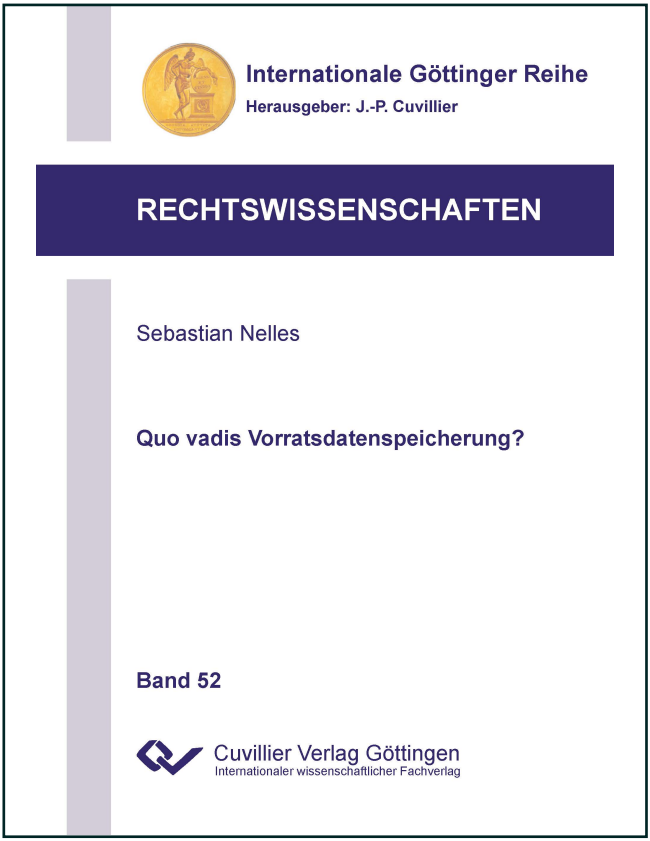
Sebastian Nelles (Autor)

Quo vadis Vorratsdatenspeicherung?



https://cuvillier.de/de/shop/publications/6671

Einleitung

In den 27 Mitgliedstaaten der Europäischen Union leben ca. 500 Millionen Menschen.[1] Für den Großteil dieser Menschen haben die modernen Kommunikationsmittel, wie Telefon, Handy und Internet, herausragende Bedeutung für ihren Alltag und sind daher so gut wie nicht mehr wegzudenken. Sie haben teilweise eine so zentrale Bedeutung, dass viele Menschen ritualartig jeden Tag mit dem Besuch des E-Mail-Accounts und der sozialen Netzwerke im Internet beginnen. Es ist daher unbestritten, dass ein herausragender Teil der schützenswerten Privatsphäre während der Kommunikation mit anderen Menschen auch über große Entfernungen stattfindet. Der Schutz dieses Bereiches vor der Öffentlichkeit ist Sinn und Zweck des Fernmeldegeheimnisses gem. Art. 10 Abs. 1 GG.[2] Um den modernen Ausprägungen des Persönlichkeitsrechts ausreichend Rechnung zu tragen, hat das Bundesverfassungsgericht aber bereits im sog. „Volkszählungsurteil“ vom 15. Dezember 1983 aus dem Allgemeinen Persönlichkeitsrecht und der Menschenwürde zusätzlich zum Fernmeldegeheimnis nach Art. 10 I GG das Recht auf informationelle Selbstbestimmung fortentwickelt.[3] Dieses gewährleistet, dass jedermann grundsätzlich nur die Daten von sich preisgibt, die er auch selber preisgeben möchte.[4] Durch die rasante Entwicklung des „Web 2.0“,[5] in deren Verlauf die sozialen Netzwerke immer mehr zusätzliche Nutzungsmöglichkeiten anbieten, verschwimmen die Grenzen zwischen freiwillig preisgegebenen Daten und solchen, die nicht öffentlich zugänglich gemacht werden sollen, mehr und mehr, da die sog. „Privatsphäre-Einstellungen“ in den sozialen Netzwerken zunehmend unübersichtlich und kompliziert werden. Folglich ist dem Fernmeldegeheimnis und dem Recht auf informationelle Selbstbestimmung, als Ausprägung des Allgemeinen Persönlichkeitsrechts, eine erhebliche Bedeutung in der modernen Kommunikationsgesellschaft beizumessen.

---

[1] Eurostat, Population on 1 January.
[2] Jarass/Pieroth, Grundgesetz Art. 10 Rn. 1.
[3] BVerfGE 65, 1 (41 ff.).
[4] Jarass/Pieroth, Grundgesetz Art. 2 Rn. 42; Epping/Hillgruber/*Lang*, Grundgesetz, Art. 2 GG Rn. 45.
[5] „**Web 2.0**“ ist ein Begriff, mit dem die neuen Nutzungsmöglichkeiten des Internet durch soziale Netzwerke und die sonstigen Möglichkeiten der Nutzer, sich aktiv am Gestalten von Internetseiten zu beteiligen, zusammengefasst werden sollen. Knor, CIO 12/2003.

Allerdings ist auch offensichtlich, dass die Grenzen dieser Freiheiten in den modernen Telekommunikationsausprägungen dort liegen, wo sie ausgenutzt werden, um die Rechte anderer zu beeinträchtigen. Bedauerlicherweise werden diese Rechte nämlich teilweise für die Begehung von Straftaten ausgenutzt. Einerseits bedienen sich Kriminelle weltweit des Mantels der Anonymität und der Eigendynamik von Massenkommunikationsmitteln im Internet, um die Unwissenheit von „normalen" Usern zur Begehung von Straftaten auszunutzen. So etwa bei den Begehungsformen des „Pharmings", „Phishings" oder „Keyloggings",[6] die zur Vorbereitung von Vermögensstraftaten jeden Tag weltweit vorgenommen werden. Andererseits nutzen Kriminelle die Anonymität im Internet insbesondere, um sich dem Zugriff der Strafverfolgungsbehörden in der Vorbereitungsphase zu den von ihnen ins Auge gefassten Straftaten zu entziehen. Daher bedienen sich parallel zur Ausbreitung der Internetkriminalität auch die Strafverfolgungsbehörden der EDV und des Internets als Ermittlungsmethode.[7] Allerdings ist es den Strafverfolgungs- oder Gefahrenabwehrbehörden aufgrund der unendlich groß erscheinenden Zahl von Kommunikationsmöglichkeiten im Internet schon quantitativ unmöglich, alle Kanäle zu überwachen, was jedoch notwendig wäre, um ihrer Aufgabe zu 100% zu entsprechen. Ein Zugriff auf die Verkehrsdaten der Internetnutzer scheint daher die einzige Möglichkeit zu sein, um dieses Problem ansatzweise in den Griff zu bekommen.

Um eine einheitlichere Strafverfolgung und Gefahrenabwehr durch die Speicherung und Verarbeitung jener Verkehrsdaten, insbesondere in den Bereichen Terrorismus und Organisierte Kriminalität, sowohl innerhalb als auch zwischen den einzelnen Mitgliedsstaaten zu etablieren,[8] verabschiedeten das Parlament der Europäischen Union und der Europäische Rat am 15. März 2006 die Richtlinie 2006/24/EG, die sog.

---

[6] **Pharming** ist die Manipulation von Systemen zur Anzeige gefälschter Webseiten. **Phishing** ist der Versuch, durch gefälschte E-Mails an Passwörter der Internetnutzer zu gelangen. Beim **Keylogging** werden Software oder Hardware zwischen Tastatur und Betriebssystem geschaltet, um die Tastatureingaben zu protokollieren und auf diesem Weg an Passwörter etc. zu gelangen.

[7] Gercke, GA 2012, S. 474 ff. (480).

[8] Europäischen Union, RL 2006/24/EG, Erwägungsgründe Nr. 5 f.

„Vorratsdatenspeicherungsrichtlinie“.[9] Mit dieser Richtlinie wurden die Mitgliedsstaaten angewiesen, ihre nationalen Telekommunikationsunternehmen dahingehend zu verpflichten, bestimmte Verkehrsdaten, die bei der Kommunikation über Telefon, Handy und Internet entstehen, für einen Zeitraum von sechs Monaten bis zu zwei Jahren zu speichern und für die Strafverfolgungsbehörden zur Weiterverarbeitung bereitzuhalten.[10] Dadurch werden ohne einen konkret-individuellen Anlass[11] enorme Mengen von Daten jedes Kommunikationsteilnehmers gespeichert und daher der Gefahr der Kenntnisnahme in einem erhöhten Maße ausgesetzt. Auf diesem Wege wurde von dem bis dato im europäischen Datenschutzrecht traditionell geltenden Grundsatz der Datensparsamkeit in erheblichem Maße abgewichen, sodass von einem „Paradigmenwechsel“ gesprochen wird,[12] da das, was bisher weitestgehend verboten war, nun verpflichtend für alle Anbieter wurde.[13] Kritiker werfen der Richtlinie vor, dass ihre formelle und materielle Vereinbarkeit zumindest zweifelhaft seien.[14] Dennoch wurde sie vom EuGH im Jahr 2009 zumindest in formeller Hinsicht bestätigt, da nach der Rechtsauffassung des EuGH Art. 95 EG a.F. als Rechtsgrundlage für die Richtlinie und somit als Kompetenztitel der Europäischen Gemeinschaft ausreicht.[15] Die „Vorratsdatenspeicherungsrichtlinie“ blieb also in Kraft und musste von den Mitgliedsstaaten gem. Art. 249 Abs. 3 EG a.F. umgesetzt werden, sodass für einen gravierenden Eingriff in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung aller EU-Bürger die rechtliche Grundlage erhalten blieb.

Dieser durch die anlasslose Speicherungspflicht entstandenen Beeinträchtigung hat das Bundesverfassungsgericht hinsichtlich der Umsetzung der Richtlinie in deutsches Recht eine deutliche, aber keinesfalls endgültige,[16] Absage erteilt. Am 02. März 2010 hat das höchste deutsche Gericht die Normen, die der Umsetzung der Richtlinie

---

[9] Europäische Union, Amtsblatt 2006 L 105/54.
[10] Breyer, StV 2007, S. 214 ff. (214 f.); Gitter/Schnabel, MMR 2007, S. 411 ff. (411 f.); Roßnagel, NJW 2010 S. 1238 ff. (1238).
[11] Leutheusser-Schnarrenberger, ZRP 2007, S. 9 ff. (11).
[12] Hoeren, Internet und Kommunikationsrecht, S. 352.
[13] Kühling/Elbracht, Telekommunikationsrecht Rn. 380.
[14] Fink/Cole/Kleber, Medienrecht Rn. 300.
[15] EuGH, Slg. 2009 I, 593 ff.
[16] Eckhard/Schütze, CR 2010, S. 225 ff. (225).

2006/24/EG dienten, also §§ 113a, 113b TKG und § 100g Abs. 1 S. 1 StPO, für verfassungswidrig und nichtig erklärt, Letzteren allerdings nur, so weit er in Verbindung mit den §§ 113a, 113b TKG angewendet wurde.[17] Darüber hinaus ordnete das BVerfG an, dass alle Datensätze, die von den Telekommunikationsunternehmen bis zum Tage der Rechtskraft des Urteils aufgrund des § 113a TKG a.F. gespeichert wurden, zu löschen seien, womit sie den Sicherheitsbehörden nicht länger zur Verfügung standen.[18]

Ein gespaltenes Echo hallte in der Folge durch die deutsche Medienlandschaft. Die Sicherheitsbehörden trauerten einem ihrer – nach eigener Aussage – wichtigsten Ermittlungswerkzeuge gegen Terrorismus und organisierte Kriminalität nach, und Innenpolitiker forderten von der Bundesregierung eine neue gesetzliche Regelung, am besten über Nacht. Dies unterstrich der Bayerische Staatsminister des Inneren, Joachim Herrmann (CSU), als er bei der Vorstellung des Verfassungsschutzberichtes Bayern 2009 feststellte, dass die Vorratsdatenspeicherung doch empfindlich im Kampf gegen den internationalen Terrorismus vermisst werde und deshalb von Bundesjustizministerin Leutheusser-Schnarrenberger forderte: „Die Bundesjustizministerin muss umgehend einen Gesetzesentwurf zur Vorratsdatenspeicherung vorlegen, damit wir Terrorplanungen frühzeitig erkennen und verhindern können.“[19] Demgegenüber waren Datenschützer über die Rückendeckung aus Karlsruhe zumindest teilweise erfreut. In der Vorratsdatenspeicherung war der Beginn eines Überwachungsstaats gesehen worden [20] Allerdings wurde teilweise auch davon gesprochen, dass der 02.03.2010 „ein schwarzer Tag für den Datenschutz“[21] gewesen sei, da das Bundesverfassungsgericht nicht die generelle Unvereinbarkeit einer wie auch immer ausgestalteten Vorratsdatenspeicherung mit dem Grundgesetz festgestellt habe. Mithin wurde gefordert, dass es auch keine Neufassung der für nichtig erklärten nationalen Regelungen geben dürfe,[22]

[17] BVerfGE 125, 260.
[18] Ebd. (263).
[19] Herrmann, Verfassungsschutzbericht 2009.
[20] SpiegelOnline, Kritiker warnen vor Überwachungsstaat.
[21] Eckhardt/Schütze, MMR 2010, S. 225 ff. (225).
[22] AK Vorratsdatenspeicherung, Stoppt die Vorratsdatenspeicherung 2.0.

auch wenn das BVerfG in seiner Entscheidung ausdrücklich die Möglichkeit einer solchen Speicherung unter bestimmten Voraussetzungen als verfassungsgemäß ansieht.[23]

In den Reaktionen spiegelt sich auch die grundsätzlich geteilte Haltung über die Vorratsdatenspeicherung in der Gesellschaft wider. Daher handelt es sich bei der Vorratsdatenspeicherung und der Verwertung dieser Daten durch staatliche Stellen auch um eine der am kontroversesten diskutierten „modernen Ermittlungsmethoden". Aber auch wenn die Vorratsdatenspeicherung in Wissenschaft, Rechtsprechung und Gesellschaft heftig umstritten ist, so verlangt Art. 288 Abs. 3 AEU von den Mitgliedsstaaten der EU, dass Richtlinien in nationales Recht umgesetzt werden. Somit ist die Bundesrepublik, wenn sie nicht gegen den AEUV verstoßen will, gezwungen, eine neue Regelung zu erlassen. Allerdings sind in diesem Zusammenhang auch die neueren Entwicklungen in der EU zu beachten, die einen Rückschluss auf die Zukunft der Richtlinie 2006/24/EG zulassen. Damit erlangen auch die europarechtlichen Entwicklungen eine erhebliche Bedeutung für eine eventuelle Neufassung.

Das Ziel dieser Arbeit ist es, einen Vorschlag für eine Neufassung der für nichtig erklärten Regelungen des Telekommunikationsgesetzes und der Strafprozessordnung zu erarbeiten. Im ersten Teil werden die im Rahmen der Vorratsdatenspeicherungsdiskussion relevanten technischen Aspekte einer Betrachtung unterzogen, auf deren Grundlage die spätere rechtliche Auseinandersetzung mit der Thematik erfolgen soll. Damit auch die datenschutzrechtliche Tragweite der Vorrastdatenspeicherung erfasst werden kann, wird auf diesem Wege, neben der Darstellung der Funktionsweisen der verschiedenen Kommunikationsformen, auch herausgestellt, welche Daten beim Stattfinden der Kommunikation anfallen bzw. benötigt werden und welche dieser Daten Gegenstand der Vorratsdatenspeicherung sind. Im zweiten Teil der Arbeit werden die verschiedenen staatlichen und gesellschaftlichen Standpunkte zur Thematik der Vorratsdatenspeicherung dargestellt. So werden die Erwartungshaltungen der staatlichen Stellen vor der Einführung der Vorratsdatenspeicherung analysiert und auf ihre Erfül-

[23] BVerfGE 125, 260.

lung hin untersucht. Außerdem geht die Arbeit auf die in anderen gesellschaftlichen Bereichen bestehenden Ansichten zur Erforderlichkeit und Realisierbarkeit einer Vorratsdatenspeicherung ein. Im dritten Teil konzentriert sich die Untersuchung dann auf den europarechtlichen Ursprung der Vorratsdatenspeicherung. Zunächst wird die Richtlinie 2006/24/EG hinsichtlich ihrer Entstehungsgeschichte und ihrer Vorgaben an die Mitgliedsstaaten untersucht. Anschließend wird dann überprüft, wie Deutschland diese Vorgaben bei der Umsetzung zum 01.01.2008 beachtet hat. Außerdem wird rechtsvergleichend analysiert, wie andere Staaten die Vorratsdatenspeicherung in ihren Rechtsordnungen etabliert haben. Diesbezüglich wird beispielhaft auf das Vereinigte Königreich, Österreich und die Schweiz eingegangen. Aber auch die Gesamtumsetzung der Richtlinie wird anhand der Erhebungen der Europäischen Kommission untersucht. Im vierten Teil steht dann das Urteil des Bundesverfassungsgerichts vom 02.03.2010 im Fokus. Hier werden anhand des Urteils die verfassungsrechtlichen Vorgaben für eine Neufassung der Vorratsdatenspeicherung zusammengetragen, indem die deutschen Umsetzungsregelungen zur Richtlinie 2006/24/EG im Lichte der von ihnen betroffenen Grundrechte analysiert werden. Der fünfte Teil der Untersuchung befasst sich sodann mit den Entwicklungen zur Frage der Vorratsdatenspeicherung auf europäischer Ebene, sprich: mit der Zukunft der Richtlinie 2006/24/EG. So wird die Vereinbarkeit der Richtlinie mit der EMRK und der Grundrechtscharta der Europäischen Union überprüft und schließlich auf die vorhandenen Novellierungsbestrebungen eingegangen, wobei die bereits im rechtsvergleichenden Teil erwähnte Erhebung der Europäischen Kommission eine wesentliche Rolle spielen wird. Zuletzt wird dann im sechsten Teil der Versuch unternommen, eine neue deutsche Fassung der Vorratsdatenspeicherung zu schaffen, wobei die im Verlauf der Untersuchung gesammelten verfassungsrechtlichen und europarechtlichen Vorgaben als Grundlage dienen. Darüber hinaus sollen die ermittelten gesellschaftlichen Interessen und Standpunkte ebenfalls einfließen.

1.Teil: Vorratsdatenspeicherung - Eine technische Betrachtung

Bevor auf die rechtliche Seite der Vorratsdatenspeicherung eingegangen werden kann, muss sich zunächst mit den technischen Grundlagen befasst werden. Denselben Gedanken werden auch die Richterin und die Richter des Ersten Senats des Bundesverfassungsgerichts gehabt haben, als sie über die Verfassungsbeschwerden 1 BvR 256/08, 263/08, 586/08 entscheiden mussten. So wurde bei der Universität Mannheim eine Stellungnahme zur technischen Seite der Vorratsdatenspeicherung in Auftrag gegeben, welche unter dem Titel „Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung“ am 22.06.2009 vorlag.[24]

I. Die Speicherung und das Abrufen der Verkehrsdaten

Der Übersichtlichkeit halber, sollte zwischen Kommunikation durch Telefon und Internet einerseits und Mobiltelefonie andererseits unterschieden werden.

1. Kommunikation via Telefon oder Internet

Im Rahmen der Vorratsdatenspeicherung werden alle Arten von Telekommunikationsdiensten, die sich eines Telefons oder des Internet via Computer bedienen, erfasst.[25]

a) Hierarchisches Schichtensystem

Bei diesen Kommunikationsarten werden die relevanten Daten digital übermittelt, also über zwischengeschaltete Computer, wobei die Datenpakete durch das *Internet(working)-Protocoll (IP)* von einem Computer zum nächsten entlang einer Kette von vernetzten Computern weitergeschickt werden.[26] Ein Protokoll wie das IP definiert dabei das Format und die Reihenfolge des Nachrichtenaustausches zwischen zwei

[24] Freiling, Vorratsdatenspeicherung.
[25] Leutheusser-Schnarrenberger, ZRP 2007, S. 9 ff. (9).
[26] Kolb, Vorratsdatenspeicherungsrichtlinie, S. 11.

oder mehreren kommunizierenden Endgeräten sowie die Handlungen, die bei Übertragung und Empfang einer Nachricht oder anderer Ereignisse ausgeführt werden.[27] Die beim Transport entlang dieser Kette eingesetzten Medien lassen sich dabei in geführte und nicht geführte Medien unterteilen.[28] Erstere zeichnen sich dadurch aus, dass die elektromagnetischen Wellen, die die Bits transportieren, über ein festes Medium, wie etwa ein Glasfaserkabel, laufen, während sich bei den nicht geführten Medien die Wellen in der Atmosphäre (bei WLAN) oder im Weltraum (bei einem Satellitenkanal) ausbreiten.[29] Bezüglich der WLAN-Verbindung ist aber festzuhalten, dass dies nur möglich ist, wenn Versende- und Empfangscomputer jeweils über eine entsprechende Hardware, also eine Empfangsantenne, verfügen und sich in der Reichweite des jeweils Anderen befinden.[30]

Bei der Übertragung der Datenpakete durch das IP werden diese nach einem hierarchischen Schichtensystem verarbeitet.[31] Dabei werden unterschiedliche Ansichten darüber vertreten, wie viele Schichten das hierarchische System enthält. Nach dem sog. DAPRA-Modell[32] handelt es sich um vier Schichten:[33]

- Physische Schicht
- Netzwerkschicht
- Transportschicht
- Anwendungsschicht

[27] Kurose/Ross, Computernetzwerke, S. 30.
[28] Ebd. S. 41.
[29] Freiling, Vorratsdatenspeicherung, S. 3.
[30] Ebd.
[31] Ebd.
[32] Die *Defense Advanced Research Projects Agency* (DARPA) ist die amerikanische Regierungsbehörde, die das IP entwickelt hat (Kolb, Vorratsdatenspeicherungsrichtlinie Fn. 30).
[33] Freiling Vorratsdatenspeicherung, S.3 ff.; Kolb, Vorratsdatenspeicherungsrichtlinie, S. 11.

Der Ansatz, nach dem fünf Schichten anzunehmen sind, ergänzt das oben gezeigte System um eine weitere Schicht zwischen der Physischen (die dort Bitübertragungsschicht genannt wird) und der Netzwerkschicht.[34] Diese Sicherheitsschicht enthält demnach verschiedene Protokolle, die die Übertragung zwischen mehreren Knotenpunkten im Netz sicherstellen sollen.[35] Zu beachten ist aber, dass diese Funktion dem Vier-Schichten-Ansatz nach von der Netzwerk- bzw. der Transportschicht übernommen wird.[36] Für die folgende Vorstellung des Kommunikationsablaufs und das Verständnis der Vorratsdatenspeicherung sind nähere Kenntnisse bezüglich dieser Unterschiede allerdings nicht erforderlich, sodass auf eine weitergehende Darstellung verzichtet werden kann.

b) Physische Schicht

In der Physischen Schicht wird gewährleistet, dass die Informationseinheiten (Bits) über ein physikalisches Medium übertragen werden, also entweder durch ein Kabel zwischen zwei Computern oder durch Funkwellen zwischen zwei Empfangsgeräten.[37] Folglich stellt die Physische Schicht die Grundlage der Kommunikation dar, weil ohne sie die Bits nicht übertragen werden könnten.[38] Auch hier werden bereits Adressen verwendet, und zwar die sogenannten MAC-Adressen, die vom Hersteller für die Netzwerkkarten, die für die Kommunikation zwischen zwei Computern notwendig sind, vergeben werden.[39] Allerdings sind die MAC-Adressen keine Datensätze, die ausweislich der Reglungen der Richtlinie 2006/24/EG Gegenstand der Vorratsdatenspeicherung sind, weshalb auf eine nähere Beschreibung dieser Schicht verzichtet werden kann.

---

[34] Kurose/Ross, Computernetzwerke, S. 70 ff.
[35] Ebd. S. 74.
[36] Freiling, Vorratsdatenspeicherung, S. 6.
[37] Kolb, Vorratsdatenspeicherungsrichtlinie, S. 11.
[38] Walke, Mobilfunknetze und ihre Protokolle I, S. 66.
[39] Kolb, Vorratsdatenspeicherungsrichtlinie, S. 11.

c) Netzwerkschicht

In der über der Physischen Schicht liegenden Netzwerkschicht werden die einzelnen Beteiligten mit IP-Adressen ausgestattet, damit die einzelnen Computer bei der globalen Vernetzung im Internet unterschieden werden können.[40] In dieser Schicht werden die Daten in Pakete aufgeteilt, wobei dem Header der Pakete (vergleichbar mit dem Briefkopf) die IP-Adressen der Kommunikationsbeteiligten zu entnehmen sind. Dadurch wird gewährleistet, dass die Bestimmung des Pakets erkennbar ist.[41] Um dies zu ermöglichen, darf eine IP-Adresse weltweit zu einem Zeitpunkt nur einmal vergeben sein.[42] Zu erwähnen ist hier noch der Unterschied zwischen lokalen und dynamischen IP-Adressen. Wegen der voranschreitenden Ausdehnung des Internet ist heute nicht mehr gewährleistet, dass jeder Computer eine eigene, eindeutige IP-Adresse hat, weshalb in vielen Bereichen IP-Adressen an Computer nur noch für die Dauer ihrer Verbindung mit dem Internet vergeben werden.[43] Daher spricht man insoweit von dynamischen IP-Adressen, die wegen ihrer Flüchtigkeit bei der Identifikation des einzelnen Nutzers zwangsläufig Probleme aufwerfen.

d) Transportschicht

Die Transportschicht hat zwei unterschiedliche Aufgaben. Zunächst erreicht sie durch die Verarbeitung einer zu der IP-Adresse hinzugefügten *Port Number*, dass nicht nur einzelne Computer weltweit zur Kommunikation verwendet, sondern auch einzelne Teile eines Computers adressiert werden können.[44] Weiterhin trägt sie dazu bei, dass möglichst keine IP-Datenpakete verloren gehen bzw. deren Verlust umgehend bemerkt und behoben werden kann.[45] Dies geschieht durch das *Transmission Control Protocol (TCP)*, das die Nachricht weiter aufteilt und mittels einer Nummerierung zusammenhängender IP-Datenpakete oder einer zusätzlichen Codierung sicherstellt, dass die

---

[40] Freiling, Vorratsdatenspeicherung, S. 5 f.
[41] Kolb, Vorratsdatenspeicherungsrichtlinie, S. 12.
[42] Ebd.
[43] Ebd. S. 56 f.
[44] Kolb, Vorratsdatenspeicherungsrichtlinie, S. 12.
[45] Freiling, Vorratsdatenspeicherung, S. 6.

Nachricht vollständig ankommt bzw. Verluste direkt bemerkt werden.[46] Mithin steuert die Transportschicht den Datenfluss, indem sie sowohl den Beginn als auch das Ende einer Datenübertragung regelt.[47]

e) Anwendungsschicht

In der Anwendungsschicht finden schließlich die modernen Anwendungen, wie etwa die Nutzung des E-Mail-Postfachs, statt, da erst durch die Nutzung der bisher vorgestellten Schichten Datenpakete versendet werden können.[48] Die eigentliche Kommunikation wird also erst auf der jeweiligen Anwendungsebene verarbeitet. Folglich ist diese Ebene für die Vorratsdatenspeicherung maßgeblich, weil die Verkehrsdaten erst hier anfallen.

2. Mobilfunkkommunikation

Die Bedeutung des Mobilfunks für die heutige Kommunikation kann allein schon aufgrund seines quantitativen Umfangs nicht hoch genug eingeschätzt werden. Folglich bedarf es auch in diesem Bereich einer technischen Betrachtung, bevor sich der rechtlichen Seite zugewendet werden kann.

a) Telefonieren im GSM-Netz

Ein GSM-Netz funktioniert so, dass die Kommunikationsdatenpakete zwischen zwei Mobilstationen (Mobiltelefonen) zunächst mittels Funkwellen an die Basisstation, in deren Reichweite sich die Mobilstation befindet, geleitet werden.[49] In welchem Basisstationen-Bereich (sog. Funkzelle) sich eine Mobilstation befindet, wird von der sogenannten Heimatdatei angegeben, die neben Namen und sonstigen Vertragsdaten des Benutzers auch dessen ungefähren Aufenthaltsort speichert. Jede Basisstation zeigt der

---

[46] Kolb, Vorratsdatenspeicherungsrichtlinie, S. 12.
[47] Walke, Mobilfunknetze und ihre Protokolle I, S. 67.
[48] Kolb, Vorratsdatenspeicherungsrichtlinie, S. 13.
[49] Ebd.

Heimatdatei an, wenn eine Mobilstation in ihren Bereich gelangt oder diesen verlässt, was dadurch möglich ist, dass die Basisstation bei der Mobilstation in regelmäßigen Abständen die Netzstärke abfragt, wobei die jeweilige persönliche Rufnummer als Zugangsschlüssel für die Heimatdatei dient.[50] Die Basisstation schickt die Datenpakete dann an eine Mobilvermittlungsstelle, die mittels der Rufnummer des Angerufenen dessen Heimatdatei einliest und so die Datenpakete an die richtige Basisstation liefert, von wo aus nun wieder über Funk der Anruf bei der Empfängermobilfunkstation eingeht.[51] Damit der einzelne Kommunikationsteilnehmer identifiziert werden kann, gibt es das *Subscriber Identity Module* (SIM), welches in Kartenform in das Mobiltelefon eingesetzt wird.[52] Dieses enthält neben den persönlichen Daten auch die *International Mobile Station Identity* (IMSI), die ihrerseits eine Länderkennung, eine Heimatdateienkennung und eine persönliche Kennung in der jeweiligen Heimatdatei enthält.[53] Folglich ist der jeweilige Teilnehmer international eindeutig zu identifizieren.[54] Bei der Identifizierung der Kommunikationsteilnehmer eines einzelnen Kommunikationsvorgangs ist die *Temporary Mobile Subscriber Identity (TMSI)* essentiell.[55] Bei dieser handelt es sich um eine Zahl, die die IMSI codiert und durch die Verschleierung der IMSI einerseits und periodische Wechsel der Codierung andererseits der Vertraulichkeit der Nachrichtenübermittlung dienen soll.[56] Mithin muss die TMSI nach ihrer Feststellung decodiert werden, um die IMSI zu erfahren, die dann die Identifikation des Kommunikationsteilnehmers ermöglicht. Weiterhin sind auch die einzelnen Mobilfunkgeräte mit einer Identitätsnummer versehen, der sogenannten *International Mobile Equipment Identity (IMEI)*.[57] Diese werden im *Equipment Identity Register (EIR)* gespeichert und nach den Kategorien einwandfreie Funktionalität, Sperrung bzw. Diebstahl und Defekt geordnet.[58]

---

[50] Freiling, Vorratsdatenspeicherung, S. 9 f.
[51] Ebd.
[52] Ebd. S. 10.
[53] Ebd.
[54] Walke, Mobilfunknetze und ihre Protokolle I, S. 315; Kolb, Vorratsdatenspeicherungsrichtlinie, S. 15.
[55] Freiling, Vorratsdatenspeicherung, S. 11.
[56] Walke, Mobilfunknetze und ihre Protokolle I, S. 317.
[57] Kolb, Vorratsdatenspeicherungsrichtlinie, S. 14.
[58] Walke, Mobilfunknetze und ihre Protokolle I, S. 151.

b) Short Messaging Service (SMS)

Das Abschicken und Empfangen einer SMS funktioniert ähnlich wie das Anrufen eines anderen Mobilfunkteilnehmers. Nachdem die SMS vom Sender abgeschickt wurde, geht sie beim *Short Messaging Service Center (SMSC)* ein und wird dort zwischengespeichert.[59] Das SMSC sendet dann eine Signalisierungsnachricht mit der TMSI des Nachrichtenempfängers an die Mobilstationen im Aufenthaltsbereich des Empfängers, den es durch die Heimatdatei eingelesen hat.[60] Die Mobilfunkstation des Nachrichtenempfängers sendet daraufhin eine Antwort an das SMSC, welches auf einer gesicherten Leitung die richtige Nachricht an den Empfänger sendet.[61]

c) GPRS

Der *General Packet Radio Service (GPRS)* fungiert als Datenübertragungsdienst, der insbesondere auf IP-Adressen zugreifen kann, um so Datenpakete in externe Netze versenden und auch aus diesen empfangen zu können.[62] Insoweit fungieren externe GPRS-Systemknoten als Bindeglieder zum externen Netz und wandeln die IP-Adressen in IMSI und umgekehrt um, sodass die Datenpakete im jeweiligen anderen System verarbeitet werden können.[63]

3. Gegenstand der Vorratsdatenspeicherung

Der Gegenstand der Vorratsdatenspeicherung sind begriffslogisch Daten, die auf den bisher vorgestellten Wegen durch die unterschiedlichen Netze (Festnetz, Internet, Mobilfunknetz) geleitet werden. Dabei muss man im Rahmen der Kommunikation zwischen Inhaltsdaten einerseits und Verkehrsdaten andererseits unterscheiden. Außerdem sind als dritte Datengruppe die Bestandsdaten zu nennen.

---

[59] Freiling, Vorratsdatenspeicherung, S. 11.
[60] Ebd.
[61] Ebd.
[62] Ebd. S. 11 f.
[63] Ebd.

a) Verkehrsdaten

Bei Verkehrsdaten handelt es sich nicht um alle bei der Kommunikation anfallenden Daten, sondern nur um eine Teilmenge. Diese definiert § 3 Nr. 30 TKG als solche Daten, die beim Stattfinden der Kommunikation notwendigerweise entstehen, verarbeitet oder genutzt werden. Ihren Ursprung hat diese Definition in Art. 2 lit. b der Datenschutzrichtlinie 2002/58 EG.[64] Als Beispiele sind etwa die Rufnummern von Sender und Empfänger, Anfang und Ende der Kommunikation sowie der persönliche Standort im Rahmen der Möglichkeiten des Mobilfunks zu nennen. Eine solche Definition fehlt der Richtlinie 2006/24/EG. Stattdessen definiert Art. 1 Abs. 2 Nr. 1 der Richtlinie „Verkehrsdaten und Standortdaten sowie alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind“, als Daten im Sinne der Richtlinie 2006/24/EG. Diese Begriffsbestimmung wird aber dadurch konkretisiert, dass in Art. 5 der Richtlinie beim Speicherungsgegenstand genau angegeben wird, welche Daten zur Identifikation des Teilnehmers erforderlich sind, wobei es sich – mit einer Ausnahme – ausschließlich um Verkehrsdaten im Sinne von § 3 Nr. 30 TKG handelt (siehe Speicherungsgegenstand).

b) Inhaltsdaten

Inhaltsdaten sind demgegenüber solche Daten, die nach dem allgemeinen Sprachgebrauch den Inhalt der Kommunikation darstellen als auch die gerade erläuterten Verkehrsdaten.[65] Andere, wie etwa der österreichische Gesetzgeber in § 92 Abs. 3 Ziffer 5 des österreichischen Telekommunikationsgesetzes,[66] sehen den Begriff der Inhaltsdaten bereits mit dem klassischen Gesprächs- oder Nachrichteninhalt als erschöpft an.

Auf eine Entscheidung dieses Streits kommt es für die vorliegende Betrachtung der Vorratsdatenspeicherung aber gar nicht an, da im Rahmen der Vorratsdatenspeicherung vielmehr die Frage entscheidend ist, in welchem Maße die bei der Telekommuni-

---

[64] Scheurle/Mayen/*Lünenburger*, TKG § 3 Rn. 81.
[65] Freiling, Vorratsdatenspeicherung, S.13.
[66] Kolb, Vorratsdatenspeicherungsrichtlinie, S.83.

kation anfallenden Verkehrsdaten ebenso schutzwürdig sind, wie der Inhalt der Kommunikation. Für die Beantwortung dieser Frage ist es irrelevant, ob die Inhaltsdaten die Verkehrsdaten und den Kommunikationsinhalt erfassen oder ob sie nur den Inhalt der Kommunikation enthalten.

c) Bestandsdaten

Bestandsdaten sind gem. § 3 Nr. 3 TKG solche Daten, die nur für das Vertragsverhältnis zwischen Kommunikationsunternehmen und dem Benutzer relevant sind und eben nicht für die einzelne Kommunikationsverbindung. Als Beispiele sind hier die Anschrift und die Bankverbindung des Verwenders oder Aufnahme und Ende des Vertragsverhältnisses zu nennen.