt den Eindruck aufkommen, es sei möglich, eine neue Richtlinie zu formulieren, die – präziser und konkreter – den vom Gerichtshof gestellten Anforderungen

²¹ Vgl. auch Dienst ÜPF, Verfügung vom 30. Juni 2014 (Fn. 8), Ziff. 27 f.

²² Vgl. etwa BGE 132 I 181; HÄFELIN/HALLER/KELLER (Fn. 15), N 323.

²³ Vgl. V. TRSTENJAK/E. BEYSEN, Das Prinzip der Verhältnismässigkeit in der Unionsrechtsordnung, EuR 3/2012, 265 ff., 269.

²⁴ TRSTENJAK/ERWIN (Fn. 23), 270.

derungen gerecht werden könnte. Entsprechend forderten Vertreter der Europäischen Volkspartei denn auch umgehend einen neuen Kommissionsvorschlag für eine Neuregelung im Einklang mit dem Urteil²⁵.

Dem Vernehmen nach ist die Hoffnung darauf, die Bedenken des Gerichtshofs ausräumen zu können, aufseiten der EU jedoch klein. Die zuständige EU-Kommissarin CECILIA MALMSTRÖM hat jedenfalls vorerst nicht vor, einen weiteren Anlauf zu unternehmen²⁶. Problematisch scheint insbesondere Rz. 59 des Urteils: Der Gerichtshof bemängelt wie bereits ausgeführt, dass kein Zusammenhang zwischen den auf Vorrat gespeicherten Daten und einer Bedrohung der öffentlichen Sicherheit gefordert werde. Insbesondere finde keine Beschränkung statt (i) auf den Zeitraum, das Gebiet und/oder den Personenkreis, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, und (ii) auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten²⁷. Es scheint schwierig, diese Kriterien mit einer anlasslosen Vorratsdatenspeicherung in Einklang zu bringen²⁸.

Auch nach ROSSNAGEL erklärt der EuGH eine anlasslose Vorratsdatenspeicherung grundsätzlich für unzulässig.

Für den EuGH sei die pauschale, unterschiedslose Datenspeicherung unvereinbar mit der gebotenen Beschränkung von Grundrechtseingriffen auf das «absolut Notwendige»²⁹.

Dass in Österreich mit dem kürzlich ergangenen Urteil des Verfassungsgerichtshofs die Vorratsdatenspeicherung ebenfalls verboten wurde, lässt aufhorchen. Denn im Gegensatz zu einer Richtlinie ist nationales Recht bereits weiter ausdifferenziert, sodass der gegen die Richtlinie erhobene Vorwurf der mangelnden Konkretisierung zumindest teilweise nicht mehr gelten kann. Dies hinderte den Österreichischen Verfassungsgerichtshof jedoch nicht daran, die entsprechenden Normen für ungültig zu erklären: Er bemängelte insbesondere die grosse «Streuung» der zu prüfenden Regeln, dass nämlich von den Massnahmen nahezu die gesamte Bevölkerung und damit ein zu breiter Kreis von Daten betroffen und der Deliktskatalog zu weit gefasst sei.

Streuung und Deliktskatalog sind Kritikpunkte, die auch in der Schweiz gegen die Vorratsdatenspeicherung angeführt werden können. Erwartungsgemäss verteidigt der Dienst ÜPF in seiner Verfügung vom 30. Juni 2014 die Verhältnismässigkeit der Vorratsdatenspeicherung denn auch unter Hinweis auf jene Anforderungen des EuGH, die die schweizerische Gesetzgebung bereits erfüllt, namentlich die gesetzliche Beschränkung des Datenzugriffs auf für die Ermittlung notwendigen Fälle, die Voraussetzung eines Entscheids eines Zwangsmassnahmengerichts, die Voraussetzung eines dringenden Verdachts und die gesetzlichen Pflichten der Fernmeldedienstanbieterinnen zur Gewährleistung des Datenschutzes³⁰.

Auf das Problem der Streubreite hinsichtlich der betroffenen Personen und der gesammelten Daten, das sowohl für den EuGH als auch für den Österreichischen Verfassungsgerichtshof zentral war, geht der Dienst ÜPF jedoch nicht ein.

7. Ausblick

Die Urteile des EuGH und des Österreichischen Verfassungsgerichtshofs sind für die Schweiz natürlich nicht bindend, sie lassen jedoch erwarten, dass auch der Europäische Gerichtshof für Menschenrechte (EGMR) die in der Schweiz praktizierte anlasslose Datenspeicherung kritisch sehen wird. Die erwähnten Begehren von Mitgliedern der Digitalen Gesellschaft Schweiz wurden kürzlich durch den Dienst ÜPF zwar abschlägig beantwortet. Nach Aussagen der Digitalen Gesellschaft soll gegen die Verfügung jedoch Beschwerde geführt und die Sache nötigenfalls bis zum EGMR weiter verfolgt werden³¹.

Der schweizerische Gesetzgeber, der derzeit gerade an einer erheblichen Verschärfung der Vorratsdatenspeicherung arbeitet, täte gut daran, die Frage nach der Verfassungsmässigkeit der Vorratsdatenspeicherung noch einmal ganz grundsätzlich zu stellen. Das «Quick-Freeze»-Verfahren gemäss Artikel 16 der Cybercrime-Konvention des Europarats beispielsweise, mit dem Telekommunikations-Verkehrsdaten für Zwecke der Strafverfolgung vorübergehend gesichert werden können, käme den Vorgaben der Menschenrechtskonvention jedenfalls deutlich näher³².

²⁵ S. SCHWEDA, EU: Politische Debatte zur Zukunft der Vorratsdatenspeicherung, MMR-Aktuell 2014, 357671.

²⁶ S. KREMPL/A. WILKENS (anw), Heise Newsticker vom 4. Juni 2014, EU-Kommission unternimmt keinen neuen Anlauf zur Vorratsdatenspeicherung, www.heise.de/newsticker/meldung/EU-Kommission-unternimmt-keinen-neuen-Anlauf-zur-Vorratsdatenspeicherung-2215883.html.

²⁷ Vgl. M. HOLLAND (mho), Heise Newsticker vom 23. Juni 2014, EU-Juristen halten Vorratsdatenspeicherung wohl für abgehakt, www.heise.de/newsticker/meldung/EU-Juristen-halten-Vorratsdatenspeicherung-wohl-fuer-abgehakt-2236498.html.

²⁸ Zweifelnd auch S. SCHWEDA, Vorratsdatenspeicherung in der EU – ja, nein, vielleicht, weiss nicht?, ZD-Aktuell 2014, 04020.

²⁹ A. ROSSNAGEL, Neue Massstäbe für den Datenschutz in Europa – Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung, MMR 2014, 372 ff., 375.

³⁰ Dienst ÜPF, Verfügung vom 30. Juni 2014 (Fn. 8), Ziff. 26 ff.

³¹ J. FLÜCKIGER, Staatstrojaner mit Risiken und Nebenwirkungen, NZZ online, 2. Juli 2014 (Kasten), www.nzz.ch/schweiz/staatstrojaner-mit-risiken-und-nebenwirkungen-1.18334794.

³² So auch SCHWEDA (Fn. 28).