



Seminararbeit zum Thema:

Neue Entwicklungen im Datenschutz

Verfasser: Johannes Pogoda
Seminar: S 205 Digitalisierung in Staat und Verwaltung
Dozent: Univ.-Prof. Dr. Hermann Hill
Semester: Wintersemester 2014/15

Speyer, 18. Januar 2015

Inhaltsverzeichnis

1	Einleitung: eine Chronologie der Ereignisse des Jahres 2014..	1
2	Der europäische Datenschutzrahmen.....	3
2.1	Datenschutz-Grundverordnung.....	4
2.1.1	Wirksame Kontrolle der personenbezogenen Daten.....	5
2.1.2	Höhere Datensicherheit.....	6
2.1.3	Stärkung des digitalen Binnenmarkts.....	6
2.1.4	Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen.....	7
2.1.5	Rechtssetzungsbefugnisse der Kommission.....	8
2.2	Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.....	9
2.3	Zwischenfazit.....	10
3	EuGH-Urteil zur Vorratsdatenspeicherungsrichtlinie.....	11
3.1	Rechtliche Folgen des Urteils.....	14
3.2	Reaktionen auf das Urteil.....	14
3.3	Eigene Bewertung.....	16
4	Fazit.....	17
5	Literaturverzeichnis.....	18

1 Einleitung: eine Chronologie der Ereignisse des Jahres 2014

Für den Datenschutz war das Jahr 2014 ein aufregendes Jahr. Nach Jahren des Stillstands hat die Debatte auf europäischer und damit auch auf Ebene der EU-Mitgliedstaaten wieder an Fahrt aufgenommen. Institutionelle Katalysatoren dieser Beschleunigung waren im zurückliegenden Jahr das Europäische Parlament und der Europäische Gerichtshof.¹

Das Europäische Parlament äußerte sich am 12. März 2014 umfassend zum Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)² und zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr³. Beide Vorschläge stammen bereits vom 25. Januar 2012.

Der Europäische Gerichtshof sorgte am 8. April 2014 für Aufsehen mit seinem Urteil zur Vorratsdatenspeicherungsrichtlinie⁴, indem er diese wegen Verstoßes gegen das Grundrecht auf Achtung des Privat- und Familienlebens (Art. 7 GRCh) und des Grundrechts auf Schutz personenbezogener Daten (Art. 8 GRCh) für nichtig erklärte.⁵ Vermeintliche Kenner der Rechtsprechung des Bundesverfassungsgerichts fühlten sich an dessen Entscheidung zur Vorratsdatenspeicherung vom 2. März 2010⁶ erinnert. Mag das Urteil aus deutscher Sicht auf den ersten Blick vielleicht keine wesentlichen Neuerungen begründen,⁷ so muss man sich

¹ Vgl. Wolff, DÖV 2014, 608 (608, 612).

² Legislative Entschließung des Europäischen Parlaments zu KOM (2012) 11: A7-0402/2013.

³ Legislative Entschließung des Europäischen Parlaments zu KOM (2012) 10: A7-0403/2013.

⁴ Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

⁵ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.).

⁶ BVerfG, Urt. v. 2.3.10 - 1 BvR 256, 263, 586/08, BeckRS 2010, 46771.

⁷ Siehe hierzu auch Wolff, DÖV 2014, 608 (608).

doch vergegenwärtigen, dass Deutschland bereits über einen der höchsten Datenschutzstandards der EU verfügt und mit dem Urteil des Gerichtshofs der Großteil der EU-Staaten nunmehr kräftig an Fahrt aufnehmen muss, um den Anforderungen des Urteils gerecht zu werden.

Knapp einen Monat später folgte das nächste „wegweisende“⁸ Urteil des EuGH. Dieser verpflichtete Suchmaschinenbetreiber, aus ihren Resultaten jene Suchergebnisse zu entfernen, auf deren Löschung der Betroffene einen Anspruch hat.⁹ Nach Ansicht des Gerichtshofs überwiegen die Grundrechte des Betroffenen (Art. 7 und Art. 8 EU-GRCh) regelmäßig gegenüber den wirtschaftlichen Interessen der Betreiber und dem Informationsinteresse der Öffentlichkeit; sollte die Abwägung aus besonderen Gründen zu einem anderen Ergebnis führen, so bestünde auch keine Löschungspflicht seitens des Suchmaschinenbetreibers.¹⁰ Da die inhärente Kritik des EuGH von der Europäischen Kommission weitestgehend bereits in den beiden oben genannten Legislativakten in vorauseilendem Gehorsam berücksichtigt wurde, soll auf eine detaillierte Besprechung dieses Urteils nachfolgend verzichtet werden.¹¹

Nach den Stellungnahmen des Europäischen Parlaments und den Urteilen des EuGH lag der Ball wieder im Spielfeld der Kommission. Die Antwort der Kommission ließ nicht lange auf sich warten und so bezog sie am 10. Juni 2014 umfassend Stellung.¹² Ein Gesetzgebungsorgan hält sich weiterhin bedeckt, gerät jedoch zusehends in Zugzwang¹³, nachdem die anderen Beteiligten ihre Arbeit vorerst abgeschlossen haben: der Rat.

In Anbetracht des Umfangs sämtlicher der eben genannten Dokumente können im Folgenden die wesentlichen Aussagen und etwaigen Diskussionen nur skizziert werden.

⁸ Nolte, NJW 2014, 2238 (2238).

⁹ EuGH, Urt. v. 13.5.14, Rs. C-131/12, Urteilstenor Rn. 3.

¹⁰ EuGH, Urt. v. 13.5.14, Rs. C-131/12, Urteilstenor Rn. 4.

¹¹ Ausführliche Besprechungen finden sich u. a. bei Nolte, NJW 2014, 2238 (2238 ff.); Jandt, MMR-aktuell 2014, 358242; Boehme-Neßler, NVwZ 2014, 825 (825 ff.).

¹² Europäische Kommission, SP (2014) 455 - abrufbar unter <http://www.europarl.europa.eu/oeil/spdoc.do?i=23714&j=0&l=en> bzw. <http://www.europarl.europa.eu/oeil/spdoc.do?i=23715&j=0&l=en> - letzter Abruf jeweils: 18.1.15 15.01 Uhr.

¹³ So die Aussage von Dr. Lotte Madlen Tittor, Europäisches Parlament, Generaldirektion Kommunikation, am 13.1.14 bei der Exkursion im Rahmen des Kolloquiums „Parlamentarismus im Mehrebenensystem“.

2 Der europäische Datenschutzrahmen¹⁴

Die EU besitzt seit dem Vertrag von Lissabon das weitgehend alleinige Recht zur Regelung des Datenschutzes in der EU.¹⁵ Von diesem Recht macht sie mit den Vorschlägen vom 25. Januar 2012 umfassend Gebrauch. Ziel der Kommission ist die weitere Harmonisierung bis hin zu einer vollständigen Vereinheitlichung des Datenschutzrechts, um dessen einheitliche Anwendung und Auslegung in der EU gewährleisten zu können.¹⁶

Alle Gesetzgebungsorgane der EU müssen sich hierbei mit einer der besonderen Schwierigkeiten des Datenschutzes auseinandersetzen, der Vielzahl gegenläufiger Interessen, die nicht selten Verfassungsrang haben und deren Ausgleich sich daher oftmals als sehr diffizile Angelegenheit herausstellt. So gilt es u. a. das Grundrecht des Einzelnen auf Schutz seiner personenbezogenen Daten (Art. 8 EU-GRCh), das Grundrecht auf Sicherheit (Art. 6 EU-GRCh) und die wirtschaftlichen Interessen von Unternehmen (Art. 16 EU-GRCh) miteinander abzuwägen.¹⁷ Nicht allen Interessen wird man in vollem Umfang gerecht werden können. Die Europäische Kommission versucht jedoch in ihren Veröffentlichungen ein anderes Bild zu zeichnen: das Bild von einem Rechtsakt, der alle Interessen nicht nur wahrt, sondern stärkt. So soll jeder seine persönlichen Informationen wirksam kontrollieren, die Wirtschaft durch mehr Vertrauen der Verbraucher ihre Umsätze steigern und durch die Rechtsvereinheitlichung ihre Kosten senken können.¹⁸ Inwiefern Anspruch und Wirklichkeit hierbei übereinstimmen, wird sogleich zu erörtern sein.

Unabhängig von den einzelnen Regelungen hat sich die Europäische Kommission für einen zweigeteilten Datenschutzrahmen entschieden: eine Verordnung und eine Richtlinie. Diese Rechtsakte gleichen sich jedoch in vielen Bereichen. Eine wesentliche Gemeinsamkeit beider besteht darin, dass sie keine Anwendung auf die

¹⁴ In Anlehnung an die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM (2012) 9.

¹⁵ Siehe Art. 16 Abs. 2 AEUV.

¹⁶ KOM (2012) 9, S. 4.

¹⁷ Vgl. KOM (2012) 11, S. 7.

¹⁸ KOM (2012) 9, S. 2, 4; KOM (2012) 11, S. 1 f.

Organe, Einrichtungen und sonstigen Stellen der EU finden sollen.¹⁹ Dies steht im Widerspruch zu der Feststellung der Europäischen Kommission von 2010, wonach es eines Gesamtkonzeptes für den Datenschutz in der EU bedürfe,²⁰ und stößt auf die Kritik des Europäischen Parlaments²¹. Es wäre im Sinne einer Vereinheitlichung, wenn alle datenverarbeitenden Stellen dem gleichen Recht unterworfen wären, anstatt hiervon die EU auszunehmen.

Ein weiterer Streitpunkt, der ebenfalls beide Gesetzgebungsverfahren betrifft, besteht hinsichtlich des Erhalts nationaler Regelungen, die ein höheres Schutzniveau vorsehen als die EU.²² Bei einer Richtlinie mag dies weniger ins Gewicht fallen, weil die zur Umsetzung der Richtlinie erlassenen Regelungen der Mitgliedstaaten häufig ohnehin Unterschiede aufweisen werden. Die Verordnung wird jedoch in allen Mitgliedstaaten unmittelbar anwendbar sein und dient gerade der Vereinheitlichung des Datenschutzrechts; es liefe diesem Ziel zuwider, gestattete man einzelnen Mitgliedstaaten ihr höheres Datenschutzniveau beizubehalten. Gleichwohl dürfte der europäische Gesetzgeber kein Interesse daran haben, dass er für die Absenkung des Datenschutzniveaus in einigen Mitgliedstaaten verantwortlich gemacht wird.

2.1 Datenschutz-Grundverordnung

Mit der Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) werden verschiedene Ziele verfolgt - wie diese erreicht werden sollen und welche Kritik an den bestehenden Vorschlägen geübt wird, ist Gegenstand dieses Abschnitts.

¹⁹ KOM (2012) 10, Art. 2 Abs. 3 lit. b, siehe auch S. 7; KOM (2012) 11, Art. 2 Abs. 2 lit. b.

²⁰ KOM (2012) 10, S. 2.

²¹ Europäisches Parlament, P7_TA(2014)0219, Abänderung 60.

²² Europäisches Parlament, P7_TA(2014)0219, Abänderung 59; vgl. auch die Forderung des Bundesinnenministers, siehe Reimer, DuD 2014, 639.

2.1.1 Wirksame Kontrolle der personenbezogenen Daten

Die Kommission möchte die Rechte der Betroffenen stärken und sie befähigen, ihre Rechte besser wahrnehmen zu können. Deswegen sollen Betroffene wissen, wer über welche ihrer Daten verfügt und wozu er diese verwendet.²³

Dies soll im Einzelnen durch folgende Veränderungen erreicht werden. Eine Datenverarbeitung bedarf grundsätzlich der ausdrücklichen Einwilligung des Betroffenen (Abkehr von der sog. Widerspruchslösung) und ihr kann im Nachhinein jederzeit widersprochen werden.²⁴ Die datenverarbeitenden Stellen werden zur Transparenz verpflichtet und müssen die Erfassung und Verarbeitung personenbezogener Daten auf ein Mindestmaß beschränken.²⁵ Sie werden zudem zur Berichtigung bzw. Löschung verpflichtet, sofern die betroffene Person dies begehrt und der Löschung keine berechtigten Gründe entgegenstehen.²⁶ Die Betroffenen erhalten außerdem das Recht auf Auskunft über die von ihnen gesammelten Daten²⁷ sowie ein umfassendes Beschwerderecht²⁸. Weiterhin soll dem sog. Profiling grundsätzlich ein Ende bereitet werden.²⁹

Da die Rechte der Betroffenen über die Verordnung verteilt sind, möchte das Europäische Parlament im Interesse der Verbraucher einen Artikel mit den allgemeinen Grundsätzen hinsichtlich der Rechte der Betroffenen in die Verordnung einfügen.³⁰

Wie bereits eingangs erwähnt, erfolgt eine Stärkung der Rechte der Verbraucher meist auf Kosten der Unternehmen. Dementsprechend kritisiert der Bundesverband der Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) u. a. die strengeren Anforderungen an die Einwilligung.³¹

²³ KOM (2012) 9, S. 6.

²⁴ KOM (2012) 9, S. 6; siehe hierzu, aber auch zu den vorgesehenen Ausnahmen KOM (2012) 11, Art. 6 f., zum Widerspruchsrecht siehe Art. 19.

²⁵ KOM (2012) 9, S. 5; KOM (2012) 11, S. 8, Art. 5 lit. a, c-e, Art. 11.

²⁶ KOM (2012) 9, S. 5 f.; KOM (2012) 11, Art. 16 f.

²⁷ KOM (2012) 9, S. 6; KOM (2012) 11, Art. 15.

²⁸ KOM (2012) 11, Art. 73 ff.

²⁹ Siehe hierzu, aber auch zu den geplanten Ausnahmen KOM (2012) 11, Art. 20.

³⁰ Philipp, EuZW 2014, 283.

³¹ ZD-Aktuell 2013, 03410; ZD-Aktuell 2013, 03418.

2.1.2 Höhere Datensicherheit

Der Schutz der Daten soll dadurch gestärkt werden, dass die Unternehmen zur Verbesserung ihrer IT-Sicherheitsmaßnahmen und zur Meldung von erfolgreichen Angriffen auf ihre Systeme verpflichtet werden.³² Die Kommission beabsichtigt diesbezüglich auch die Förderung von Technologien, die die Verarbeitung personenbezogener Daten auf ein Minimum reduzieren (Privacy by Design).³³ An diesem Beispiel wird deutlich, dass die Interessen der Betroffenen und jene der Unternehmen keineswegs immer kompatibel sind. Die eben genannte Verpflichtung dient dem Datenschutz, bedeutet aber für die Unternehmen zusätzliche Kosten.

2.1.3 Stärkung des digitalen Binnenmarkts

Die derzeit bestehenden, unterschiedlichen nationalen Regelungen bedeuten höhere Kosten für die Unternehmen, da sie ihre Leistung für den jeweiligen Mitgliedstaat entsprechend anpassen müssen. Dies kann dazu führen, dass Unternehmen ihre Leistung nicht in allen Mitgliedstaaten anbieten und der europäische Binnenmarkt daher nur eingeschränkt funktioniert.³⁴ Um dem entgegenzutreten, soll nicht nur das Datenschutzrecht EU-weit vereinheitlicht werden, sondern auch die Überwachung von dessen Einhaltung seitens der Unternehmen nur noch der Datenschutzbehörde eines Mitgliedstaates obliegen. Zuständig soll die Behörde sein, in dessen Staat das jeweilige Unternehmen seinen Sitz hat.³⁵

Bezug nehmend auf die obigen Ausführungen sei kurz erwähnt, dass die Beibehaltung höherer nationaler Datenschutzstandards diesem Ziel zuwiderliefe.

Unabhängig davon, muss befürchtet werden, dass in Anbetracht der wirtschaftlichen Bedeutung der Digitalwirtschaft in der gesamten EU, aber auch für die einzelnen Mitgliedstaaten trotz einheitlichen Rechts die Durchsetzung des Rechts uneinheitlich bleibt. Exemplarisch sei hier Irland genannt, in dem sich der Hauptsitz vieler Branchenprimusse befindet.³⁶ Das irische „Geschäftsmodell“ bestand bisher darin, das Datenschutzniveau niedrig zu halten, um im Gegenzug von den

³² KOM (2012) 9, S. 5 f., 7; KOM (2012) 11, Art. 30 ff.

³³ KOM (2012) 9, S. 7; KOM (2012) 11, Art. 23.

³⁴ KOM (2012) 9, S. 7.

³⁵ KOM (2012) 9, S. 8 f., 12.; KOM (2012) 11, S. 14, Art. 51.

³⁶ <http://www.tagesspiegel.de/wirtschaft/unternehmensstandort-irland-die-angst-geht-um-im-steuerparadies/10766838.html> - letzter Abruf: 18.1.15 17.04 Uhr.

Steuereinnahmen zu profitieren.³⁷ Der irische Datenschutzbeauftragte klagt bereits jetzt, dass es ihm an den nötigen Mitteln fehle, um die Einhaltung des irischen Datenschutzrechts zu überprüfen.³⁸ Es darf bezweifelt werden, dass er nach Inkrafttreten der Datenschutz-Grundverordnung mehr Rückendeckung seitens der irischen Politik erfahren wird. Ähnlich könnte es anderen kleineren Mitgliedstaaten ergehen, denen es schlicht an den Ressourcen fehlt, um große Unternehmen effektiv überwachen zu können. Damit könnte die Reform im Ergebnis zu einer veränderten Rechts-, nicht aber zu einer veränderten Sachlage führen. Ähnlich sah dies auch das Europäische Parlament. Wenn es nach dessen Willen ginge, würde die Verordnung um eine Regelung ergänzt, welche die Mitgliedstaaten zu einer hinreichenden Ausstattung der Behörden verpflichtet, um die wirksame Wahrnehmung der Aufgaben sicherzustellen.³⁹

2.1.4 Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

Mit der zunehmenden Globalisierung unserer Wirtschaft steigt auch der Umfang der Daten, die von einem Staat in einen anderen übermittelt werden. Gleichwohl die Vereinheitlichung des Datenschutzrechts innerhalb der EU ein Schritt in die richtige Richtung bedeutet, können so nicht alle bestehenden Probleme gelöst werden. Vielmehr bedarf es internationaler Standards, um diesen zu begegnen.⁴⁰ Die Europäische Kommission beabsichtigt ihrerseits, die Weitergabe personenbezogener Daten in Drittländer oder an internationale Organisationen zu „überwachen“. So sollen personenbezogene Daten grundsätzlich nur dann an diese übermittelt werden, sofern die Europäische Kommission einen sog. Angemessenheitsbeschluss erlassen hat. Entscheidend für dessen Erlass ist das Datenschutzniveau im jeweiligen Land, insbesondere dessen Rechtsstaatlichkeit sowie die Existenz gerichtlichen Rechtsschutzes und von mindestens einer unabhängigen Aufsichtsbehörde.⁴¹

³⁷ Vgl. <http://www.golem.de/1109/86766.html> - letzter Abruf: 18.1.15 17.04 Uhr.

³⁸ http://www.deutschlandradiokultur.de/google-facebook-co-europas-zahnloser-datenschutz.1162.de.html?dram:article_id=281318 - letzter Abruf: 18.1.15 17.04 Uhr.

³⁹ Europäisches Parlament, A7-0402/2013, S. 238.

⁴⁰ So auch Gola/Klug, NJW 2014, 667 (671). ⁴⁰ Dass die EU dieses Problem erkannt hat, zeigt nicht zuletzt KOM (2012) 11, Art. 45.

⁴¹ KOM (2012) 11, S. 12 f., Art. 40 ff.

2.1.5 Rechtssetzungsbefugnisse der Kommission

Der Vorschlag der Europäischen Kommission enthält derzeit über 27 Ermächtigungsgrundlagen⁴² zu ihren Gunsten, was auf verhältnismäßig scharfe Kritik seitens des Europäischen Parlaments stieß, da dies weder der Rechtssicherheit noch der Rechtsklarheit diene.⁴³ Das Europäische Parlament schlägt daher vor, entweder jene Regelungen, die durch einen Rechtsakt der Europäischen Kommission präzisiert werden sollten, in die Verordnung aufzunehmen oder dem Europäischen Datenschutzausschuss die Zuständigkeit für den Erlass der fraglichen Rechtsakte zu übertragen. Letzteres wird mit der größeren Sachnähe des Ausschusses begründet. Dabei sollte aber auch die Intention des Grundrechts auf den Schutz personenbezogener Daten (Art. 8 EU-GRCh) im Auge behalten werden. Dieses ist in erster Linie ein Abwehrrecht des Bürgers gegenüber dem Staat - die bestehende Schutzpflicht des Staates hinsichtlich der Verarbeitung personenbezogener Daten durch Private ist insofern eher zweitrangig. Es liefe der Konzeption dieses Grundrechts zuwider, wenn man den Datenschutz weitestgehend zur Disposition der Europäischen Kommission stelle.

Während sich die Europäische Kommission mit einer Vielzahl der Abänderungen des Europäischen Parlaments - teils zwar mit Einschränkungen - einverstanden erklärte, widerspricht sie in diesem Punkt dem Europäischen Parlament vehement.⁴⁴ Es zeichnet sich jedoch ab, dass das Europäische Parlament in dieser Frage zugunsten anderer einlenken wird.⁴⁵

⁴² Siehe hierzu die Aufzählung in KOM (2012) 11, Art. 86 Abs. 2; vgl. auch Art. 21, 62.

⁴³ Europäisches Parlament, A7-0402/2013, S. 235, 240.

⁴⁴ SP (2014) 455-0.

⁴⁵ Der zuständige Berichterstatter des Europäischen Parlaments, Albrecht, machte am 13.1.14 bei einer Diskussion im Rahmen der Exkursion des Kolloquiums „Parlamentarismus im Mehrebenensystem“ deutlich, dass er die Argumente der Europäischen Kommission gut nachvollziehen könne. So seien Gesetze bereits am Tage ihres Inkrafttretens veraltet, was gerade in Anbetracht des raschen technischen Fortschritts eine äußerst missliche Situation für den Datenschutz sei.

2.2 Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

Die soeben skizzierte Datenschutz-Grundverordnung findet ausdrücklich keine Anwendung auf die Verarbeitung personenbezogener Daten zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden.⁴⁶ Um jedoch den grenzübergreifenden Informationsaustausch der Polizei- und Justizbehörden zu vereinfachen und somit die Kriminalität besser bekämpfen zu können, sollen auch in diesem Bereich die nationalen Vorschriften harmonisiert werden.⁴⁷ Der hierfür üblicherweise gewählte Rechtsakt ist die Richtlinie, welche gemäß Art. 288 Abs. 3 AEUV nur hinsichtlich ihres Zieles verbindlich ist, während die Wahl der Form und der Mittel den Mitgliedstaaten überlassen ist.

Ziele dieser Richtlinie sind einerseits die Statuierung allgemeiner Datenschutzgrundsätze⁴⁸ und andererseits die Harmonisierung der Beschränkungsmöglichkeiten.⁴⁹ Letzteres betrifft insbesondere die Rechte der Betroffenen,⁵⁰ über die Erhebung oder Verarbeitung ihrer Daten durch die Behörden der Polizei und der Justiz informiert zu werden, und die nach dem jeweiligen Status (z. B. Zeuge, Opfer, Verdächtiger, verurteilter Straftäter)⁵¹ vorzunehmende Differenzierung.⁵² Insgesamt soll die Richtlinie „ein hohes, einheitliches Datenschutzniveau in diesem Bereich [...] garantieren“⁵³. Der Berichterstatter im Europäischen Parlament zu diesem Gesetzgebungsverfahren, Droutsas, plädiert ebenfalls für letztgenanntes Ziel,⁵⁴ vertritt jedoch die Auffassung, dass „die vorgeschlagene Richtlinie in vielerlei Hinsicht den Anforderungen eines hohen Datenschutzniveaus nicht gerecht

⁴⁶ KOM (2012) 11, Art. 2 Abs. 2 lit. e.

⁴⁷ KOM (2012) 9, S. 10, vgl. auch KOM (2012) 10, S. 2, 5.

⁴⁸ Siehe KOM (2012) 10, Art. 4.

⁴⁹ KOM (2012) 9, S. 11.

⁵⁰ Umfassend hierzu KOM (2012) 10, Kap. III (Art. 10 ff.).

⁵¹ Siehe i. E. hierzu KOM (2012) 10, Art. 5.

⁵² KOM (2012) 9, S. 11.

⁵³ KOM (2012) 10, S. 5

⁵⁴ Europäisches Parlament, A7-0403/2013, S. 125.

[werde]⁵⁵. Es werde beispielsweise nicht überprüft, ob die Erfassung und Verarbeitung des jeweiligen Datums überhaupt notwendig und verhältnismäßig ist und welchem Ziel dies dienen soll.⁵⁶

Das Problem der Globalisierung stellt sich auch im Bereich der polizeilichen und justiziellen Zusammenarbeit. Auf der einen Seite machen Kriminalität und Terror nicht an Staatsgrenzen halt, auf der anderen Seite machen zumindest einige Staaten nicht an ihren Staatsgrenzen halt, wenn es um die Bekämpfung von Kriminalität und Terror geht. Dies wurde nicht zuletzt durch die sog. NSA-Affäre deutlich. Die Richtlinie versucht jedoch nur, eine Antwort auf die erste Frage zu geben. So dürfen Daten in Drittländer oder an internationale Organisationen nur übermittelt werden, sofern „dies für die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten oder für die Strafverfolgung notwendig ist“⁵⁷ - vorausgesetzt, es liegt für das jeweilige Land, respektive die jeweilige Organisation ein Angemessenheitsbeschluss der Europäischen Kommission vor oder es bestehen hinreichende Garantien, die einen angemessenen Schutz der Daten gewährleisten.⁵⁸

Droutsas bemängelt auch hier den zu geringen Schutz der Daten der Betroffenen. „So würde beispielsweise der Vorschlag der Kommission die Weitergabe von Daten an die Behörden eines Drittlandes oder internationale Organisationen, die nicht für die Strafverfolgung zuständig sind, ermöglichen.“⁵⁹

2.3 Zwischenfazit

Unabhängig von bestehenden Meinungsverschiedenheiten zu einzelnen Punkten besteht Einigkeit⁶⁰ darüber, dass eine weitere Harmonisierung des Datenschutzrechts zu einer Anhebung des Datenschutzniveaus in der EU führen wird.⁶¹ Es bleibt daher zu hoffen, dass sich alle Beteiligten nun um eine rasche Beendigung

⁵⁵ Europäisches Parlament, A7-0403/2013, S. 128.

⁵⁶ Europäisches Parlament, A7-0403/2013, S. 126 f.; siehe auch Europäisches Parlament, P7_TA(2014)0219, Abänderung 62.

⁵⁷ KOM (2012) 10, S. 11, Art. 33.

⁵⁸ KOM (2012) 10, S. 11, Art. 34.

⁵⁹ Europäisches Parlament, A7-0403/2013, S. 127.

⁶⁰ Siehe bspw. ZD-Aktuell 2013, 03441.

⁶¹ Vgl. auch Eckhardt, CR 2012, 195 (203), der dies jedoch für Deutschland aufgrund des schon bestehenden, hohen Datenschutzniveaus bezweifelt.

des Gesetzgebungsverfahrens bemühen⁶² - immerhin war die Verabschiedung bereits für Ende 2012 geplant⁶³.

3 EuGH-Urteil zur Vorratsdatenspeicherungsrichtlinie⁶⁴

Der irische High Court und der österreichische Verfassungsgerichtshof hatten dem EuGH im Jahr 2012 verschiedene Fragen hinsichtlich der Gültigkeit und der Auslegung der Richtlinie über die Vorratsdatenspeicherung vorgelegt.⁶⁵ In seinem Urteil stellt der Gerichtshof die Unvereinbarkeit der Richtlinie mit dem Grundrecht auf Achtung des Privat- und Familienlebens (Art. 7 EU-GRCh) und dem Grundrecht auf Schutz personenbezogener Daten (Art. 8 EU-GRCh) und infolgedessen die Ungültigkeit der Richtlinie fest, ohne dem Unionsgesetzgeber die Möglichkeit einzuräumen, innerhalb einer angemessenen Frist die Vorratsdatenspeicherung neu zu regeln.⁶⁶

Der EuGH bejaht zunächst den Eingriff der Richtlinie in den Schutzbereich der beiden eben genannten Grundrechte.⁶⁷ Dieser Eingriff wiege besonders schwer, da die Speicherung der Daten anlasslos erfolge, die Betroffenen hierüber keine Information erhielten,⁶⁸ und, weil sich aus der Gesamtschau der gespeicherten Daten detaillierte Personenprofile ergäben.⁶⁹ Hinzu käme die Betroffenheit nahezu aller Unionsbürgerinnen und -bürger.⁷⁰

Diese Eingriffe könnten jedoch trotz ihrer besonderen Schwere gerechtfertigt sein. Hierzu führt der Gerichtshof allgemein aus: „Nach Art. 52 Abs. 1 der Charta muss jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und

⁶² Eine entsprechende Roadmap wurde bereits im Oktober 2013 verabschiedet, siehe hierzu Reimer, DuD 2014, 639.

⁶³ KOM (2012) 9, a. E.

⁶⁴ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.).

⁶⁵ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 17 ff.

⁶⁶ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 69 und a. E.; interessant hierzu und m. w. N. Schweda, ZD-Aktuell 2014, 04020.

⁶⁷ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 29 f., 33 ff. Der Gerichtshof stellt zwar ebenfalls einen Eingriff in den Schutzbereich der Meinungsfreiheit fest, sieht jedoch infolge des bereits festgestellten Verstoßes gegen Art. 7 und Art. 8 EU-GRCh von dessen Rechtfertigungsprüfung ab, siehe hierzu Rn. 26 ff., 70.

⁶⁸ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 37, 56 ff.

⁶⁹ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 27.

⁷⁰ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 56.

Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten⁷¹. Beide Voraussetzungen liegen nach Ansicht des EuGH vor, so sei insbesondere der Kernbereich des Grundrechts auf Achtung des Privat- und Familienlebens (Art. 7 EU-GRCh) nicht verletzt, da die Kenntnisnahme des Kommunikationsinhalts nicht gestattet sei.⁷²

Das entscheidende Kriterium bei der Rechtfertigung von Eingriffen in eine Gewährleistung der EU-GRCh stellt ebenso wie im nationalen Recht der Grundsatz der Verhältnismäßigkeit dar.⁷³ Der EuGH definiert diesen in ständiger Rechtsprechung wie folgt: „[D]er Grundsatz der Verhältnismäßigkeit [...] verlangt, dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenze dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist“⁷⁴. Gleichwohl diese Prüfung teilweise nur eingeschränkt erfolgt, stellt der EuGH für die Vorratsdatenspeicherungsrichtlinie fest, dass diese in Anbetracht ihrer Eingriffsintensität und des an eine Schutzbereichsverstärkung erinnernden Zusammenspiels der von Art. 7 und Art. 8 EU-GRCh gewährleisteten Grundrechte einer „strikten Kontrolle“ unterläge.⁷⁵

Zulässigerweise verfolgt werden, dürfen nur solche Ziele, die entweder einem von der Union anerkannten, dem Gemeinwohl dienenden Ziel oder dem Schutz der Rechte und Freiheiten anderer dienen.⁷⁶ Der Gerichtshof erkennt die Bekämpfung schwerer Kriminalität und des Terrorismus in ständiger Rechtsprechung als ein dem unionalen Gemeinwohl dienendes Ziel an und verweist in diesem Zusammenhang auf das in Art. 6 EU-GRCh verbürgte Recht auf Sicherheit.⁷⁷ Die Vorratsdatenspeicherung sei zudem als Mittel geeignet, da diese zur Strafverfolgung beitragen könne, indem sie den zuständigen Behörden zusätzliche Möglichkeiten

⁷¹ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 38.

⁷² EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 39 f.

⁷³ Zu den Gemeinsamkeiten und Unterschieden in der Auslegung dieses Grundsatzes Wolff, DÖV 2014, 608 (611), vgl. auch Kühling, NVwZ 2014, 681 (682).

⁷⁴ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 46 m. w. N.

⁷⁵ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 47 ff.

⁷⁶ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 38.

⁷⁷ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 41 f. m. w. N.; siehe hierzu auch die Anmerkung von Wolff, DÖV 2014, 608 (611 f.).

zur Aufklärung von Straftaten einräume, wobei deren Bedeutung in Anbetracht der stetig steigenden Nutzung elektronischer Kommunikationsmittel zunähme.⁷⁸

Der Gerichtshof verneint jedoch im Folgenden die Erforderlichkeit der Vorratsdatenspeicherung aus mehreren Gründen.⁷⁹ Hervorgehoben werden muss, dass der EuGH eine Vorratsdatenspeicherung nicht kategorisch ausschließt, vielmehr betont er in seinem Urteil, dass nur eine „Speicherungsmaßnahme - wie sie die Richtlinie [...] vorsieht“⁸⁰ nicht erforderlich ist. Bei der Überarbeitung der Richtlinie sollte sich der europäische Gesetzgeber dementsprechend an den Ausführungen des Gerichtshofs orientieren. Demnach gebieten Art. 7 und Art. 8 EU-GRCh eine Beschränkung auf das absolut Notwendige.⁸¹ Wer jedoch alle Verbindungsdaten elektronischer Kommunikationsmittel nahezu der gesamten EU-Bevölkerung für mindestens sechs Monate auf Vorrat speichere, ohne einen konkreten Anlass oder eine irgendwie geartete Verbindung zu einer Straftat zu fordern, beschränke sich nicht auf das absolut Notwendige, so der EuGH.⁸²

Es bedarf ferner klarer und präziser Regeln bezüglich des Anwendungsbereichs und der Reichweite der Vorratsdatenspeicherung; zudem müssen Mindestanforderungen normiert werden, die personenbezogene Daten wirksam vor Missbrauchsrisiken schützen und den unberechtigten Zugriff oder Gebrauch verhindern.⁸³ Dem genügt die bisherige Richtlinie nach Ansicht des EuGH nicht.⁸⁴ So fehle es u. a. an entsprechenden Regelungen, die sicherstellten, dass die Daten nur entsprechend dem Ziel der Richtlinie, der Bekämpfung schwerer Kriminalität, eingesetzt werden, und eines Gerichts oder einer anderen unabhängigen Instanz, das über den Zugang zu den Daten anhand festgelegter Kriterien entscheidet.⁸⁵

⁷⁸ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 43 f., 49.

⁷⁹ Umfassende Darstellung und Analyse der einzelnen Gründe bei Kühling, NVwZ 2014, 681 (682 f.).

⁸⁰ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 51.

⁸¹ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 52.

⁸² EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 56 ff., 63.

⁸³ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 54.

⁸⁴ EuGH, Urt. v. 8.4.14, Rs. C-293/12 u. C-594/12 (Digital Rights Ireland u. Seitlinger u. a.), Rn. 60 ff.

⁸⁵ Siehe Fn. 84.

3.1 Rechtliche Folgen des Urteils

Durch das Urteil wird die Richtlinie ex tunc ungültig. Damit entfällt die Pflicht der Mitgliedstaaten zur Umsetzung der Richtlinie. Jenen nationalen Regelungen, die zur Umsetzung der Richtlinie ergingen, mangelt es nur auf den ersten Blick an einer Rechtsgrundlage, denn die Mitgliedstaaten können diese Regelungen auch auf Art. 15 Abs. 1 S. 3 der Datenschutzrichtlinie⁸⁶ stützen.⁸⁷ Allerdings fordert bereits die Norm selbst die Beachtung der Grundrechte der Union. So bleiben die Normen zwar bestehen, jedoch können sie ebenfalls auf ihre Vereinbarkeit mit der EU-GRCh hin überprüft werden.⁸⁸ Die Mitgliedstaaten sind unabhängig von einer etwaigen gerichtlichen Überprüfung dazu angehalten, ihre Gesetze entsprechend den Vorgaben des EuGH anzupassen.⁸⁹ Es steht ihnen aber infolge des Urteils ebenso frei, bereits erlassene Regelungen aufzuheben.

3.2 Reaktionen auf das Urteil

Die Europäische Kommission hat infolge des Urteils das Vertragsverletzungsverfahren gegen Deutschland wegen der Nichtumsetzung der Richtlinie eingestellt und angekündigt, Schweden, das 2013 vom EuGH wegen der Nichtumsetzung der Richtlinie zu einem Bußgeld verurteilt wurde, das Bußgeld zurückzuzahlen.⁹⁰ Ob es zu einer Neuregelung käme, ließ die damalige EU-Innenkommissarin Malmström offen; dies habe die nächste Kommission zu entscheiden.⁹¹ Sie betont jedoch in diesem Zusammenhang die Notwendigkeit der zügigen Verabschiedung der Datenschutzreform, insbesondere der Richtlinie zum Datenschutz bei der Strafverfolgung.⁹² Die Sozialisten und Demokraten schlossen sich dieser Forderung an und stellen den Sinn der Vorratsdatenspeicherung generell infrage - anders die Europäische Volkspartei, die eine rasche Neuregelung der Vorratsdatenspeicherung fordert, denn auch das von Art. 6 EU-GRCh verbürgte Recht auf Si-

⁸⁶ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

⁸⁷ Priebe, EuZW 2014, 456 (458); Schweda, ZD-Aktuell 2014, 04020.

⁸⁸ Schweda, ZD-Aktuell 2014, 04020.

⁸⁹ Vgl. Kahl, in: Calliess/Ruffert: EUV/AEUV, Art. 4 EUV, Rn. 54; vgl. auch Kingreen, in: Calliess/Ruffert: EUV/AEUV, Art. 51 EU-GRCh, Rn. 7 f.

⁹⁰ Schweda, MMR-Aktuell 2014, 357671; siehe auch Streinz, JuS 2014, 758 (760).

⁹¹ Schweda, MMR-Aktuell 2014, 357671.

⁹² Siehe Fn. 91.

cherheit sei zu gewährleisten.⁹³ Die Allianz der Liberalen und Demokraten für Europa, die Grünen und die Linken fordern - mehr oder minder drastisch - Konsequenzen für die nationalen Regelungen zur Vorratsdatenspeicherung und fordern die Europäische Kommission auf, ggf. Vertragsverletzungsverfahren einzuleiten.⁹⁴

Ähnlich stellt sich das Meinungsspektrum auf nationaler Ebene dar. Bundesinnenminister De Maizière stellt in seiner Pressemitteilung die Feststellung des EuGH in den Mittelpunkt, dass „die Vorratsdatenspeicherung ein geeignetes und nützliches Mittel zur Verhütung und Verfolgung schwerer Straftaten darstellt [...]“⁹⁵. Nur die konkrete Ausgestaltung sei mit der EU-GRCh unvereinbar, die Vorratsdatenspeicherung allgemein sei jedoch „sowohl verfassungsrechtlich als auch europarechtlich zulässig“⁹⁶. Abschließend wird die Vorratsdatenspeicherung als ein unverzichtbares Instrument bei der Verbrechensbekämpfung bezeichnet.⁹⁷ Bundesjustizminister Maas begrüßte das Urteil des EuGH und drängt in Anbetracht der nun entfallenen Verpflichtung zur Umsetzung der Richtlinie nicht auf eine schnelle Neuregelung - im Gegensatz zum Bundesinnenminister.⁹⁸

Kühling, Roßnagel und Wolff arbeiten heraus, dass der EuGH mit seinem Urteil über die BVerfG-Entscheidung vom 2. März 2010⁹⁹ hinausgeht, da dieses die Vorratsdatenspeicherung mit gewissen Einschränkungen für grundsätzlich verfassungskonform erachtete.¹⁰⁰ Hieraus ergäbe sich ein Dilemma für den europäischen Gesetzgeber, dem nur wenig bis gar kein Spielraum mehr verbliebe, um eine neue Vorratsdatenspeicherungsrichtlinie auf den Weg zu bringen, da die Grundidee der Vorratsdatenspeicherung und das Urteil des EuGH sich grundle-

⁹³ Siehe Fn. 91.

⁹⁴ Siehe Fn. 91.

⁹⁵ <http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2014/04/eugh.html> - letzter Abruf: 11.1.14 11.08 Uhr.

⁹⁶ Siehe Fn. 95.

⁹⁷ <http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2014/04/eugh.html> - letzter Abruf: 11.1.14 11.08 Uhr; so auch die Gewerkschaft der Polizei, siehe ZD-Aktuell 2014, 04017.

⁹⁸ Kuntz, MMR-Aktuell 2014, 357210; zur Forderung des BMI siehe Fn. 95. Interessant hierzu auch die Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, siehe ZD-Aktuell 2014, 04028.

⁹⁹ BVerfG, Urt. v. 2.3.10 - 1 BvR 256, 263, 586/08, BeckRS 2010, 46771.

¹⁰⁰ Kühling, NVwZ 2014, 681 (681 f.); Roßnagel, MMR 2014, 372 (374 f.); Wolff, DÖV 2014, 608 (609); vgl. auch Ogorek, JA 2014, 798 (800).

gend widersprüchen.¹⁰¹ Die drei Wissenschaftler würdigen das Urteil als „einen Meilenstein für den europäischen Grundrechtsschutz insgesamt und speziell für den grundrechtlichen Datenschutz“,¹⁰² der belege, „dass die Union auf ihrem Weg zu einer Rechtsgemeinschaft beharrlich und kontinuierlich voranschreitet“.¹⁰³

Priebe weist daraufhin, dass der Unionsgesetzgeber nicht zu einer Neuregelung verpflichtet sei - ihm stünde es frei, dies den Mitgliedstaaten zu überlassen.¹⁰⁴ Berücksichtigt man jedoch, dass zumindest die Europäische Kommission eine Vereinheitlichung des Datenschutzrechts in der EU beabsichtigt, dürfte dieser Hinweis wohl eher theoretischer Natur bleiben.¹⁰⁵

3.3 Eigene Bewertung

Die Debatte in der EU um die Vorratsdatenspeicherung scheint jedes Mal erneut aufzuflammen, wenn in einem EU-Mitgliedstaat ein Terroranschlag verübt wird. Bedenkt man jedoch, dass die jüngsten Anschläge in Paris nicht verhindert werden konnten, obwohl Frankreich sich seit Anfang 2006 der Vorratsdatenspeicherung bedient,¹⁰⁶ so muss dieser Automatismus in Frage gestellt werden. Es handelt sich hierbei nicht um einen Einzelfall. Ein Gutachten des Max-Planck-Institut für ausländisches und internationales Strafrecht ergab, dass es keinerlei empirischen Beweis für einen kriminologischen Mehrwert der Vorratsdatenspeicherung gäbe; es läge zudem noch nicht einmal ein Hinweis vor, dass Vorratsdatenspeicherung zur Verhinderung von Terroranschlägen geführt hätte,¹⁰⁷ wie auch das jüngste Beispiel zeigt. In Frankreich verfügte man über die entsprechenden Daten, diese wurden allerdings nicht umfassend ausgewertet. Diese Feststellung dürfte sich auch auf andere Staaten übertragen lassen. Es mangelt nicht am Datenbe-

¹⁰¹ Wolff, DÖV 2014, 608 (610); Kühling, NVwZ 2014, 681 (683 f.); Roßnagel, MMR 2014, 372 (375); ähnlich auch Streinz, JuS 2014, 758 (760), Classen, EuR 2014, 441 (447) und Schweda, ZD-Aktuell 2014, 04020.

¹⁰² Ähnlich Durner, DVBI 2014, 712 (715).

¹⁰³ So wörtlich Wolff, DÖV 2014, 608 (612); sinngemäß Kühling, NVwZ 2014, 681 (682, 684) und Roßnagel, MMR 2014, 372 (372, 376 f.); vgl. auch Ogorek, JA 2014, 798 (800) und Streinz, JuS 2014, 758 (760).

¹⁰⁴ Priebe, EuZW 2014, 456 (459).

¹⁰⁵ Ähnlich Priebe, EuZW 2014, 456 (459).

¹⁰⁶ Loi n° 2006-64 du 23 janvier 2006 - abrufbar unter: <http://www.jurizine.net/2006/01/29/40-loi-n-2006-64-du-23-janvier-2006> - letzter Abruf: 18.1.15 16.38 Uhr.

¹⁰⁷ Max-Planck-Institut für ausländisches und internationales Strafrecht: Schutzlücken durch Wegfall der Vorratsdatenspeicherung, 219.

stand, sondern an deren Auswertung. Hierauf sollten die Sicherheitsbehörden künftig ihre Konzentration lenken.

Es bleibt zu hoffen, dass nationale wie europäischer Gesetzgeber einsehen, dass eine Vorratsdatenspeicherung mit den Grundrechten ihrer Bürgerinnen und Bürger schwerlich zu vereinbaren ist, und sie künftig ihr Volk nicht mehr unter Generalverdacht stellen. Sollten Sie nicht generell von diesem Instrument absehen wollen, so sollten sie doch Kühling beherzigen: „[D]ie Sicherheitsgesetzgebung [wird] gezügelt, nicht das technisch Machbare, sondern das grundrechtlich Zumutbare anzustreben.“¹⁰⁸

4 Fazit

Der europäische Gesetzgeber versucht mit seinem neuen Datenschutzrahmen einen Spagat, der nicht gelingen kann. Droutsas formuliert daher zu Recht: „Europa [muss] entscheiden, wie [...] Informationen genutzt werden sollen, insbesondere im Hinblick auf die Strafverfolgung und den Kampf gegen und die Prävention von Kriminalität, ohne die Grundrechte und -normen zu verraten, für die wir so lange gekämpft haben.“¹⁰⁹

¹⁰⁸ Kühling, NVwZ 2014, 681 (685).

¹⁰⁹ Europäisches Parlament, A7-0403/2013, S. 125.

5 Literaturverzeichnis

- Boehme-Neßler, Volker 2014: Das Recht auf Vergessenwerden - Ein neues Internet-Grundrecht im Europäischen Recht. NVwZ 2014, 825-830.
- Calliess, Christian; Ruffert, Matthias 2011: EUV/AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta. Kommentar. 4. Aufl. München: C. H. Beck.
- Classen, Claus Dieter 2014: Datenschutz ja - aber wie?. EuR 2014, 441-448.
- Durner, Wolfgang 2014: Anmerkung zu EuGH, (große Kammer), Urteil vom 08.04.2014, - C-293/12 und C-594/12 - Digital Rights Ireland, Seitlinger u.a., Nichtigkeit der Richtlinie über die Vorratsdatenspeicherung. Zum Jagen getragen - der EuGH entdeckt den Datenschutz. DVBl 2014 ,712-715.
- Eckhardt, Jens 2012: EU-DatenschutzVO - Ein Schreckgespenst oder Fortschritt?. DuD 2012, 195-203.
- Gola, Peter; Klug, Christoph 2014: Die Entwicklung des Datenschutzrechts im zweiten Halbjahr 2013. NJW 2014, 667-672.
- Jandt, Silke 2014: EuGH stärkt den Schutz der Persönlichkeitsrechte gegenüber Suchmaschinen. MMR-Aktuell 2014, 358242.
- Kuntz, Wolfgang 2014: Stellungnahme des BMJ zum EuGH-Urteil zur Vorratsdatenspeicherung. MMR-Aktuell 2014, 357210.
- Kühling, Jürgen 2014: Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht. NVwZ 2014, 681-685.
- Max-Planck-Institut für ausländisches und internationales Strafrecht 2011: Schutzlücken durch Wegfall der Vorratsdatenspeicherung. Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten. Abrufbar unter: http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/20120127_MPI_Gutachten_VDS_Langfassung.pdf;jsessionid=9A59E53B144FE0F707A4BBBC2D3B877D.1_cid334?__blob=publicationFile - letzter Abruf: 11.1.2014 12.42 Uhr.

- Nolte, Norbert 2014: Das Recht auf Vergessenwerden - mehr als nur ein Hype?. NJW 2014, 2238-2242.
- Ogorek, Markus 2014: Ungültigkeit der Richtlinie über die Vorratsdatenspeicherung. JA 2014, 798-800.
- Philipp, Otmar 2014: Datenschutzrecht: Annahme der Datenschutz-Grundverordnung. EuZW 2014, 283.
- Priebe, Reinhard 2014: Reform der Vorratsdatenspeicherung - strenge Maßstäbe des EuGH. EuZW 2014, 456-459.
- Reimer, Helmut 2014: Report. BMI: Initiative zur Datenschutz-Grundverordnung: Konkrete deutsche Einwände!. DuD 2014, 639.
- Roßnagel, Alexander 2014: Neue Maßstäbe für den Datenschutz in Europa. Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung. MMR 2014, 372-377.
- Schweda, Sebastian 2014: EU: Politische Debatte zur Zukunft der Vorratsdatenspeicherung. MMR-Aktuell 2014, 357671.
- Ders. 2014: Vorratsdatenspeicherung in der EU - ja, nein, vielleicht, weiß nicht?. ZD-Aktuell 2014, 04020.
- Streinz, Rudolf 2014: Europarecht: Vorratsdatenspeicherung. Verstoß der Vorratsdatenspeicherungsrichtlinie gegen EU-Grundrechte. JuS 2014, 758-761.
- Wolff, Heinrich Amadeus 2014: Anmerkung zum Urteil des Europäischen Gerichtshofs vom 8.4.2014 zur Vorratsdatenspeicherung. DÖV 2014, 608-612.