Iustum Aequum Salutare
XIV. 2018. 1. • 141–155.

DISSERTATIONES

GESETZLICHE REGELUNG ZUM DATENSCHUTZ UND FRAGEN DER VORRATSDATENSPEICHERUNG

Zsófia Ádám
Doktorandin (PPKE JÁK)

1. Einleitung

Das Thema der Vorratsspeicherung und Datenschutz wird heutzutage nicht nur in der Europäischen Union, sondern weltweit umfassend diskutiert.

Vor kurzem veröffentlichte die Europäische Polizeibehörde Europol den Terrorismusbericht für das Jahr 2016.

Der Bericht zeigt, dass nur im letzten Jahr europaweit 142 Terroranschläge registriert wurden, einbezüglich der von Europol vereitelten Anschläge. 142 Menschen sind letztes Jahr durch Terrorattacken um das Leben gekommen, davon 135 durch radikal islamistische Personen. Ermittler haben inzwischen über 700 Verdächtige festgenommen.[1] Die Täter dieser grausamen Straftaten nutzten soziale Netzwerke und diverse Telekommunikationssysteme, um verborgen miteinander Verbindung zu halten. Zunehmend werden immer mehr Jugendliche für die Anschlägen eingesetzt, das Internet wird für Propaganda und Rekrutierung benutzt.

Es ist kaum zu bezweifeln, dass Telekommunikationsmittel nicht nur für Terroranschläge benutzt werden können, sondern auch im Allgemeinen, bei Begehung vieler Straftaten als Kommunikationskanal dienen.

Wohl aus diesem Grund erkannten Gesetzgeber, dass das Speichern von Telekommunikationsdaten eine wichtige Rolle bei der Verhinderung und Verfolgung von Straftaten spielt.

Technisch gesehen, kann man davon ausgehen, dass die Gesetzgeber den Herausforderungen der Telekommunikations- und Computerforschung schrittweise nachkommen können. In den letzten Jahren wurden immer strengere staatliche

[1] https://www.europol.europa.eu/newsroom/news/2017-eu-terrorism-report-142-failed-foiled-and-completed-attacks-1002-arrests-and-142-victims-died

Kontrollen eingesetzt, jedoch wird die Art und Weise dieser Kontrollen häufig gesetzlich verändert.

Kurz vor ihrer Einführung erklärte das Oberverwaltungsgericht Münster am 22. Juni 2017 die Regelung der Vorratsdatenspeicherung in Deutschland für nicht mit EU Recht vereinbar.

Das Gesetz zur Vorratsdatenspeicherung aus dem Jahr 2015 beinhaltete ab dem 1. Juli 2017 die Pflicht für die Telekommunikationsdienste, die Verkehrs- und Standortdaten für eine begrenzte Zeit von 10 Wochen auf Vorrat zu speichern.[2]

Anlässlich dieser Entscheidung können Telekommunikationsunternehmen ab dem 1. Juli nicht mehr verpflichtet werden, Telefon- und Internetverbindungsdaten aller Bürger zehn Wochen lang speichern zu müssen.

Wie kam es zu dieser Entscheidung?

Die Geschichte der Datenspeicherung begann in den Vereinigten Staaten von Amerika. Im Jahre 1965 unter der Regierung von John F. Kennedy schlug eine Kommission der Yale Universität vor, eine nationale Datenbank zu errichten. Dem Plan nach sollte diese die Daten der amerikanischen Bürger zusammenführen und über jeden der Bürger einen Datensatz anlegen. Hierdurch sollten die einzelnen US-Behörden Zugriff zu den Daten der Bürger „von der Geburt bis zum Tod" erhalten und auf einen umfassenden Lebenslauf der Staatsbürger zugreifen können.[3]

Die Frage, inwieweit eine solche Datenbank die Grundrechte der Bürger verletzt, hat in der amerikanischen Öffentlichkeit heftige Diskussionen ausgelöst. Der Kongress versagte dem Vorhaben die notwendige Zustimmung, nachdem die Öffentlichkeit gesetzliche Grundlagen für die Verarbeitung personenbezogener Daten gefordert hatte.[4] Die Menschen befürchteten, dass mit einem solch unbeschränkten Zugang zu personenbezogenen Daten ihre Privatsphäre beeinträchtigt werden könnte und sich die Überwachung auch auf Intimbereiche der privaten Lebensführung erstrecken könnte. Hierbei wurde auch die Nutzung von Computern durch die Bevölkerung zunehmend kritisch diskutiert, da in dieser Hinsicht ein unbemerkter staatlicher Datenzugriff befürchtet wurde. Die Erkenntnis, dass die Entwicklung der technischen Geräte nicht mehr aufzuhalten war, führte zur Ausarbeitung von umfassenden Datenschutzregelungen.

Festgestellt werden kann insoweit, dass schon vor der zwingenden Koppelung des Begriffs „Datenschutz" mit der Computertechnologie in den meisten Ländern Datenschutzvorschriften existierten. Hierzu zählen das Berufsgeheimnis, das Steuergeheimnis, das Fernmeldegeheimnis, das Statistikgeheimnis, das Sozialgeheimnis, das Brief- und Postgeheimnis usw. Unter den Segmenten des Datenschutzes hat aber das Arztgeheimnis die älteste Tradition, da es im Eid des

---

2 http://www.ovg.nrw.de/behoerde/presse/pressemitteilungen/36_170622/index.php

3 Marie Theres Tinnefeld – Helga Tubies: *Datenschutzrecht.* München, Oldenbourg, 1989. 1.

4 James Martin – Adrian Normann: *Halbgott computer.* München, Oldenbourg, 1942. 262.

Hippokrates vorgeschrieben wurde.[5] Hiernach ist der Arzt verpflichtet, über die Patientendaten Stillschweigen zu wahren: *„Was ich bei der Behandlung oder auch außerhalb meiner Praxis im Umgange mit Menschen sehe und höre, das man nicht weiterreden darf, werde ich verschweigen und als Geheimnis bewahren.“*[6]

2. Die Entstehung des Datenschutzes in Deutschland

Da die oben genannten Regelungen den Datenschutz nur in einigen ausgewählten Bereichen regeln, hat sich die Bundesregierung entschieden, eine lückenfüllende Regelung für die Informationsverarbeitung von Daten des Bürgers in der Wirtschaft und der öffentlichen Verwaltung zu schaffen. Im Jahre 1970 hat das Bundesministerium des Innern die Universität Regensburg beauftragt, ein Konzept für ein Bundesdatenschutzgesetz auszuarbeiten. 1971 wurde das Gutachten „Grundfragen des Datenschutzes“[7] erstellt. Die Ausgangsthese lautete: *„Datenschutz ist die Kehrseite der Datenverarbeitung. Wo Datenverarbeitung, da Datenschutz. Wie der Schatten notwendig dem Licht folgt, und ohne Licht kein Schatten bestehen kann, so begleitet Datenschutz die Datenverarbeitung.“*[8]

Die Datenschutzgesetze des Bundes und der Länder regeln den Umgang mit personenbezogenen Daten.

2.1. Landesdatenschutzgesetze

Das erste Datenschutzgesetz in Deutschland (und auch in der Welt) war das Datenschutzgesetz des Landes Hessen, das unter Ministerpräsident Albert Oswald verkündet wurde und am 13. Oktober 1970 in Kraft trat. Im Jahre 1971 wurde erstmals ein „Datenschutz-Beauftragter“ angewiesen, die behördlichen Daten vor unberechtigtem Zugriff und die Bürger vor staatlichem Missbrauch bei der Datenverarbeitung zu schützen. Albert Oswald betonte: *„Diese Einrichtung gibt es erstmals in der Bundesrepublik, und auch aus dem Ausland ist mir keine gleichartige Regelung bekannt.“*[9] Im hessischen Datenschutzgesetz wurden erstmals konkrete Datenschutzmaßnahmen bestimmt. Diese gesetzlichen Restriktionen banden fortan die Landesbehörden im Rahmen der Datennutzung.[10]

---

5 Tinnefeld–Tubies aaO. 3.

6 Charles Lichtenthaeler: *Der Eid des Hippokrates, Ursprung und Bedeutung.* Köln, Deutscher Ärzte-Verlag, 1984. 3.

7 Wilhelm Steinmüller*: Grundfragen des Datenschutzes, Gutachten.* Berlin, BT-Drucksache VI/3826 vom 7.9.1972., 1971. 1.

8 Steinmüller aaO. 34.

9 http://www.spiegel.de/spiegel/print/d-43176393.html

10 http://erdbeerfleisch.de/wp-content/uploads/2011/07/W%C3%A4hnert-Geschichte_des_Datenschutzrechts.pdf 2.

Das zweite Datenschutzgesetz erließ nach Hessen das Bundesland Rheinland-Pfalz 1974.[11] Bis 1981 folgten auch alle anderen Bundesländer dem hessischen Vorbild und verabschiedeten Landesdatenschutzgesetze und setzten Datenschutz-Beauftragte ein.

Das hessische Datenschutzgesetz wurde insgesamt dreimal novelliert. Die erste Novellierung trat 1978 in Kraft und entstand vor dem Hintergrund der Diskussionen um das Bundesdatenschutzgesetz. Im Jahre 1986 wurde das Gesetz wegen des Volkszählungsurteils und des Rechts auf informationelle Selbstbestimmung reformiert. Der Grund der letzten Novellierung war die Umsetzung der EG-Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995.[12]

2.2. Bundesdatenschutzgesetz

Im Jahre 1977 wurde beschlossen, ein „brauchbares Bundesdatenschutzgesetz" zu erlassen.[13] Das Bundesdatenschutzgesetz trat am 1. Januar 1978 in Kraft und hat sich den Schutz vor Missbrauch zum Ziel gesetzt. Das Bundesdatenschutzgesetz beruht auf dem Gedanken des Persönlichkeitsschutzes, wurde von den Organen der Gesetzgebung aber auch als Reaktion auf die Informationstechnik verstanden. Gemäß § 1 Abs. 1 BDSG i.d.F.v. 1977 ist es Ziel des Datenschutzes, dass *„den Schutz personenbezogener Daten von Missbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) sicherzustellen sowie der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken."* Der Fokus des BDSG i.d.F.v. 1977 richtete sich damals aber weniger auf den Schutz von Daten vor Missbrauch, sondern vielmehr auf den Schutz der Individuen vor Gefahren und Schäden, die bei einem unangemessenen Umgang mit Informationen entstehen.[14]

Das BDSG wurde mehrfach durch verschiedene Novellierungen verändert. Die nachfolgenden Änderungen sind Folge des sich verändernden Verständnisses des Datenschutzes in Zeiten der Informationstechnologie und maßgebend für die Entwicklung des Datenschutzes.

Das BDSG wurde nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 geändert. Am 31. Mai 1990 verabschiedete der Bundestag das „Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes". Dieses wurde aber vom Bundesrat abgelehnt. Daraufhin wurde ein neuer Gesetzesentwurf erarbeitet, so dass das novellierte Bundesdatenschutzgesetz am 1. Juni 1991 schließlich doch in Kraft treten konnte. In dieser Novelle wurde das Ziel des Datenschutzes dem vom Bundesverfassungsgericht abgeleiteten Grundrecht entsprechend modifiziert. Das primäre Anliegen des Gesetzes war demnach nicht mehr der Schutz vor Missbrauch,

---

[11] Peter Gola – Rudolf Schomerus*: Bundesdatenschutzgesetz Kommentar.* München, C.H. Beck, 2012. 57.

[12] http://erdbeerfleisch.de/wp-content/uploads/2011/07/W%C3%A4hnert-Geschichte_des_Datenschutzrechts.pdf 7.

[13] Frank Haenschke: *Modell Deutschland? Die Bundesrepublik in der technologischen Krise.* München, Reinbek, 1977. 146.

[14] Hans Peter Bull: *Ziele und Mittel des Datenschutzes.* Königstein im Taunus, Athenäum, 1981. 24.

sondern deutlich mehr der Schutz vor Beeinträchtigung des Persönlichkeitsrechts.[15] Umgesetzt wurden auch die anderen Vorgaben des Bundesverfassungsgerichts, wie zum Beispiel die Zweckbindung der erhobenen Daten oder das Verbotsprinzip mit Erlaubnisvorbehalt.[16]

Das Bundesdatenschutzgesetz wurde ab dem Jahr 2009 insgesamt durch drei Novellen überarbeitet. In diesen Novellen sind einige wichtige Vorschriften des Bundesdatenschutzgesetzes bereits als Spezialregelungen zu den allgemeinen Grundsätzen ausgestaltet worden.[17]

3. Das Datenschutzrecht in der Europäischen Union

Nicht nur die nationalen Gesetzgeber hatten die Pflicht, auf dem Gebiet des Datenschutzes tätig zu werden. Die Europäische Union musste auch zahlreiche datenschutzrechtliche Fragen beantworten. Bereits 1976 hat das Europäische Parlament die EU-Kommission aufgefordert, eine EU-Datenschutzrichtlinie zu erstellen.[18]

3.1. Die Datenschutzregelungen in der Europäischen Union bis zur Verabschiedung der Richtlinie 95/46/EG

Es dauerte fast 20 Jahre, bis die Richtlinie 95/46/EG verabschiedet werden konnte. Im Jahre 1995 wurde die Richtlinie der Europäischen Gemeinschaft zum *„Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr"*[19] erlassen. Auch in Deutschland kam es bei der Umsetzung der Richtlinie zu Verzögerungen: Innerhalb von drei Jahren sollten die Mitglieder der Europäischen Union die Datenschutzvorschriften umsetzen. Das novellierte Datenschutzgesetz der Bundesrepublik trat jedoch erst am 23. Mai 2001 in Kraft.

Auch die Charta der Grundrechte der Europäischen Union beinhaltet wesentliche Regelungen hinsichtlich des Datenschutzes: *„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation"* (Artikel 7) und *„Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten."* (Artikel 8).[20] Es wurde zudem eine neue Rechtsgrundlage für die Schaffung einer umfassenden und kohärenten Regelung der Europäischen Union zum Schutz

---

15 https://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript%20Internetrecht_April_2016.pdf. 390.

16 http://erdbeerfleisch.de/wp-content/uploads/2011/07/W%C3%A4hnert-Geschichte_des_Datenschutzrechts.pdf 8.

17 Hans Peter Bull: *Informationelle Selbstbestimmung- Vision oder Illusion?* Tübingen, Mohr Siebeck, 2009. 29.

18 Hoeren aaO. 391.

19 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

20 Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000.

natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr geschaffen.[21]

Die europäischen Entscheidungsgremien haben sich Anfang der 2000er Jahre für den Bereich der Infokommunikation zum Ziel gesetzt, die Voraussetzungen für die technologische Entwicklung und den Markt zu erfüllen.[22] Die Datenschutzrichtlinie 95/46/EG der Europäischen Union wurde im Jahr 2002 durch die „Datenschutzrichtlinie für elektronische Kommunikation" ergänzt.[23] Die Mitgliedstaaten wurden hierbei verpflichtet, Datenschutzregelungen für die Telekommunikation zu verabschieden. Diese Richtlinie beinhaltet bezüglich der Richtlinie 95/46/EG spezielle Vorschriften, die nur in der elektronischen Kommunikation anwendbar sind. Soweit die Richtlinie in einigen Fällen keine spezielle Regelung vorschreibt, findet die allgemeine Datenschutzrichtlinie unverändert Anwendung.[24] Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ermöglicht, den Mitgliedstaaten einen einheitlichen Rahmen für die Aufbewahrung von Daten vorzugeben. Diese Aufgabe wurde an die Mitgliedstaaten delegiert (Umsetzung mittels einer Richtlinie anstatt durch eine Verordnung), weshalb innerhalb der Europäischen Union unterschiedliche – richtlinienkonforme – Ausgestaltungen existieren.[25]

In Deutschland wurde die Richtlinie im Jahre 2004 durch eine Novellierung des Telekommunikationsgesetzes umgesetzt.[26] In Ungarn wurden die Vorgaben bereits 2003 im Gesetz Nr. C. über die elektronische Kommunikation, das am 27. November 2003 in Kraft trat, umgesetzt.[27]

3.2. Die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten

Die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten ist eine Reaktion der Europäischen Union auf die Terroranschläge von New York, Madrid und London. Als Konklusion regte die Europäische Union mit dieser Richtlinie an, alle Telekommunikationsverbindungsdaten der Europäer zu speichern, um diese den Ermittlungsbehörden zur Verfügung zu stellen.[28] Die Anschläge haben gezeigt, dass eine erfolgreiche Strategie gegen den internationalen Terrorismus auch eine

---

21 Hoeren aaO. 391.

22 Anett Karner: Die Pflichten der Mobilanbieter im Bereich des Datenschutzes, insbesondere die Zusammenarbeit mit den Strafverfolgungsorganen. *Infokommunikáció* és *Jog,* 2012. Sept. 139.

23 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

24 Karner aaO. 139.

25 Péter Szabolcsi: Die Pflicht von Aufbewahrung von Daten für Strafverfolgungszwecke im Zusammenhang mit dem EU Recht. Die Implementierung der Richtlinie 2006/24/EG. *Európai Jog,* 2012/3. 1.

26 http://erdbeerfleisch.de/wp-content/uploads/2011/07/W%C3%A4hnert-Geschichte_des_Datenschutzrechts.pdf 9.

27 Szabolcsi aaO. 1.

28 Felix Rettenmeyer – Lisa Palm: Vorratsdatenspeicherung,Bestandsaufnahme und Ausblick. *Zeitschrift für Internationale Strafrechtsdogmatik,* 8–9/2012. 469.

moderne Kommunikationsstrategie beinhalten sollte. Den Strafverfolgungsbehörden der Mitgliedstaaten müssen die entsprechenden Mittel zur Verfügung stehen, um technologisch eine effektive Gefahrenabwehr sicherzustellen.

Es wurde lange diskutiert, ob und inwieweit der Rat der Europäischen Union die Mitgliedstaaten durch einen Rahmenbeschluss zur Vorratsspeicherung von Telekommunikationsdaten verpflichten kann.[29] Vorgeschlagen wurden eine europaweit einheitliche Speicherung von Verbindungs- und Verkehrsdaten im Rahmen der justiziellen Zusammenarbeit in der sogenannten "dritten Säule" der Europäischen Union.[30] Der vorgelegte Entwurf erreichte jedoch die erforderliche Einstimmigkeit nicht, so dass an dieser Stelle eine Richtlinie erlassen wurde, deren Annahme lediglich eine qualifizierte Mehrheit im Mitentscheidungsverfahren erforderte.[31]

Ziel des Vorschlages war die Entschärfung einzelner Regelungen. So sollte z. B. die Speicherfrist erheblich reduziert, die Verwendung der gespeicherten Daten begrenzt, datenschutzrelevante Regelungen eingeführt und der Zugriff auf Daten limitiert werden. Am 14. Dezember 2005 wurde der Richtlinie 2006/24/EG zugestimmt.[32]

Im Mai 2006 erhoben Irland und die Slowakei vor dem Europäischen Gerichtshof Klage gegen die Richtlinie. Ihrer Auffassung nach hätte man die Richtlinie als Rahmenbeschluss erlassen sollen. Auch der Deutsche Bundestag hatte bezüglich der angewandten Grundlagen Bedenken. Diese wurden durch ein Urteil des EuGH[33] bestätigt, in dem der Gerichtshof den Beschluss zur Weitergabe der Daten wegen fehlender Rechtsgrundlage für nichtig erklärte. Der Bundestag hat einen Antrag zur Prüfung der Richtlinie durch den EuGH in seiner Sitzung vom 20. Juli 2006 abgelehnt.[34]

Der wesentliche Inhalt der Richtlinie ist, dass Daten zwischen 6 bis maximal 12 Monaten gespeichert werden dürfen. Es wurden auch verschiedene Kategorien von auf Vorrat zu speichernden Daten erstellt. Die Mitgliedstaaten sollen sicher stellen, dass nach diesen Regelungen die vorgeschriebenen Datenkategorien auf Vorrat gespeichert werden. Hierzu gehören insbesondere Telefonfestnetz und Mobilfunk, Internetzugang, Email und Internet-Telefonie. Die Richtlinie beinhaltet auch Regelungen bezüglich Datenschutz und Datensicherheit. Die Mitgliedstaaten sollen sicher stellen, dass eine oder mehrere öffentliche Stellen für die Kontrolle des Datenschutzes zuständig sind.

4. Datenschutzgesetze in Deutschland

Die Gesetzgebungskompetenz des Bundes wird nach dem Grundgesetz in zwei Kategorie anordnet. Die erste ist nach Art. 71, 73, 105 Abs. 1 GG die ausschließliche Bundesgesetzgebung. Die zweite ist nach Art. 72, 74, und 105 Abs. 22 GG die

---

29 Alexander Alvaro: Die Richtlinie zur Vorratsdatenspeicherung. *Datenschutz Nachrichten,* 2/2006. 52.

30 Rudolf Streinz: *Europarecht.* Heidelberg, C. H. Beck, 2012. 498.

31 Gabriela Sierck – Frank Schöning – Matthias Pöhl: Zulässigkeit der Vorratsdatenspeicherung. *Wissenschaftliche Dienste,* 3-282/06. Berlin, 2006. 7.

32 Alvaro aaO. 52.

33 C-31704 C-318/04 Urteil des EuGH vom 30. Mai 2006 zur Weitergabe von Fluggastdaten an die USA.

34 Ibid.

konkurrierende Bundesgesetzgebung. Unter konkurrierender Gesetzgebung versteht man, dass die Länder die Gesetzgebungsbefugnis haben, solange und soweit der Bund von seiner Gesetzgebungszuständigkeit nicht durch Gesetz Gebrauch gemacht hat. Nach Art. 72 Abs. 1 GG hat der Bundesgesetzgeber den Vorrang. Wenn er eine Materie regelt, schließt er automatisch die Zuständigkeit der Länder aus. Die Gesetzgeberischen Regelungen über Informationssysteme im privaten Bereich fallen in das „Recht der Wirtschaft" (Art. 74 Nr. 11 GG). Zur Wahrung einer einheitlichen Ordnung im Wirtschaftsleben (Art. 72 Abs. 2 Nr. 3 GG) hat der Bundesgesetzgeber den Datenschutz für diesen Rechtsbereich bundeseinheitlich geregelt.[35]

4.1. Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz gilt für die Bundesrepublik Deutschland und regelt den Umgang mit personenbezogenen Daten, und deren Verarbeitung. Einbezogen sind in den Datenschutz sowohl die elektronische, als auch die manuelle Verarbeitung von Daten.

§ 39 des Bundesdatenschutzgesetzes regelt die Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

Durch Abs. 2 wird darauf hingewiesen, dass eine Verarbeitung der Daten für einen anderen Zweck zulässig ist, wenn dies durch ein besonderes Gesetz zugelassen ist. Hierzu gehört die Verpflichtung der Telekommunikationsdienstleister zur Vorratsspeicherung der Kommunikationsdaten und die Herausgabepflicht an die Sicherheitsbehörden.[36]

4.2. Telekommunikationsgesetz

Das Telekommunikationsgesetz hat sich zum Ziel gesetzt, „durch technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten" (§ 1 TKG).

Die Richtlinie 2006/24/EG wurde in dem Telekommunikationsgesetz durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 umgesetzt und trat am 1. Januar 2008 in Kraft.

Nach § 113a TKG sollten die Telekommunikationsdienstleister die Verkehrsdaten sechs Monate lang speichern, § 113b hat vorgeschrieben, zu welchen Zwecken die gespeicherte Daten verwendet werden dürfen.

Neulich sind in Deutschland Telekommunikationsanbieter seit 2015 gesetzlich verpflichtet, Daten bis zu zehn Wochen aufzubewahren. Darauf sollen Ermittler bei der Bekämpfung von Terror und schweren Verbrechen zugreifen können. Dieses muss bis zum 1. Juli 2017 abgeschlossen sein.

---

35 Tinnefeld–Tubies aaO. 17.

36 Gola–Schomerus aaO. 742.

Gespeichert werden in Deutschland etwa Rufnummern, sowie Zeitpunkt und Dauer von Anrufen. Beim Surfen im Internet werden IP-Adressen, sowie Details zu deren Vergabe vorgehalten. E-Mails sind ausgenommen.

4.3. Datenschutz und Verfassungsrecht

Das Bundesverfassungsgericht in Deutschland wurde nach der Rechts- und Verfassungsverwüstung in der Zeit des Nationalsozialismus 1949 im Grundgesetz eingefügt worden. Das Gericht hat seine Arbeit 1951 angefangen, und hat durch seine Rechtsprechung zu den Grundrechten großen Einfluss auf die Entwicklung des demokratischen Rechtsstaats ausgeübt.[37]

Der Datenschutz beruht auf dem Grundgesetz für die Bundesrepublik Deutschland, insbesondere basiert es im Wesentlichen auf zwei Säulen. Die eine bildet der Grundsatz der Gewaltenteilung und der Gesetzmäßigkeit der Verwaltung. Die zweite bilden die Persönlichkeitsrechten der Art. 2 GG.

Das Grundrecht auf informationelle Selbstbestimmung wurde vom BVerfG aus der Art 1, 2 GG (allgemeine Persönlichkeitsrecht) abgeleitet. Den Begriff „Recht auf informationelle Selbstbestimmung“ wurde in einem Gutachten von 1972 verwendet.[38]

4.4. Urteil zur Vorratsdatenspeicherung vom 2. März 2010

Der Deutsche Bundestag hat am 9. November 2007 den Entwurf zur Einführung des Gesetzes über die Vorratsdatenspeicherung in Deutschland beschlossen. Am 31. Dezember 2007 wurde eine Verfassungsbeschwerde beim Bundesverfassungsgericht gegen das Gesetz eingereicht. Die Beschwerde wurde im Namen von acht Erstbeschwerdeführern und am 29. 02. 2008 im Namen rund 34.000 Beschwerdeführer eingereicht. In der Verfassungsbeschwerde wurde beantragt, das Gesetz bis zur Entscheidung des Bundesverfassungsgerichts außer Kraft zu setzen.[39] Die Verfassungsbeschwerde wurde gegen die §§ 113a, 113b des Telekommunikationsgesetzes in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG[40] eingereicht.

Im Antrag haben die Beschwerdeführer die Verletzung des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung (Artikel 10 Abs. 1 Var. 3 GG und Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG), der Berufsfreiheit (Artikel 12 Abs. 1 GG), der Eigentumsgarantie (Artikel 14 Abs. 1 GG), der Meinungsfreiheit, der Informationsfreiheit, der Rundfunkfreiheit und der Pressefreiheit (Artikel 5 Abs.

---

37 Marie Therese Tinnefeld – Benedict Buchner – Thomas Petri: *Einführung in das Datenschutzrecht*. München, Walter de Gruyter, 2012. 120.

38 Steinmüller aaO. 83.

39 http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html.

40 https://dejure.org/BGBl/2007/BGBl._I_S._3198

1 GG) sowie die Verletzung des allgemeinen Gleichheitssatzes (Artikel 3 Abs. 1 GG) behauptet.[41]

Das Bundesverfassungsgericht hat in seinem Urteil[42] die § § 113a und 113b des Telekommunikationsgesetzes und auch der § 100g Abs. 1 S. der Strafprozessordnung für verfassungswidrig und nichtig erklärt, da es in seiner jetzigen Fassung gegen Art.10 Abs. 1. des Grundgesetzes verstößt. Die bisher gespeicherten Daten seien sind unverzüglich zu löschen.[43] Zur Begründung wurde in der Entscheidung ausgeführt, dass eine solche Speicherung ein schwerwiegender Eingriff begründet, und dass die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, die belastende Wirkung verschärfen können. Insgesamt wurde festgestellt, dass „die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.“[44] Aus der Sicht des Bundesverfassungsgerichts ist der Ansatz der Vorratsdatenspeichrung nicht grundsätzlich unvereinbar mit den Regelungen des Grundgesetzes. Es handelt sich um einen besonders schweren Eingriff, den die Rechtsordnung bisher nicht kennt. Die Speicherung für die Dauer von sechs Monaten muss die zeitliche Obergrenze darstellen, und die Speicherung soll mit einem Begründungsauftrag verbunden sein. Die Daten sollen insbesondere nicht anlasslos, sondern ausschließlich zur Strafverfolgung genutzt werden können.[45] Nach der Entscheidung des Bundesverfassungsgerichts ist in Deutschland nicht gestattet, ohne Anlass auf Vorrat Daten zu speichern, weil die Gesetzgrundlage für nichtig erklärt wurde.

Im Januar 2011 wurde ein Eckpunktepapier von Bundesjustizministerin Sabine Leutheusser-Schnarrenberger veröffentlicht, die einen Lösungsansatz vorschlug, der eine unterschiedslose Speicherung der Daten aller Bürger in Deutschland vermeiden sollte. Nach dem Vorschlag sollten die Telekommunikationsunternehmen die bereits vorhandenen Verkehrsdaten aus geschäftlichen Gründen den Strafverfolgungsbehörden unter Richtervorbehalt für eine begrenzte Zeit zur Verfügung stellen. Die Speicherungsdauer sollte strikt auf das notwendige Maß beschränkt bleiben und sollte sieben Tage auf Vorrat gespeichert werden. Die Daten sollten unverzüglich gelöscht werden, sobald die Sicherungsfrist abläuft.

Der Wissenschaftliche Dienst des Deutschen Bundestages hat eine Ausarbeitung zur Vereinbarkeit der Richtlinie über die Vorratsdatenspeicherung von Daten mit der Europäischen Grundrechtcharta verfertigt. In diesem Gutachten entstand das folgende Ergebnis: „An der Vereinbarkeit der Richtlinie 2006/24/EG mit der

---

41 http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html

42 http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html.

43 Moritz Tremmel: *Die Vorratsdatenspeicherung und der Panopzismus. Anwendbarkeit und Erkenntnisse aus der Analyse der Vorratsdatenspeicherung mit Foucaults Machttheorie.* Tübingen, Studienarbeit, 2010. 6.

44 http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html. 212.

45 Rettenmayer–Palm aaO. 469.

von ihr vorgesehenen Verpflichtung zur anlasslosen Vorratsdatenspeicherung mit dem gemeinschaftsrechtlichen Grundsatz der berufs- und wirtschaftlichen Betätigungsfreiheit bestehen Zweifel".[46]

2013 wurde in Luxemburg ein Rechtsgutachten[47] am Europäischen Gerichtshof über die Vorratsdatenspeicherung veröffentlicht. Das Rechtsgutachten stellte fest, die Vorratsdatenspeicherung verstöße gegen EU-Grundrechte. „Art. 6 der Richtlinie 2006/20/EG [die Regelungen über den Speicherungsfrist] ist mit den Art. 7 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union unvereinbar, soweit er den Mitgliedstaaten vorschreibt, sicherzustellen, dass die in ihrem Art. 5 genannten Daten für die Dauer von bis zu zwei Jahren auf Vorrat gespeichert werden."[48]

4.5. Datenschutz im Strafrecht

Die neuen Entwicklungen im Wirtschaftsleben haben auch im Bereich des Strafrechts neue Herausforderungen generiert. Hierzu gehört der verstärkte Einsatz der Datenverarbeitung, die vorher nicht bekannte Kriminalitätsformen hervorgebracht hat, mit denen das Strafrecht schritthalten musste. Es sind bei der Bekämpfung der Wirtschaftskriminalität in verschieden Bereichen Gesetzeslücken entstanden. Das führe zur Entstehung von Tatbeständen bestimmter Formen der Computerkriminalität.[49] Die Straftaten bezüglich der Daten sind im Strafgesetzbuch im Fünfzehnten Abschnitt „Verletzung des persönlichen Lebens- und Geheimbereichs" erfasst. Die Straftaten sind: Ausspähen und Abfangen von Daten und Vorbereiten des Ausspähens und Abfangens von Daten.

5. Die Entscheidung des Gerichtshofs der Europäischen Union vom 8. April 2014 (C-293/12 und C-594/12)

Der Gerichtshof der Europäischen Union hat ein entscheidendes Urteil bezüglich der Vorratsdatenspeicherung erlassen. In seinem Urteil hat der Gerichtshof die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten (Große Kammer, 8. April 2014) für ungültig erklärt.

In der Rechtsache C- 293/12 wurde eine Klage vor dem irischen High Court erhoben, in deren Rahmen die Eigentümerin eines Mobiltelefons die Rechtsmäßigkeit nationaler legislativer und administrativer Maßnahmen zur Vorratsspeicherung von Daten in Frage stellte. Der High Court hat das Verfahren ausgesetzt und wandte sich an den Gerichtshof mit Fragen bezüglich der Richtlinie 2006/24/EG zur Vorabentscheidung. Die Fragen richteten sich darauf, ob die Regelungen der Richtlinie mit den durch

---

46 Roland Derksen: Zur Vereinbarkeit der Richtlinie über Vorratsdatenspeicherung von Daten mit der Europäischer Grundrechtcharta. *Wissenschaftliche Dienste,* 18/2011. 21.

47 http://curia.europa.eu/juris/document/document.jsf?docid=161370&doclang=DE.

48 http://curia.europa.eu/juris/document/document.jsf?docid=161370&doclang=DE.

49 http://dipbt.bundestag.de/doc/btd/10/050/1005058.pdf 28.

die Charta der Grundrechte der Europäischen Union gewährleisteten Grundrechten vereinbar sind.

In der Rechtsache C-594/12 wurde den Gerichtshof vom österreichischen Verfassungsgericht zur Vorabentscheidung ersucht. Es wurden beim Verfassungsgericht von der Kärntner Landesregierung und 11.130 von weiteren Antragstellern Anträge bezüglich der Umsetzung der Richtlinie 2006/24/EG vorgelegt. Die Antragsteller waren der Ansicht, dass § 102a des Telekommunikationsgesetztes in Österreich das Grundrecht der Staatsbürger auf Schutz ihrer Daten verletzt. Das Verfassungsgericht hat zur Vorabentscheidung Fragen gestellt, inwiefern die Richtlinie mit der Charta vereinbar sei.

Das Urteil wurde in den verbundenen Rechtsachen von (C-293/12 und C-594/12 erlassen.

Der Gerichtshof hat festgestellt, dass die Verpflichtung zur Vorratsspeicherung von Daten und die Gestattung des Zugangs der zuständigen nationalen Behörden ein besonders schwerwiegender Eingriff in das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten sind. Die Vorratsspeicherung von Daten, ohne dass die Teilnehmer darüber wussten, war geeignet, bei den Betroffenen das Gefühl hervorzubringen, ständig beobachtet zu werden.

Die Richtlinie mit dem Vorschreiben der Vorratsspeicherung von Daten hat eine Zielsetzung dargestellt, die dem Gemeinwohl dient, und zwar der Bekämpfung schwerer Kriminalität. Das Gericht hat festgestellt, dass die Richtlinie geeignet ist, um das verfolgte Ziel zu erreichen. Es wird aber nicht gewährleistet, dass sich der Eingriff tatsächlich auf das absolut notwendige beschränkt. Die Richtlinie erstreckt sich generell auf alle Personen, die elektronische Kommunikationsdienste nutzen, und auf sämtliche Verkehrsdaten ohne Differenzierung, Einschränkung oder Ausnahme. Außerdem sieht die Richtlinie kein objektives Kriterium vor, welches es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung auf Straftaten zu beschränken, die die Schwere des Eingriffs in die Art. 7 und Art. 8 der Grundrechtscharta rechtfertigen.

Das Gericht findet die Speicherungsfrist von mindestens 6 Monaten fragwürdig, weil es nicht zwischen den verschiedenen Datenkategorien nach Maßgabe des Nutzens oder anhand der betroffenen Personen differenziert wird. Die Festlegung der Speicherungsfrist sollte auf objektive Kriterien beruhen, die gewährleisten, dass sie auf das absolut Notwendige beschränkt werden. Darüber hinaus stellt der Gerichtshof fest, dass die Richtlinie keine hinreichenden Garantien beinhaltet, dass die Daten wirksam vor Missbrauchsrisiken, sowie vor jedem unberechtigten Zugang geschützt sind. Es wird auch nicht gewährleistet, dass die Daten nach dem Ablauf der Speicherungsfrist unwiderruflich vernichtet werden.

Der Gerichtshof bemängelt auch, dass die Richtlinie die Speicherung auf Vorrat von den Daten nicht auf Unionsebene vorschreibt, wodurch es nicht als vollumfänglich gewährleistet angesehen werden kann, dass die Einhaltung der Vorschriften des Datenschutzes durch eine unabhängige Stelle überwacht sind.

6. Die Entscheidung des Gerichtshofs der Europäischen Union vom 21. Dezember 2016 (C-203/15)

Mit seinem Urteil hat der Gerichtshof die Richtlinie von 2014 über der Vorratsspeicherung von Daten für ungültig erklärt und untersagte eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortsdaten. Die Mitgliedsstaaten dürfen aber gezielte Vorratsdatenspeicherung führen, zum alleinigen Zweck der Bekämpfung schwerer Kriminalität, sofern die Speicherung auf das absolut Notwendige beschränkt ist.

In Bezug auf die Vorratsspeicherung stellt der Gerichtshof fest, dass aus den gespeicherten Daten zahlreiche personenbezogene Daten erkennbar sind, was als besonders schwerwiegender Grundrechtseingriff gilt. Der Umstand, dass verschiedene Daten gespeichert werden, ohne dass die Nutzer elektronischer Kommunikationsdienste darüber informiert werden, kann das Gefühl geben, das man ständig überwacht ist. Der Gerichtshof meint deshalb, dass allein die Bekämpfung schwerer Straftaten eine solche Grundrechtsangriff nicht rechtfertigen.[50]

7. Die Entscheidung des Gerichtshofs der Europäischen Union vom 6. Oktober 2015 in der Rechtssache C-362/14 (Schrems)

In dem Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14 (Schrems) hat der Gerichtshof der Europäischen Union bestätigt, dass das in der EU-Grundrechtecharta verankerte Grundrecht auf den Schutz personenbezogener Daten, und die Übermittlung solcher Daten in Drittstaaten ein angemessenes Schutzniveau erreichen muss.

Der Anlass dieses Urteils war die sog. Safe-Harbor-Entscheidung[51] der Kommission vom 20. Juli 2000 (2000/520/EG), in der die Kommission anerkannte, dass die Vereinigten Staaten im Rahmen der Safe-Harbor-Regelung ein angemessenes Schutzniveau der übermittelten personenbezogenen Daten gewährleisten. Aufgrund dieser Entscheidung konnten personenbezogene Daten aus EU-Mitgliedstaaten an Unternehmen in den Vereinigten Staaten übermittelt werden, obwohl es in den Vereinigten Staaten kein allgemeines Datenschutzgesetz gibt. Diese Kommissionsentscheidung wurde in dem Schrems-Urteil für ungültig erklärt, da die nationalen Datenschutzbehörden in der Lage sein müssen, in Unabhängigkeit prüfen zu können, ob bei der Übermittlung der Daten einer Person in ein Drittland die in der Richtlinie aufgestellten Anforderungen gewahrt werden.[52] Nach der EuGH Entscheidung wurde die *Datenschutzgruppe* gemäß *Artikel 29* der Richtlinie 95/46/EG eingesetzt, die vier wesentliche Garantien bei allen Übermittlungen personenbezogenen Daten aus der EU und andere Drittstaaten feststellte.[53]

---

50 https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145de.pdf

51 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:DE:HTML

52 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62014CJ0362

53 https://www.datenschutz-bayern.de/faq/FAQ-SafeHarbor-Art29-2.pdf

8. Fazit

In Ungarn enthält das Gesetz Nr. C. aus dem Jahre 2003 über die elektronische Kommunikation die Regelungen der Datenverarbeitung der Telekommunikationsanbieter. Hierzu gehören insbesondere die Verpflichtung zur Datenübertragung von dem Telekommunikationsdienstleister, die Art vom Datenschutz bei generellen Dienstleistungen und auch die Vorschriften für die Anwendung bei dem Telekommunikationsanbieter gespeicherten personenbezogenen Daten für Forschungszwecken. Durch das Gesetz Nr. CLXXIV. vom Jahre 2007 wurde das Gesetz über die elektronische Kommunikation bedeutsam verändert, es wurden die Klauseln zur Vorratsdatenspeicherung wegen der Umsetzung der Richtlinie 2006/24/EG in das ungarischen Datenschutzsystem eingeführt.

Große Änderung bringt das Jahr 2018 sowie in Ungarn, als auch in der EU, weil die Datenschutz-Grundverordnung [54] ab 25. Mai 2018 anzuwenden ist. Die Verordnung wird die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ersetzen. Wie alle Verordnungen, ist diese nicht in nationales Recht umzusetzen, sondern unmittelbar verbindlich.

Es wurden die bedeutenden juristischen Ereignisse und Gesetze der Entwicklung des Datenschutzes und der Vorratsdatenspeicherung vorgestellt. Wie es im Vorwort bereits angedeutet wurde, ist die Entscheidung des Oberverwaltungsgerichts Münster und des EUGH ein Rücktritt im Vergleich zu der früheren – strengeren – staatlichen Regelung.

Die Gewerkschaft der Polizei äußerte die Meinung, dass das Aussetzen der Vorratsdatenspeicherung den Kampf gegen den Terror deutlich erschweren werde. Falls die Ermittler nach einem Attentat nämlich nicht nach den Kommunikationsstrukturen der Täter nachgehen können, können Hintermänner und Unterstützer nicht verhaftet werden. [55]

Viele Parteien und Organisationen meinen, dass die Vorratsdatenspeicherung keine weiteren Attentate verhindert. Diese Meinung spiegelt sich auch in der Entscheidung des Oberverwaltungsgerichts Münsters wider.

Der Kampf gegen die Kriminalität ist ein rechtspolitisch und verfassungslegitim anerkannter, dem Gemeinwohl dienender Zweck. Dieser Zielsetzung stehen allerdings der Schutz der Individualsphäre und der Schutz von personenbezogenen Daten gegenüber. Die Abwägung der widerstreitenden Interessen ist eine juristische Herausforderung *(ars aequi)*. Zum Einen ist die Gesetzgebung stark motiviert durch internationale Geschehnisse (9/11, Kampf gegen den Terrorismus, Cyber-crime, Hacker-Attacken) und durch die Erwartungen der Bürger gegenüber einem effektiven Gewaltmonopol des Staates, zum Anderen wird jeglicher Eingriff in die Privatsphäre skeptisch betrachtet. Der EuGH bezeichnet diese Skepsis mit dem „Gefühl […] einer

---

[54] https://dsgvo-gesetz.de/

[55] https://www.gdp.de/gdp/gdp.nsf/id/DE_GdP-Aussetzen-der-Vorratsdatenspeicherung-wirft-Terrorismusbekaempfung-massiv-zurueck-?open&ccm=000.

ständigen Überwachung."[56] Edward Snowden mag diesem „Gefühl" einen Stoß gegeben haben.

Eine weitere, wichtige Frage lässt sich nicht umgehen. Führt die Vorratsspeicherung von Daten zum Orwellischen Staat? Die vorliegende Arbeit zeigt, dass die Antwort grundlegend im Spannungsfeld zwischen dem Schutz der Individualsphäre und dem Schutz von Rechtsgütern der Allgemeinheit zu finden ist. In dieser Hinsicht muss ein Äquilibrium zwischen den Rechtsgebieten Datenschutz, Strafrecht, Verfassungsrecht und EU-Recht hergestellt werden. Datenschutz steht für die informationelle Selbstbestimmung und ist ein Ausfluss der Menschenwürde. Strafrecht verkörpert den Rechtsgüterschutz des Staates als letztes Mittel *(ultima ratio)*, und ist demnach nur dann einzusetzen, wenn andere Sanktionsmöglichkeiten nicht mehr ausreichen. Verfassungsrecht umfasst die nationalen sozialethischen und politischen Werte des Staates und gewährt durch das Grundgesetz eine Rahmenordnung für die staatlichen System- und Werteentscheidungen. Durch übertragene Hoheitsrechte gemäß Art 23 I GG repräsentiert die EU einen überstaatlichen Kompetenzträger, dessen Hoheitsgewalt als rechtlich verbindlich zu akzeptieren und im deutschen Verfassungsraum zur Anwendung zu bringen ist.[57]

Die Arbeit wies darauf hin, dass die Vorratsspeicherung von Daten innerhalb der rechtsstaatlichen Grenzen möglich ist. Es wurde gezeigt, dass die verschiedenen Rechtsgebiete unterschiedliche rechtspolitische Ziele haben, die „harmonisiert", miteinander abgestimmt werden müssen. Nur so kann eine Mäßigung des Staates erreicht werden und zugleich der Wesensgehalt der Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten erhalten bleiben.

---

[56] https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145de.pdf.

[57] http://www.europawissenschaften-berlin.de/media/pdf/Publikationen/Nettesheim.pdf?1304502229, 36.