Thea Riebe, Jasmin Haunschild, Felix Divo, Matthias Lang, Gerbert Roitburd, Jonas Franken, Christian Reuter

Die Vorratsdatenspeicherung in Europa

Thea Riebe

ist wissenschaftliche Mitarbeiterin und Doktorandin am Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) im Fachbereich Informatik der Technischen Universität Darmstadt. Ihre Forschungsinteressen liegen im Bereich Dual-Use Bewertung und Cybersicherheit.
E-Mail: riebe@peasec.tu-darmstadt.de

Jasmin Haunschild

ist wissenschaftliche Mitarbeiterin und Doktorandin am Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) im Fachbereich Informatik der Technischen Universität Darmstadt. Ihre Forschungsinteressen liegen im Bereich Sicherheitsinstitutionen, Recht, Datensicherheit und Compliance.
E-Mail: haunschild@peasec.tu-darmstadt.de

Felix Divo

ist Master Student der Informatik an der TU Darmstadt, Forschungsinteresse für Technik und Politik

E-Mail:
felix.divo@stud.tu-darmstadt.de

Matthias Lang

ist Schlagzeug-Lehrer an der Akademie für Tonkunst Darmstadt, sowie Orchestermusiker, freier Hörspiel-Autor und freischaffender Informatiker.
E-Mail:
matthias.lang@stud.tu-darmstadt.de

Gerbert Roitburd

ist Masterstudent am Fachbereich Informatik der TU Darmstadt. Zudem tätig als Penetrationtester und Security Researcher.

E-Mail: gerbert.roitburd@
stud.tu-darmstadt.de

Die Diskussion um die Vorratsdatenspeicherung ist europaweit weiterhin relevant, da es keine einheitliche Gesetzgebung der EU-Mitgliedsstaaten gibt. So werden in einigen EU-Staaten weiterhin Vorratsdaten gespeichert, obwohl der EuGH die Vorratsdatenspeicherung für teilweise rechtswidrig erklärt hat. Dabei unterscheiden sich die Speicherdauer, die erhobenen Daten und die Rechte der Behörden erheblich. Der Beitrag vergleicht den Umgang mit der Vorratsdatenspeicherung in zehn EU- und Schengen-Staaten im Hinblick auf Einführung und Aussetzung, Speicherdauer, Speicherinhalte und Zugriffsrechte.

1 Einleitung

Unter Vorratsdatenspeicherung (VDS) wird die tatverdachtsunabhängige und präventive Speicherung von personenbezoge-

Jonas Franken

ist studentischer Mitarbeiter am Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) im Fachbereich Informatik, sowie Masterstudent Internationalen Studien / Friedens- und Konfliktforschung an der Goethe Uni Frankfurt und der TU Darmstadt
E-Mail: jonas.franken@stud.tu-darmstadt.de

Prof. Dr. Christian Reuter

ist Universitätsprofessor und Inhaber des Lehrstuhls Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) im Fachbereich Informatik mit Zweitmitgliedschaft im Fachbereich Gesellschafts- und Geschichtswissenschaften der Technischen Universität Darmstadt.
E-Mail: reuter@peasec.tu-darmstadt.de

nen Daten verstanden.[1] Dabei werden Provider verpflichtet, bestimmte Tele- und Internetkommunikationsdaten ihrer Kunden über längere Zeit aufzubewahren.[2] Das Datenschutzrecht unterscheidet zwischen Bestandsdaten (Namen, Anschrift, genutzter Dienst), Verkehrsdaten (Telefonnummern, Anrufzeitpunkte, Dauer der Telefonate, Standortdaten) und Inhaltsdaten (tatsächlich ausgetauschte Informationen).[3] Für die VDS sind nur die Verkehrs- und Bestandsdaten relevant und dürfen zum Beispiel von der Polizei zu Ermittlungs- oder Verfahrenszwecken abgerufen werden. Außerhalb der erlaubten Speicherpflicht liegen die Inhaltsdaten.[4]

Aus der Sicht Vieler greift die VDS nicht nur in die Privatsphäre, sondern auch in die Unschuldsvermutung der Bürger ein und ist technisch aufwendig. Die VDS verspricht allerdings rückblickende Einsicht in sonst flüchtige Daten und kann somit eine wertvolle Informationsquelle bei Ermittlungsverfahren darstellen. Das Thema birgt somit Konfliktpotential zwischen den Datenschutzrechten des Individuums und den Strafverfolgungspflichten des Staates.[5]

Die VDS ist in Europa nicht nur gesellschaftlich umstritten, sondern wird auch rechtlich keineswegs einheitlich bewertet. So hat die EU zwar im Jahr 2006 mit der *Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten*[6] (RL 2006/24/EG) ihre Mitglieder zur VDS verpflichtet, doch wurde diese Richtlinie 2014 vom Europäischen Gerichtshof (EuGH) wiederum für ungültig befunden.[7]

Die Agentur der Europäischen Union für Grundrechte (FRA) hat im aktuellen Jahresbericht 2019 darauf hingewiesen, dass ein Festhalten an nationalen VDS-Gesetzgebungen, die sich an der ungültigen EU-RL orientieren, das Risiko der Missachtung der EU-Grundrechte und die Untergrabung der Rechtssicherheit in der gesamten Union bergen.[8] Andere Beiträge zum Thema europäische VDS diskutieren primär die Grundrechtskonformität. Im Zusammenhang mit der Wiedereinführung der deutschen VDS stellen Gärtner und Kipker 2015 fest, es sei „vor allem die Sicherheit, die im Vordergrund steht, nicht die Freiheit. Dass aber die Sicherheit kein Selbstzweck sein kann, sondern letztlich dem Schutz der Freiheit zu dienen bestimmt ist, gerät dabei schnell aus dem Fokus."[9]

Zu einer ähnlichen Bewertung kommt Koshan 2016[10] und fordert eine „informationsverfassungsrechtliche Grundlegung", die durch Lernprozesse den technologiebedingten gesellschaftlichen Veränderungen gerecht wird, ohne den Sicherheitsaspekt gegenüber den Grundrechten zu priorisieren.

In einem Vergleich der nationalen Umsetzung der RL 2008 urteilen Forgó et al., „Europa [tue] sich mit der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung schwer"[11], und zeigen die schleppende Umsetzung durch die Mitgliedstaaten. Ein Vergleich von Privacy International zeigt 2017 zudem die vorgenommenen (und ausgelassenen) Anpassungen durch die zweite Rechtsprechung des EuGH 2016 zur VDS.[12]

Aufbauend darauf liegt der Fokus dieses Beitrags auf einem Vergleich der aktuellen Unterschiede sowie der Entwicklungen der Speicherdauern, inklusive der Regelung des Zugriffs auf die gespeicherten Informationen, wie auch auf einer Exploration der Wechselwirkungen zwischen nationalstaatlicher und europäischer Rechtsprechung. Einige Länder hatten die VDS erst in Reaktion auf die europäische Richtlinie und nicht aufgrund national festgestellter Notwendigkeit eingeführt. Es wäre daher erwartbar, dass besonders jene Länder die VDS nach dem EuGH-Urteil wieder ausgesetzt hätten. Zudem wäre aufgrund der ähnlichen politisch-sozialen Situation der westeuropäischen Staaten bei einer bedarfsorientierten Umsetzung mit einer großen Übereinstimmung der nationalen Implementierungen zu rechnen. Ein Vergleich kann daher Erkenntnisse über den Einfluss europäischer Richtlinien oder des EuGH sowie die nationale Implementierung von Sicherheitsmaßnahmen liefern und zur Theoriegenerierung beitragen.[13]

Abbildung 1 | Betrachtete Staaten des Schengenraumes (dunkel): Deutschland, Österreich, Schweiz, das Vereinigte Königreich, Frankreich, Niederlande, Irland, Italien, Spanien und Polen

1 Moser-Knierim, A. (2014): *Vorratsdatenspeicherung*, Berlin: Springer, S. 139–206.

2 Europäisches Parlament und der Rat der Europäischen Union (2006): *Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates*. Zugriff über: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32006L0024 (zugegriffen am 05.12.2018).

3 Kühnl, C. (2016): *Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA*, Berlin: Walter de Gruyter GmbH, S. 144.

Moser-Knierim, 2014.

4 Moser-Knierim, 2014

5 Moser-Knierim, 2014

6 Europäisches Parlament und der Rat der Europäischen Union, 2006

7 Gerichtshof der Europäischen Union. (2014). *Urteil des Gerichtshofs in den verbundenen Rechtssachen C293/12 und C594/12*, Zugriff über: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:62012CJ0293 (zugegriffen am 05.12.2019), S. 22.

8 European Union Agency for Fundamental Rights (2019): Fundamental Rights Report 2019, Luxembourg: Publications Office of the European Union, S. 162-163.

9 Gärtner, H. & Kipker, D (2015): Die Neuauflage der Vorratsdatenspeicherung, in: *Datenschutz und Datensicherheit (DuD)*, Bd. 39, Ausg. 9 (09/2015), S. 593-599.

10 Koshan, M. (2016). Vorratsdatenspeicherung – verfassungsrechtliche Rahmenbedingungen und rechtspolitische Verortung. DuD, 40, 167–171.

11 Forgó, N.; Jlussi, D.; Klügel, C.; Krügel, T (2008): Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung, in: *Datenschutz und Datensicherheit (DuD)* Bd. 32, Ausg. 10 (10/2008), S. 680.

12 Privacy International (2017): *A Concerning State of Play for the Right to Privacy in Europe – National Data Retention Laws since the CJEU's Tele-2/Watson Judgment*, Zugriff über: https://privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf (zugegriffen am 05.12.2019).

13 Lauth et al., 2016, S. 26.

2 Methode

Der synchrone Vergleich zum Zeitpunkt 12/2019 unter Anwendung der Differenzmethode[14] schließt den Einfluss verschiedener Kontextvariablen aus, indem Fälle betrachtet werden, die historisch und durch die Mitgliedschaft in der EU viele Gemeinsamkeiten haben (s. Abb. 1). Folgende Daten werden für die Länder erhoben:

- Existenz einer Form von VDS,
- Speicherdauern für Vorratsdaten,
- Umfang des Zugriffs staatlicher Stellen auf die Vorratsdaten,
- qualitative Hürden für den Zugriff auf die Daten, z. B. die Voraussetzung eines richterlichen Beschlusses.

Dabei variiert die Datenlage je nach Land von Transparenz bis zu sporadischen, teilweise nur durch Whistleblower veröffentlichten Informationen.

3 Vergleichende Analyse

Die Richtlinie 2006/24/EG gab den einzelnen Mitgliedsstaaten viel Freiraum bei der Umsetzung der VDS, die den Ermittlern bei der Verfolgung schwerer Straftaten helfen soll, wobei der Straftatbestand nicht definiert wurde. Der Umfang der Speicherdauer wurde in der RL flexibel zwischen sechs Monaten und zwei Jahren vorgesehen. Hinsichtlich der Speicherinhalte wurden Verkehrs- und Standortdaten für Telekommunikation (Mobilfunk und Festnetz) und Internetnutzung festgelegt. Zusätzlich durften alle weiteren Daten erhoben werden, die im Zusammenhang mit den Verkehrs- und Standortdaten standen und zur Identifizierung eines Teilnehmers oder Nutzers erforderlich waren. Die Umsetzungsgesetze unterscheiden sich von Land zu Land hinsichtlich ihrer Speicherinhalte, -fristen und Kontrollinstanzen deutlich.

3.1 Vergleich der Einführung und Aussetzung von VDS

Die Betrachtung der historischen Entwicklung der VDS in Europa zeigt, dass die nationale Rechtsprechung stark von der europäischen abhängig war und ist (siehe Abb. 2). So sind der Zeitpunkt der EU-RL 2006/24/EG und die darauffolgenden nationalen Reaktionen klar erkennbar. Allerdings zeigt der Vergleich auch, dass es Länder gibt, die die VDS schon vor 2006 eingeführt haben:

- Dabei war **Irland**, mit einer Einführung um 1993, Vorreiter.[15] Dort war auf nationaler Ebene das Abhören von Metadaten („*metering*“) nicht reguliert. VDS wurde von der damaligen Regierung bereits seit 1983 auch tatsächlich praktiziert.[16] Bei einer Gesetzesanpassung im Jahr 1993 waren kein Richtervorbehalt sowie keine Einschränkungen im Hinblick auf Dauer, Umfang und die Schwere der Straftaten vorgesehen.[17] Zudem war die irische Regierung zusammen mit Frankreich, Schweden und Großbritannien maßgeblich für die Verabschiedung der EU-RL 2006 mitverantwortlich.[18]
- Erst im Januar 2000 folgte in den beobachteten Ländern die nächste VDS-Einführung in den **Niederlanden**. Dort wurde ein Gesetz verabschiedet, welches Telekommunikationsunternehmen verpflichtete, alle 24 Stunden ihre gesammelten Verkehrsdaten an den *Centraal Informatiepunt Onderzoek Telecommunicatie* (CIOT) als zentralen, staatlichen Speicherpunkt zu übermitteln.[19]
- Als einziges Nicht-EU-Mitglied im Vergleich wurde in der **Schweiz** auch bereits im Oktober 2001 mit dem *Bundesgesetz betreffend Überwachung des Post- und Fernmeldeverkehrs* (BÜPF) eine VDS gesetzlich verankert.[20]
- VDS wurde in **Polen** seit 2003 praktiziert.[21]
- **Italien** führte die VDS im Juli 2003 mit dem Gesetz 196/2003 ein.[22] Im Gesetz war der Begriff der VDS jedoch noch nicht vorhanden, sondern nur die Verpflichtung der Provider, die Weiterleitung älterer Daten für Ermittlungszwecke zu garantieren.

Nach den Madrider Zuganschlägen vom 11. März 2004 rückte das Thema in den EU-weiten Fokus.[23] Der Terroranschlag am 7. Juli 2005 in London[24] verstärkte die Debatte, sodass im selben Jahr ein Entwurf für eine RL eingereicht wurde.[25] 2006 verabschiedeten das Europäische Parlament und der Europäische Rat die Richtlinie 2006/24/EG, die am 3. Mai 2006 in Kraft trat und 18 Monate Zeit zur Umsetzung in nationales Recht einräumte.

- Bemerkenswert ist dabei, dass **Frankreich**, welches mitverantwortlich für den Entwurf war, schon am 23. Januar 2006, also vor der EU-Richtlinie, eine richtlinienkonforme Gesetzgebung verabschiedete.[26]

14 Nohlen, 2004, S. 1046.

15 McIntyre, T. (2008). Data Retention in Ireland: Privacy, Policy and Proportionality. Computer Law & Security Review, 24(4), 326-34. Zugriff über: https://ssrn.com/abstract=2426208 (zugegriffen am 05.12.2019).

16 Ebd., S. 329.

17 Seanad Éireann (1993): *Interception of Postal Packets and Telecommunications Act, Zugriff über: http://www.irishstatutebook.ie/eli/1993/act/10/enacted/en/print.html (*zugegriffen am 10.12.2019).

18 Rat der Europäischen Union (2004): *Explanatory Memorandum. Framework Descision on the Retention of Communications Data*, Dok.-Nr. 8958/04, Zugriff über: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%208958%202004%20ADD% 201, zugegriffen am 10.12.2019).

19 Ministry of Security and Justice Netherlands (2000): *Besluit verstrekking gegevens telecommunicatie*, Zugriff über: http://wetten.overheid.nl/BWBR0011123/2016-12-28 (zugegriffen am 10.12.2019).

20 Bundesrat (Schweiz) (2000): *Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF*), Zugriff über: https://www.admin.ch/opc/de/classified-compilation/20002162/index.html (zugegriffen am 05.12.2019).

21 Szymielewicz, K. (2014): Data Retention in Poland: The issue and the Fight. Zugriff über: https://en.panoptykon.org/sites/default/files/Katarzyna_Szymielewicz_Data%20Retention%20in%20Poland_The%20Issue%20and%20the%20Fight.pdf#overlay-context= (zugegriffen am 05.12.2019).

22 Parlamento Italiano (2003): Decreto Legislativo 30 giugno 2003, n. 196, Zugriff über: https://www.camera.it/parlam/leggi/deleghe/03196dl.htm (zugegriffen am 05.12.2019).

23 Spiegel Online (2004): Terror in Madrid – Züge von Bomben zer-fetzt – 192 Tote, mehr als 1400 Verletzte. Spiegel Online. Zugriff über: http://www.spiegel.de/panorama/terror-in-madrid-zuege-von-bomben-zerfetzt-192-tote-mehr -als-1400-verletzte-a-290117.html (zugegriffen am 05.12.2019).

24 Spiegel Online (2005): Anschlagsserie in London – Tag des Schreckens, Zugriff über: http://www .spiegel.de/panorama/anschlagsserie-in-london-tag-des-schreckens-a-364144.html (zugegriffen am 05.12.2019).

25 Europäische Kommission (2005): Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC.Zugriff über: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission _europeenne/sec/2005/1131/COM_SEC(2005)1131_EN.pdf (zugegriffen am 05.12.2019).

26 L'Assemblée nationale et le Sénat (2006): *LOI N° 2006-64 du 23 janvier 2006.* Zugriff über: http://www.jurizine.net/ 2006/01/29/40-loi-n-2006-64-du-23-janvier-2006 (zugegriffen am 05.12.2019).

- In **Spanien** wurde die VDS erstmalig im Telekommunikationsgesetz 25/2007 als Umsetzung der RL 2006/24/EG geregelt.[27]
- Die Richtlinienumsetzung in deutsches Recht, das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der RL 2006/24/EG"[28] wurde allerdings erst am 09.11.2007 im Bundestag verabschiedet und trat schließlich zum 1. Januar 2008 in Kraft.[29] **Deutschland** konnte somit bei der Umsetzung, wie 19 andere EU-Mitgliedsstaaten auch, die von der EU gesetzte Frist nicht einhalten.[30] Hinzu kam, dass gem. § 150 Absatz 12b des aktualisierten Telekommunikationsgesetzes (TKG) Verstöße gegen die Speicherung erst ab dem 1. Januar 2009 verfolgt wurden und sich daher die Umsetzung durch die Provider zunächst über ein ganzes Jahr verteilte. So zeigte eine von netzpolitik.org durchgeführte Befragung der Provider, dass nur wenige Provider zum 1. Januar 2008 die Daten rechtskonform speicherten.[31]
- Ein Beispiel für ein EU-Mitgliedsstaat, der die Umsetzung der RL 2006/24/EG noch später als Deutschland vollzog, ist **Österreich**. Nachdem dort die Richtlinie der EU noch nicht umgesetzt wurde, reichte die EU-Kommission im Mai 2009 Klage vor dem EuGH ein (Kommission der Europäischen Gemeinschaften, 2009). Letztlich beschloss der österreichische Nationalrat im April 2011 die Einführung der VDS zum April 2012.[32]

Noch vor der Umsetzung in Österreich erklärte das deutsche Bundesverfassungsgericht die bestehende Rechtslage in Deutschland 2010 nach einer Verfassungsbeschwerde für nichtig, da diese und auch die RL 2006/24/EG unvereinbar mit Art. 10 Abs. 1 (Brief-, Post- und Fernmeldegeheimnis) des deutschen Grundgesetzes seien und das Gesetz Eingriffe nicht ausreichend klar regele.[33] Vier Jahre später, im April 2014 erklärte auch der **EuGH** die EU-Richtlinie für unionsrechtswidrig[34], was direkt dazu führte, dass der **österreichische** Verfassungsgerichtshof im Juni desselben Jahres die nationale VDS für verfassungswidrig erklärte.[35] Bis auf die **niederländische** VDS, welche im März 2015 per Eilverfahren gekippt wurde[36], blieben die nationalen Umsetzungen jedoch bestehen.

Bemerkenswert ist, dass **Deutschland** der einzige Staat der Auswahl ist, welcher, nachdem die EU-Richtlinie für nichtig erklärt wurde, noch eine neue VDS-Gesetzgebung beschloss. Diese trat im Dezember 2015 in Kraft und sollte ab Juli 2017 alle Provider zur Speicherung verpflichten.[37,38] Jedoch wurde diese kurz vor dieser Frist am 28. Juni 2017 von der Bundesnetzagentur zunächst ausgesetzt, was dazu führte, dass die VDS in Deutschland effektiv nicht durchgeführt wird.[39] Ermittelnde Behörden haben in der Folge nur Zugriff auf von Anbietern zur Kostenabrechnung gespeicherten Daten, die von Letzteren unterschiedlich lange gespeichert werden.

Eine neue Entwicklung zeigt sich aktuell in **Österreich**, wo seit Anfang Juni 2018 die VDS-Alternative *Quick Freeze* praktiziert wird.[40] Das *Quick-Freeze*-Verfahren sieht die Speicherung von individuellen Daten allein im Verdachtsfall vor.[41] Eine ex-ante-Betrachtung von Kommunikationsdaten vor dem Verdachtsfall wird damit verwehrt und Daten der Gesamtbevölkerung werden nicht mehr anlasslos erhoben.[42] Dieses Verfahren könnte in Zukunft auch Vorbild für andere Staaten werden.

Somit sind in der getroffenen Auswahl aktuell (Dezember 2019) nur Deutschland, die Niederlande und Österreich ohne eine VDS, während die VDS in der Schweiz, dem Vereinigten Königreich, Irland, Frankreich, Italien, Spanien und Polen weiterbesteht. Trotz fehlender EU-Richtlinie kam es ab 2014 zu weiteren nationalen Anpassungen der Rechtslage, wie zum Beispiel dem *Data Retention and Investigatory Powers Act* 2014 in Großbritannien[43], dem *French Intelligence Act* 2015[44] und einem neuen Gesetz zur

27 Statewatch/Rat der Europäischen Union (2017): *Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15; Report 10098/17.* Zugriff über: http://statewatch.org/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf (Der Rat der Europäischen Union hat am 03.01.2018 eine gekürzte Fassung des von Statewatch veröffentlichten voll-ständigen Berichts deklassifiziert, siehe dazu http://data.consilium.europa.eu/doc/document/ST-10098-2017-INIT/en/pdf; zugegriffen am 05.12.2019);

Cortes Generales de España (2007): *Ley 25/2007, de 18 de octubre, de con-servación de datos relativos a las comunicaciones electrónicas y a las redes públicas de Comunicaciones,* Zugriff über: https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243 (zugegriffen am 05.12.2019).

28 Deutscher Bundestag (2007): *Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*, BT-Drs. 16/5846, Zugriff über: http://dip21 .bundestag.de/dip21/btd/16/058/1605846.pdf (zugegriffen am 05.12.2019).

29 Krempl, S. (2007): Bundestag verabschiedet Gesetz zur Vorratsdatenspeicherung und TK-Überwachung, Zugriff über: https://www.heise.de/newsticker/meldung/Bundestag-verabschiedet-Gesetz-zur-Vorratsdatenspeicherung-und-TK-ueberwachung-193892.html (zugegriffen am 05.12.2019).

30 Forgó et al. (2008), S. 681-682.

31 Meister, A. (2008) Vorratsdatenspeicherung: Umsetzung und Kosten, Zugriff über: https://netzpolitik.org/2008/vorratsdatenspeicherung-umsetzung-und-kosten/ (zugegriffen am 05.12.2019).

32 Sokolov, D. A. (2011): SPÖ und ÖVP beschließen Vorratsdatenspeicherung in Österreich. Zugriff über: https://www.heise .de/newsticker/meldung/SPOe-und-OeVP-beschliessen-Vorratsdatenspeicherung-in-Oesterreich-1234732.html (zugegriffen am 05.12.2019).

33 Bundesverfassungsgericht (2010): *Urteil des Ersten Senats vom 02. März 2010* – 1 BvR 256/08 – Rn. (1-345). Zugriff über: http://www.bverfg.de/e/rs20100302_1bvr 025608.html (zugegriffen am 05.12.2019).

34 Gerichtshof der Europäischen Union, 2014, S. 22.

35 Bundeskanzler (2014): *Kundmachung des Bundeskanzlers über die Aufhebung von Bestimmungen des Telekommunikationsgesetzes 2003, der Strafprozeßordnung 1975 und des Sicherheitspolizeigesetzes durch den Verfassungsgerichtshof.* Zugriff über: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2014_I_44/BGBLA_ 2014_I_44.pdfsig (zugegriffen am 05.12.2019).

36 Rechtbank Den Haag (2015): *ECLI:NL:RBDHA:2015:2498,* C/09/480009 / KG ZA 14/1575. Zugriff über: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498 (zugegriffen am 05.12.2019).

37 Deutscher Bundestag, 2015

38 Warislohner, F. (2015): Vorratsdatenspeicherung tritt heute in Kraft. Zugriff über: https://netzpolitik.org/2015/vorratsdaten-speicherung-tritt-heute-in-kraft/ (zugegriffen am 05.12.2019).

39 Bundesnetzagentur (2017): Mitteilung zur Speicherverpflichtung nach § 113b TKG, Zugriff über: https:// www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/ (zugegriffen am 05.12.2019).

40 Justizausschusses des Nationalrates XXVI. GP (2018): Bericht des Justizausschusses. Zugriff über: https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00092/fnameorig_688853.html (zugegriffen am 05.12.2019).

41 Fanta, A. (2018): Lauschen wie noch nie: Österreich beschließt Überwachungspaket. Zugriff über: https://netzpolitik.org/2018/lauschen-wie-noch-nie-oesterreich-beschliesst-ueberwachungspaket/ (zugegriffen am 05.12.2019).

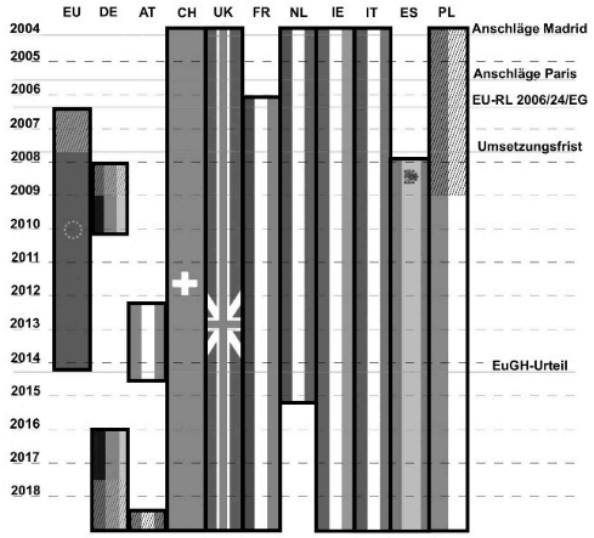
42 Moenikes, J. (2011): Quick Freeze – der Wolf im Schafspelz, Zugriff über: https://www.moenikes.de/ITC/2011/01/18/ quick-freeze-%E2%80%93-der-wolf-im-schafspelz/ (zugegriffen am 12.12.2019).

43 Regierung des Vereinigten Königreichs (2014): *Data Retention and Investigatory Powers Act 2014.* Zugriff über: https://www.gov.uk/government/collections/data-retention-and-investigatory-powers-act-2014/ (zugegriffen am 05.12.2019).

44 L'Assemblée nationale et le Sénat (2015): *LOI n° 2015-912 du 24 juillet 2015 relative au renseignement.* Zugriff über: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899 (zugegriffen am 05.12.2019).

Terrorbekämpfung in Italien.[45] Im März 2018 trat in der Schweiz eine Totalrevision des BÜPF in Kraft, wobei sich diese auch an der mittlerweile ungültigen EU-RL orientierte.[46]

Abbildung 2 | Übersicht über den zeitlichen Verlauf der VDS-Anwendung in den betrachteten Ländern. Ein Balken steht für eine aktive Form von VDS. Die Schraffur stellt Sonderfälle dar, die einer VDS nahekommen: In Deutschland aktuell eine bestehende, aber nicht ausgeführte VDS und in Österreich das Quick-Freeze-Verfahren.



3.2 Die Speicherinhalte

Hinsichtlich der Speicherinhalte ist eine große Varianz zwischen den einzelnen Mitgliedsstaaten zu erkennen. Die Hälfte der untersuchten EU-Mitgliedsländer verabschiedete Gesetze zur VDS erst nach der Veröffentlichung der Telekommunikationsrichtlinie 2006/24/EG. Die restlichen Länder, die bereits eine Form der VDS betrieben, passten ihre Gesetze an die eingeführte RL an. Länder wie Frankreich, Niederlande, Spanien, Italien und Irland speicherten exakt die Daten, die durch die RL vorgegeben waren.

Die Schweiz bildet eine Ausnahme, da hier nicht nur die elektronische Kommunikation überwacht wird, sondern auch die des Postverkehrs sowie Rechnungsdaten und Verkehrsdaten durch Postunternehmen. Im Vereinigten Königreich wird statt der IP des Zieldienstes die gesamte URL festgehalten, die ggf. sensible Informationen bezüglich der Nutzungsart des Dienstes beinhalten kann.[47] Diese Informationen sind detaillierter und aufschlussreicher als nur die IP-Adresse des genutzten Dienstes, welche aber laut EU-Richtlinie bereits ausreichend wäre. Eine weitere Ausnahme bildet Österreich. Dort wird die Quick-Freeze-Methodik zur Speicherung von Daten angewandt, bei der neben Verkehrsdaten, Zugangsdaten und Standortdaten auch Inhaltsdaten elektronischer Kommunikation im Klartext gespeichert werden können.[48]

3.3 Speicherdauern

RL 2006/24/EG sah vor, Verkehrs- und Standortdaten für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren zu speichern.[49] Die Speicherdauern für Vorratsdaten in Europa variieren stark (s. Abb. 3): zwischen vier und zehn Wochen in Deutschland und sechs Jahren in Italien.

Abbildung 3 | Speicherdauer in Monaten, Stand September 2018: keine VDS, weniger als 12, 12, >= 24. Bei mehreren Speicherdauern (Deutschland, Italien) jeweils die längste.

Dabei legen Deutschland und Italien auch unterschiedliche Speicherdauern für verschiedene Datentypen fest.[50] Die bei Weitem restriktivsten Speicherdauern finden sich in Deutschland, wo Standortdaten für vier Wochen und alle weiteren Daten für zehn Wochen gespeichert werden müssen.[51] In der Schweiz und den Niederlanden gilt dagegen eine Speicherdauer von sechs Monaten.[52] Auf den britischen Inseln (UK und Irland) müssen die Daten für ein Jahr auf Vorrat gehalten werden.[53] Eine vergleichsweise lange Speicherdauer von zwei Jahren ist in Polen zu finden.[54] In Italien werden die längsten Speicherdauern für Telefondaten vorgeschrieben; diese müssen hier für sechs Jahre gespeichert werden, während sonstige Vorratsdaten für nur zwei Jahre zu speichern sind.[55] Eine Übersichtsdarstellung über die verschiedenen Speicherdauern ist in Abb. 4 zu sehen.

45 Parlamento Italiano (2015): *Misure urgenti per il contrasto del terrorismo nonché proroga delle missioni internazionali delle Forze armate e di polizia.* Zugriff über: http://documenti.camera.it/leg17/dossier/Testi/D15007a.htm (zugegriffen am 05.12.2019).

46 Bundesamt für Justiz (Schweiz) (2017): *Überwachung des Fernmeldeverkehrs*, Zugriff über: https://www.bj.admin.ch/ bj/de/home/sicherheit/gesetzgebung/archiv/fernmeldeueberwachung.html (zugegriffen am 12.12.2019).

47 Big Brother Watch (2016): Internet Connection Records, Zugriff über: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Internet-Connection-Records.pdf.

48 Justizausschuss des Nationalrates XXVI. GP, 2018.

49 Europäisches Parlament und der Rat der Europäischen Union, 2006.

50 Deutscher Bundestag, 2015; Parlamento Italiano, 2015.

51 Bundestag 2015.

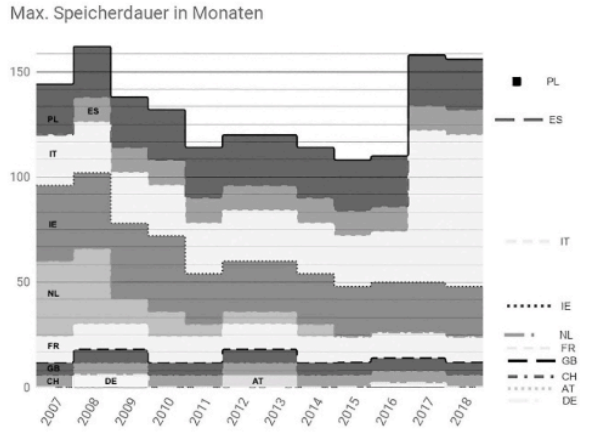
52 Eerste Kamer der Staten-Generaal (2011): *Staatsblad van het Koninkrijk der Nederlanden – 2011 350*, Zugriff über: https://zoek.officielebekendmakingen.nl/stb-2011-350.pdf (zugegriffen am 05.12.2019); Bundesrat (Schweiz) (2001): Verordnung über die Überwachung des Post- und Fernmeldeverkehrs. Zugriff über: https:// www.admin.ch/opc/de/official-compilation/2001/3111.pdf (zugegriffen am 05.12.2019).

53 Regierung der Republik Irland (2011): *Communications (Retention of Data) Act 2011*, Zugriff über: http://www.irishstatutebook.ie/eli/2011/act/3/enacted/print.html (zugegriffen am 05.12.2019). Regierung des Vereinigten Königreichs (2014): *c. 27 / Data Retention and Investigatory Powers Act 2014*, Zugriff über: http://www.legislation.gov.uk/ukpga/2014/27/enacted (zugegriffen am 05.12.2019).

54 Szymielewicz, 2014.

55 Parlamento Italiano, 2015.

Abbildung 4 | Jahrweise Übersicht der kumulierten nationalen Speicherdauern in Monaten. Bei mehreren Speicherdauern (Deutschland und Italien) je die höchste.



3.4 Zugriffsrechte

Die Spannweite der Behörden, die auf die Vorratsdaten zugreifen können, ist sehr weit und unterscheidet sich auch in der Weise der Festlegung in den betrachteten Ländern stark.

In allen Ländern dürfen die Polizei bzw. Strafverfolgungsbehörden Zugriff auf die Daten anfordern. In Österreich ist die Polizei die einzige Behörde, die auf Daten des dortigen Quick Freeze zugreifen darf.[56] In der Schweiz, Irland und dem Vereinigten Königreich haben die Nachrichtendienste Zugriff auf die Vorratsdaten, während in Deutschland strenge Voraussetzungen an den Zugriff der Nachrichtendienste geknüpft werden.[57] Im Vereinigten Königreich, in Irland und Polen haben zusätzlich noch militärische Einrichtungen eine Zugriffsberechtigung. In diesen drei Ländern können insgesamt auffällig viele Akteure auf die Daten zugreifen, wie etwa in Irland z. B. das Zoll- und Finanzamt oder in Polen z. B. das Amt für Steuern.[58] Im Vereinigten Königreich haben noch viele weitere Stellen Zugriff.[59] In Frankreich[60] und Spanien[61] ist nicht explizit festgelegt, welche Behörden auf die Daten zugreifen können. In den meisten Ländern wird ein richterlicher Beschluss benötigt, um auf die Daten zugreifen zu können. Ausnahmen bilden Italien[62] und Polen[63].

Die großen Differenzen zwischen den verschiedenen nationalen Regelungen lassen sich auch auf die bezüglich Zugriffsrechten und -schutz fehlenden Vorgaben der EU RL 2006/24/EG zurückführen, die lediglich abstrakte Kontrollmechanismen forderte. [64]

4 Fazit

Wegen der wiederkehrenden Diskussionen und zunehmenden Nutzung von Telekomunikation ist die Thematik der VDS noch immer aktuell. Im Jahr 2006 wurde Richtlinie 2006/24/EG zur VDS verabschiedet, die 2014 vom EuGH als ungültig erklärt wurde und 2016 auf schwere Straftaten und das Vorliegen eines Anlasses beschränkt wurden.[65] Die jeweilige Umsetzung in nationales Recht ist von Land zu Land unterschiedlich. Zum Zeitpunkt des Richtlinienbeschlusses hatten einige Länder bereits Maßnahmen eingeführt (z. B. die Schweiz und Irland), einige Agenda-Setter innerhalb der EU waren im Begriff dies zu tun (z. B. Frankreich) und andere ergriffen Maßnahmen erst in Reaktion auf die RL (z. B. Deutschland). Die Richtlinie wurde sowohl national vor Verfassungsgerichten (Deutschland und Österreich) als auch auf EU-Ebene vor dem EuGH angefochten und 2014 außer Kraft gesetzt, weil sie einen unverhältnismäßigen Eingriff in die Grundrechte der Menschen darstelle.

Die Analyse der vorliegenden Fälle deutet darauf hin, dass die Einführung und die aktuelle Nutzung der VDS zum Teil unabhängig von der europäischen Richtlinie stattgefunden hat. Dies liegt einerseits daran, dass Richtlinien die Umsetzung immer den Mitgliedsstaaten offenlassen. Andererseits zeigt sich, dass jene Staaten, die an einer Einführung der VDS interessiert waren, diese bereits vor der RL einzuführen begannen. Die zunächst widerstrebenden Staaten wie Deutschland und Österreich fochten die Regelung zwar rechtlich an, verfügen inzwischen aber wieder über eine Art der VDS, obwohl diese seitens EU nicht mehr gefordert ist, sondern im Gegenteil zum Teil sogar als den europäischen Grundrechten widersprechend beurteilt wurde. Diese Feststellungen werfen weitere Fragen über das Zusammenspiel europäischer und nationaler Gesetzgebung auf: Dabei ist unklar, ob das Verbleiben (ESP) bei oder erneute Einführen der VDS (DEU, AUT) als Pfadabhängigkeit zu verstehen ist oder ein versicherheitlichender Diskurs die Weiterführung notwendig erscheinen lässt.

56 Justizausschuss des Nationalrates XXVI. GP, 2018.

57 Gemäß § 113c Abs. 1 Nr. 2 TKG haben Gefahrenabwehrbehörden der Länder nur Zugriffsrechte „zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes". Zudem ist der Status von Nachrichtendiensten als Gefahrenabwehrbehörden i.S.d. § 113c Abs .1 Nr. 2 TKG umstritten. Vgl. hierzu: Biselli, A. (2016): Bundesregierung: Kein Kommentar zu Zugriff auf Vorratsdaten durch Bayerischen Verfassungsschutz, Zugriff über: https://netzpolitik.org/2016/bundesregierung-kein-kommentar-zu-zugriff-auf-vorratsdaten-durch-bayerischen-verfassungsschutz/ (zugegriffen am 10.12.2019).

58 Szymielewicz, 2014.

59 Regierung des Vereinigten Königreichs (2016a): *2016 c. 25 / Investigatory Powers Act 2016* Zugriff über: http:// www.legislation.gov.uk/ukpga/2016/25/ enacted (zugegriffen am 05.12.2019).

60 L'Assemblée nationale et le Sénat, 2015.

61 Cortes Generales de España (2014): *Ley 9/2014, de 9 de mayo, General de Telecomunicaciones*, Zugriff über: https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950 (zugegriffen am 05.12.2019).

62 Parlamento Italiano, 2015.

63 Szymielewicz, 2014.

64 Europäisches Parlament und der Rat der EU, 2006, Art. 9 Abs. 1.

65 Gerichtshof der Europäischen Union. (2016). *Urteil des Gerichtshofs in den verbundenen Rechtssachen C-203/15 und C-698/15*, Zugriff über: http://curia.europa.eu/juris/document/document.jsf?docid=1864928 (zugegriffen am 10.12.2019).