Hauptteil B

Aufbau der Unterrichtseinheit	Materialien
B DATEN RUND UMS MOBILTELEFON	
Kennenlernen der verschiedenen Daten, die ein Mobiltelefon produziert Overheadfolie 5 bzw. 6 gibt einen Überblick über die vier Datengruppen, die ein Mobiltelefon produziert: Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten. Im Klassenverband wird erarbeitet, welche Informationen zu welcher Datengruppe gehören. Anschließend werden die Tagesprotokolle auf Arbeitsblatt 9 ausgefüllt und anhand folgender Fragen analysiert: ● Was verrät das Mobiltelefon über den Tagesablauf eines Menschen? ● Welche Rückschlüsse kann man daraus auf soziale Kontakte und tägliche Gewohnheiten eines Menschen ziehen?	**Datenproduzent Handy** Overheadfolie 5, Seite 107 **Mobiles Tagesprotokoll** Arbeitsblatt 9, Seite 109 **The mobile phone - producer of data** Overheadfolie 6, Seite 108 **Mobile daily record** Arbeitsblatt 9, Seite 110
Auf Arbeitsblatt 10 sollen die die SchülerInnen Satzteile richtig kombinieren. Diese haben die möglichen Rückschlüsse vom Telefonierverhalten eines Menschen auf dessen soziales Umfeld bzw. tägliche Gewohnheiten zum Thema.	**Richtig kombiniert?** Arbeitsblatt 10, Seite 111 **The right connection?** Arbeitsblatt 10, Seite 112
Auseinandersetzung mit den gesetzlichen Vorgaben Die SchülerInnen setzen sich mit Abschnitt 12, §§ 96-102 des österreichischen Telekommunikationsgesetzes auseinander. Diese Paragraphen widmen sich dem Kommunikationsgeheimnis und dem Datenschutz. *Tipp:* Geben Sie Ihren SchülerInnen die Aufgabe, einzeln oder in Gruppenarbeit weitere Richtig-/Falsch-Sätze zu den Gesetzesauszügen zu erstellen. Gemeinsam kann anschließend ein Quiz durchgeführt werden.	**Wer hat Zugriff?** Arbeitsblatt 11, Seite 113-114 Overheadfolie 6, Seite 117 **Free access? The legal situation** Arbeitsblatt 11, Seite 115-116 Overheadfolie 7, Seite 118
Vorratsdatenspeicherung ● *Schritt 1 – inhaltlicher Überblick* Arbeitsblatt 12 liefert einen kurzen Überblick zum Thema. ● *Schritt 2 – Sammeln von Pro- und Kontra-Argumenten* Basierend auf den vorhandenen Informationen sammeln die SchülerInnen im Klassenverband oder in Gruppenarbeit Argumente für und gegen die Vorratsdatenspeicherung. *Tipp für eine Weiterführung der Sammlung von Pro- und Kontra-Argumenten mit anschließendem Rollenspiel* Teilen Sie Ihre SchülerInnen in vier Gruppen. Jede Gruppe erhält den Auftrag, Argumente für und gegen die Vorratsdatenspeicherung aus einer der nachfolgenden Perspektiven zu sammeln: ❍ Argumente seitens der Gesetzgebung ❍ Argumente seitens der Justiz/der Exekutive ❍ Argumente seitens der Mobilfunkbetreiber	**Big Brother?** Arbeitsblatt 12, Seite 119 **Big Brother?** Arbeitsblatt 12, Seite 120 **Pro & Kontra** Arbeitsblatt 13, Seite 121 **Pros & Cons** Arbeitsblatt 13, Seite 122

Nach Abschluss des Rollenspiels werden der Diskussionsverlauf sowie die Stimmigkeit der Argumente innerhalb der Rollenspielgruppe besprochen und analysiert – das Ergebnis dieser Analyse wird den anderen Rollenspielgruppen präsentiert.

Tipp zur Erweiterung und Hinterfragung bereits gesammelter Argumente durch Recherche
Geben Sie Ihren SchülerInnen die Aufgabe, sich in den Medien zum Thema zu informieren und basierend auf diesen zusätzlichen Informationen neue Argumente zu sammeln bzw. bereits gesammelte Argumente zu hinterfragen.

- *Schritt 3 – Auseinandersetzung mit der medialen Berichterstattung rund um die Einführung der Vorratsdatenspeicherung in Österreich*
  Nachdem die SchülerInnen Argumente für und gegen die Vorratsdatenspeicherung gesammelt haben, setzen sie sich abschließend mit der medialen Berichterstattung zu diesem Thema auseinander.

  Die Klasse wird in sechs Gruppen geteilt. Jede Gruppe erhält einen der Presseartikel auf Arbeitsblatt 13. Die Artikel werden ausgehend von vier Analysefragen näher beleuchtet:

  1. Welche Argumente werden im Artikel genannt, die für eine Vorratsdatenspeicherung sprechen?
  2. Welche Argumente werden im Artikel genannt, die gegen eine Vorratsdatenspeicherung sprechen?
  3. Wie gut informiert fühlt man sich nach dem Lesen des Artikels?
  4. Stimmen die im Artikel angeführten Informationenzur Vorratsdatenspeicherung beim Telefon?

  Die Ergebnisse der einzelnen Gruppen werden miteinander verglichen. Abschließend können die aus den Artikeln gesammelten Argumente mit jenen der SchülerInnen verglichen werden.

  Tipp:
  Erfolgt die Analyse der Zeitungsartikel im Stationenbetrieb, so können die SchülerInnen die einzelnen Artikel auch direkt miteinander vergleichen.

Tipp zur Internationalisierung des Themas „Vorratsdatenspeicherung" am Beispiel Deutschland
Ausgangspunkt für die Einführung der Vorratsdatenspeicherung in Österreich ist eine EU-Richtlinie aus dem Jahr 2006. Diese gilt für alle EU-Mitgliedsstaaten.
Geben Sie den SchülerInnen die Aufgabe zu recherchieren, wie die Richtlinie in Deutschland umgesetzt wurde, und welche Entwicklung es dort bis zum jetzigen Zeitpunkt gegeben hat.

Gut informiert?
Arbeitsblatt 14,
Seite 123-132

Overheadfolie 5 bzw. 6: Datenproduzent Handy/The mobile phone - producer of data

Zusatzinformation

Im Telekommunikationsgesetz wird unter anderem definiert, welche Daten ein Mobiltelefon erzeugt und wie diese bezeichnet werden. Nachfolgend die entsprechenden Auszüge aus dem Telekommunikationsgesetz:

> *„Stammdaten"* sind alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:
>
> - Familienname und Vorname,
> - akademischer Grad,
> - Wohnadresse,
> - Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
> - Information über Art und Inhalt des Vertragsverhältnisses,
> - Bonität
>
> *„Verkehrsdaten"* sind Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden. Zu den Verkehrsdaten zählen auch die „Zugangsdaten", die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.
>
> *„Standortdaten"* sind Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben.
>
> *„Inhaltsdaten"* sind die Inhalte übertragener Nachrichten.
>
> Als *„Nachricht"* gilt jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können.
>
> Dem Kommunikationsgeheimnis unterliegen die Verkehrsdaten, die Standortdaten und die Inhaltsdaten: Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.
>
> *Quelle:* www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849
> – vollständige Fassung des Telekommunikationsgesetzes vom 15.05.2013

Arbeitsblatt 9: Mobiles Tagesprotokoll/Mobile daily record

- *Quelle Studie Marketagent:* http://derstandard.at/1285199348055/Jugendstudie-Schlussmachen-per-SMS-bei-717-Prozent-verpoent
- *Quelle Handybesitz:* www.oe24.at/digital/Nur-2-Prozent-wollen-ohne-Handy-leben/813578

Arbeitsblatt 10: Richtig kombiniert?/The right connection?

Lösung:

- Wenn jemand weiß, mit wem du telefonierst, kann er daraus auf deinen Freundes- und Bekanntenkreis schließen.
- Wer über die zeitliche Nutzung deines Handys Bescheid weiß, ist auch über deinen Tagesablauf informiert.
- Wie oft und wie lang du mit jemandem telefonierst, zeigt, wie wichtig dir diese Person ist.
- Wo du den lieben langen Tag unterwegs bist, kann man aus den Standortdaten deines Handys ablesen.
- Die Verkehrs- und Standortdaten deines Telefons verraten nichts über Gesprächs- oder Nachrichteninhalte.

Arbeitsblatt 12: Big Brother?/Big Brother?
Arbeitsblatt 14: Gut informiert?

Zusatzinformation

- **Die Debatte rund um die Vorratsdatenspeicherung in Österreich**
  Der folgende Auszug aus dem österreichischen Telekommunikationsgesetz definiert nicht nur die Daten, die im Zusammenhang mit Telefondiensten im Rahmen der Vorratsdatenspeicherung gesammelt werden, sondern auch jene Daten, die Internet-Anbieter sowie Anbieter von E-Mail-Diensten sammeln müssen.

Vorratsdaten

§ 102a. (1) Über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 hinaus haben Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Speicherung erfolgt ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt.

(2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:
1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war;
2. Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internet-Zugangsdienst unter Angabe der zugrundeliegenden Zeitzone;
3. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;
4. die eindeutige Kennung des Anschlusses, über den der Internet-Zugang erfolgt ist.

(3) Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten obliegt die Speicherung folgender Daten:
1. Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;
2. bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;
3. Name und Anschrift des anrufenden und des angerufenen Teilnehmers;
4. Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;
5. die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste).
6. Bei Mobilfunknetzen zudem
   a) der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;
   b) der internationalen Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses;
   c) Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt;
   d) der Standortkennung (Cell-ID) bei Beginn einer Verbindung.

(4) Anbietern von E-Mail-Diensten obliegt die Speicherung folgender Daten:
1. die einem Teilnehmer zugewiesene Teilnehmerkennung;
2. Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war;
3. bei Versenden einer E-Mail die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders sowie die E-Mail-Adresse jedes Empfängers der E-Mail;
4. beim Empfang einer E-Mail und deren Zustellung in ein elektronisches Postfach die E-Mail-Adresse des Absenders und des Empfängers der Nachricht sowie die öffentliche IP-Adresse der letztübermittelnden Kommunikationsnetzeinrichtung;
5. bei An- und Abmeldung beim E-Mail-Dienst Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse des Teilnehmers unter Angabe der zugrunde liegenden Zeitzone.

(5) Die Speicherpflicht nach Abs. 1 besteht nur für jene Daten gemäß Abs. 2 bis 4, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden. Im Zusammenhang mit erfolglosen Anrufversuchen besteht die Speicherpflicht nach Abs. 1 nur, soweit diese Daten im Zuge der Bereitstellung des betreffenden Kommunikationsdienstes erzeugt oder verarbeitet und gespeichert oder protokolliert werden.

(6) Die Speicherpflicht nach Abs. 1 besteht nicht für solche Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 34 KommAustriaG unterliegen.

(7) Der Inhalt der Kommunikation und insbesondere Daten über im Internet aufgerufene Adressen dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(8) Die nach Abs. 1 zu speichernden Daten sind nach Ablauf der Speicherfrist unbeschadet des § 99 Abs. 2 unverzüglich, spätestens jedoch einen Monat nach Ablauf der Speicherfrist, zu löschen. Die Erteilung einer Auskunft nach Ablauf der Speicherfrist ist unzulässig.

(9) Im Hinblick auf Vorratsdaten, die gemäß § 102b übermittelt werden, richten sich die Ansprüche auf Information oder Auskunft über diese Datenverwendung ausschließlich nach den Bestimmungen der StPO.

Auskunft über Vorratsdaten

§ 102b. (1) Eine Auskunft über Vorratsdaten ist ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässig.

(2) Die nach § 102a zu speichernden Daten sind so zu speichern, dass sie unverzüglich an die nach den Bestimmungen der StPO und nach dem dort vorgesehenen Verfahren für die Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden übermittelt werden können.

(3) Die Übermittlung der Daten hat in angemessen geschützter Form nach Maßgabe des § 94 Abs. 4 zu erfolgen.

Datensicherheit, Protokollierung und Statistik

§ 102c. (1) Die Speicherung der Vorratsdaten hat so zu erfolgen, dass eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist. Die Daten sind durch geeignete technische und organisatorische Maßnahmen vor unrechtmäßiger Zerstörung, zufälligem Verlust oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung zu schützen. Ebenso ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den Vorratsdaten ausschließlich dazu ermächtigten Personen unter Einhaltung des Vier-Augen-Prinzips vorbehalten ist. Die Protokolldaten sind drei Jahre ab Ende der Speicherfrist für das betreffende Vorratsdatum zu speichern. Die Kontrolle über die Einhaltung dieser Vorschriften obliegt der für die Datenschutzkontrolle gemäß § 30 DSG 2000 zuständigen Datenschutzkommission. Eine nähere Beschreibung des Sorgfaltsmaßstabs zur Gewährleistung der Datensicherheit kann der Bundesminister für Verkehr, Innovation und Technologie per Verordnung festschreiben.

(2) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben zu gewährleisten, dass jeder Zugriff auf Vorratsdaten sowie jede Anfrage und jede Auskunft über Vorratsdaten nach § 102b revisionssicher protokolliert wird. Diese Protokollierung umfasst

1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt,
2. in den Fällen des § 99 Abs. 5 Z 3 und 4 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
3. das Datum der Anfrage sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft,
4. die nach Datum und Kategorien gemäß § 102a Abs. 2 bis 4 aufgeschlüsselte Anzahl der übermittelten Datensätze,
5. die Speicherdauer der übermittelten Daten zum Zeitpunkt der Anordnung der Übermittlung,
6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt sowie
7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben.

(3) Die Speicherung der Protokolldaten hat so zu erfolgen, dass deren Unterscheidung von Vorratsdaten sowie von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherter Daten möglich ist.

(4) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben

1. für Zwecke der Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit die Protokolldaten gemäß Abs. 2 an die Datenschutzkommission und den Datenschutzrat sowie
2. zum Zweck der Berichterstattung an die Europäische Kommission und an den Nationalrat die Protokolldaten gemäß Abs. 2 Z 2 bis 4 an den Bundesminister für Justiz zu übermitteln.

(5) Die Übermittlung der Protokolldaten hat auf schriftliches Ersuchen der Datenschutzkommission bzw. des Bundesministers für Justiz zu erfolgen; die Übermittlung an den Bundesminister muss darüber hinaus jährlich bis zum 31. Jänner für das vorangegangene Kalenderjahr erfolgen.

(6) Über die Protokollierungspflichten nach Abs. 2 hinaus ist eine Speicherung der übermittelten Datensätze selbst unzulässig.

In Österreich gibt es massive Kritik an der Vorratsdatenspeicherung. Von Gegnern wird sie als massiver, unzulässiger Eingriff in die Freiheit und Privatsphäre der ÖsterreicherInnen empfunden.

Linksammlung zu kritischen Stimmen zur Vorratsdatenspeicherung in Österreich:

- http://akvorrat.at: Bürgerinitiative gegen die Vorratsdatenspeicherung
- www.argedaten.at/php/cms_monitor.php?q=DATA-RETENTION: Informationsseite der „ARGE-Daten" zur Vorratsdatenspeicherung

- **Die Vorratsdatenspeicherung im EU-Zusammenhang**

  Die Idee, Kommunikationsdienste zur Speicherung von Daten zu verpflichten, um bei Bedarf darauf zurückgreifen zu können, wurde von der EU nach den Terroranschlägen 2005 in London massiv vorangetrieben. Dahinter steckt der Wunsch, Daten zu sichern, die zur Auflösung oder im besten Fall zur Verhinderung von Verbrechen dienen sollen. Die EU-Richtlinie 2006/24/EG äußert sich *„über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden"* [1] und gibt einen groben Rahmen vor, welche Daten für welchen Zeitraum gespeichert werden sollen. Die Umsetzung der Richtlinie bleibt den jeweiligen Mitgliedsstaaten überlassen.
  Die im März 2006 beschlossene Verordnung war von den Mitgliedsstaaten bis September 2007 umzusetzen, bezüglich der Internetdaten galt die Frist bis März 2009.

  - *Entwicklung in Österreich*

    Das BMVIT (Bundesministerium für Verkehr, Innovation und Technologie) hat im April 2007 einen entsprechenden Entwurf des Telekommunikationsgesetzes (TKG) ausgearbeitet und ein Begutachtungsverfahren eingeleitet. Allerdings konnte sich die Regierung auf keine Umsetzung einigen. Ein Vorwurf von Kritikern war z.B., dass der österreichische Entwurf zur Vorratsdatenspeicherung umfangreicher ausgefallen wäre als in der EU-Richtlinie vorgegeben. 2009 kam der nächste Entwurf, zu dem ebenfalls ein Begutachtungsverfahren eingeleitet wurde. Wieder gab es keine Einigung.
    2010 wurde Österreich wegen Vertragsverletzung vom europäischen Gerichtshof verurteilt. 2011 wurde schließlich die Novelle des Telekommunikationsgesetzes verlautbart, die am 1. April 2012 in Kraft getreten ist.

  - *Entwicklung in Deutschland*

    In Deutschland wurde die Vorratsdatenspeicherung bereits 2004 und 2005, also noch vor Beschluss der EU-Richtlinie diskutiert, aber beide Male abgelehnt. Die EU-Richtlinie zur Vorratsdatenspeicherung aus dem Jahr 2006 wurde 2007 in einem Gesetzestext verarbeitet. Das Gesetz wurde im selben Jahr verabschiedet und trat am 1.1.2008 in Kraft.
    Gegen das neue Gesetz wurden 2007 und 2008 drei Verfassungsbeschwerden beim Bundesverfassungsgericht eingereicht.
    2010 verkündete das deutsche Verfassungsgericht, dass die Vorratsdatenspeicherung nicht mit dem deutschen Grundgesetz vereinbar ist. Seither gibt es (Stand: April 2012) in Deutschland kein gültiges Gesetz zur Regelung der Vorratsdatenspeicherung. Die EU hat Deutschland aufgefordert, eine Vorratsdatenspeicherung schnellstmöglich wieder einzuführen und eine Frist bis zum 26. April 2012 gesetzt. Einen Gesetzesentwurf des deutschen Bundesjustizministeriums lehnte das Innenministerium am 16. April 2012 ab.

[1] www.internet4jurists.at/gesetze/rl_vorratsdaten01.htm – EU Verordnung 2006/24/EG

- *Reaktionen der EU*
  Die EU-Kommission hat mittlerweile eine Prüfung der Richtlinie zu den Vorratsdaten durchgeführt. Dazu gab Innenkommissarin Malmström im April 2011 folgendes Statement ab:

  > *„Unsere Prüfung hat gezeigt, dass die Richtlinie in den verschiedenen EU-Ländern unterschiedlich umgesetzt worden ist", sagte Innenkommissarin Cecilia Malmström der „Welt". „Das ist zwar grundsätzlich für die Umsetzung von EU-Recht nicht ungewöhnlich. Aber ich glaube, dass die derzeitige Richtlinie den Regierungen zu viel Spielraum bei der Umsetzung der Vorratsdatenspeicherung gibt. Auch lässt sie zu viel Raum für die Aufbewahrung und den Umgang der Telekommunikationsanbieter mit den Daten." Zudem sei der Rahmen, in dem sich Strafverfolger Zugang zu diesen Daten beschaffen können, zu groß."*[2]

  Eine neue Richtlinie wurde bislang nicht bekanntgegeben. Am 16. April 2013 hat die EU-Kommission allerdings beschlossen, eine neue Expertengruppe zur Vorratsdatenspeicherung einzusetzen. (Stand: Mai 2013)

Linksammlung zur Vorratsdatenspeicherung im EU-Zusammenhang:

- http://register.consilium.eu.int/pdf/de/05/st03/st03677.de05.pdf : EU-Richtlinie zur Vorratsdatenspeicherung
- www.bfdi.bund.de/cln_007/nn_533578/DE/Schwerpunkte/Vorratsdaten/Artikel/Vorratsdatenspeicherung.html : offizielle Seite des Bundesbeauftragten für Datenschutz in Deutschland
- www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html : Urteil des Bundesverfassungsgerichts vom 2. März 2010
- www.spiegel.de/netzwelt/netzpolitik/0,1518,681122,00.html : Artikel zur Entscheidung des deutschen Verfassungsgerichts 2010
- www.spiegel.de/politik/ausland/0,1518,757499,00.html : Artikel zur Aufforderung der EU an Deutschland, die Vorratsdatenspeicherung wieder einzuführen
- www.fnp.de/fnp/nachrichten/politik/innenministerium-lehnt-fdpentwurf-zu-vorratsdaten-ab_rmn01.c.9764503.de.html : Artikel zur Frist bis 26.4.2012 in Deutschland
- http://fm4.orf.at/stories/1716492 : Artikel zur Ausweitung der Vorratsdatenspeicherung auf Soziale Netzwerke vom 22.4.2013

[2] www.welt.de/print/die_welt/politik/article13179292/Bruessel-will-neue-Regeln-fuer-Vorratsdaten-erlassen.html