Diplomarbeit

Data Retention

Zur aktuellen Rechtslage in einigen ausgewählten EU-Mitgliedsländern unter Berücksichtigung der EU-Richtlinie zur Vorratsdatenspeicherung

von

Karin Larnhof

betreut von

Dr. Christian Reiser

im Fachbereich: Informationstechnologie

Fachhochschul-Studiengang Informationsberufe
Eisenstadt 2005/2006

Ehrenwörtliche Erklärung

Ich habe diese Diplomarbeit selbstständig verfasst, alle meine Quellen und Hilfsmittel angegeben, keine unerlaubten Hilfen eingesetzt und die Arbeit bisher in keiner Form als Prüfungsarbeit vorgelegt.

Eisenstadt, am 30. Mai 2006 Unterschrift

I Kurzreferat

Mitte Dezember 2005 hat das EU-Parlament eine Richtlinie bezüglich Data Retention verabschiedet, welche die Mitgliedstaaten verpflichtet, Ruf- und Verkehrsdaten für mindestens 6 Monate und maximal 2 Jahre zu speichern. Bei der Verwendung von Telekommunikationsdiensten fallen Verkehrsdaten an, die momentan nur zu Abrechnungszwecken und zum Anbieten von Mehrwertdiensten verwendet werden dürfen.

Ziel dieser Diplomarbeit ist es, die EU-Richtlinie der aktuellen Rechtslage in Österreich und jener in anderen EU-Ländern gegenüber zu stellen. Die Hypothesen, dass die Richtlinie durch das Fehlen eines Kostenersatzes eine zusätzliche massive finanzielle Belastung für die Anbieter bedeutet und dass die Richtlinie einen massiven Eingriff in die Privatsphäre der EU-Bürger bedeutet, werden überprüft.

Eine Dokumentenanalyse der aktuellen Literatur, der aktuellen Studien und der relevanten Rechtstexte war Ausgangspunkt dieser Arbeit, danach wurden Leitfadeninterviews mit Experten auf diesem Gebiet durchgeführt. Der Fragenkatalog hierfür umfasste Fragen zu Details der Richtlinie, zu den Sicherheitsaspekten, zur Umsetzung der Richtlinie in nationales Recht und zu den Problemen, die dabei auftreten könnten. Es hat sich herausgestellt, dass die Richtlinie vage formuliert wurde und wichtige Themen nicht abgedeckt wurden. Die Kosten, die bei Anbietern für die Vorratsdatenspeicherung anfallen, müssen nicht verpflichtend ersetzt werden. Auch die Höhe des Kostenersatzes ist nicht geregelt. Überdies können einige Teile der Richtlinie aus technischen Gründen nicht realisiert werden.

Die Ergebnisse zeigen, dass Data Retention ein brisantes Thema ist, dass sie von Datenschutzexperten und Anbietern von Telekommunikationsdiensten abgelehnt und von Strafverfolgungsbehörden befürwortet wird. Außerdem wird befürchtet, dass Probleme bei der Umsetzung in nationales Recht auftreten werden, sodass Klagen beim Europäischen Gerichtshof einlangen werden und das Europäische Parlament die Richtlinie überarbeiten und eine neue wird verabschieden müssen.

Schlagwörter: *Data Retention, Vorratsdatenspeicherung, EU-Richtlinie, Datenschutz*

II Abstract

In December 2005 the European Parliament passed a directive about Data Retention that obliges every member state to save all connection data for six to 24 months. The use of telecommunication services results in connection data, which is normally used for billing and for offering value-added services. The aim of this thesis is to analyse this EU-guideline and compare it with the current legal position in Austria and in the EU. The hypothesis is tested that the directive will have competitive disadvantages for small and medium-sized businesses and that it will have a massive influence on the privacy of the users.

A review of current literature on this topic is undertaken. Then four experts on this subject are interviewed. The questionnaire for these interviews covers issues regarding details of the guideline, security aspects, the conversion to Austrian legislation and problems that could occur. It is found that the wording using in the directive is very vague and important fields are not covered. The expenses arising for the provider for saving the connection data or for implementing security provisions can be covered by the member states, but they are not obliged to do so. Moreover some of the specifications of the EU-directive cannot be realised for technical purposes.

The findings show that Data Retention is a very controversial subject, being advocated by privacy experts and providers of telephony and Internet and endorsed by law enforcement agencies. Furthermore, problems will occur converting the EU-directive to national legislation because of the problems mentioned in the paper. Therefore the European Parliament will have to revise the directive and agree to adapt the directive.

Keywords: *Data Retention, connection data, EU-directive, EU-guideline, data protection*

III Executive Summary

Zentrale Frage dieser Arbeit ist es, wie sich die derzeitige rechtliche Lage in Österreich und in den anderen EU-Ländern darstellt und welche Regelungen die EU-Richtlinie bezüglich Data Retention beinhaltet.

Ziel ist es herauszufinden, welche Auswirkungen die Richtlinie haben wird und wo bei der Umsetzung Probleme auftreten könnten.

Die wesentlichen Ergebnisse meiner Arbeit werden in den Hauptkapitlen „Derzeitige rechtliche Lage“ und „Data Retention“ beschrieben.

Das dritte Kapitel dieser Diplomarbeit (Derzeitige rechtliche Lage) beschäftigt sich hauptsächlich mit der aktuellen Gesetzgebung in Österreich. Zunächst werden die Überwachungsmöglichkeiten bezüglich Festnetz- und Mobiltelefonie sowie Internet behandelt. Danach werden die unterschiedlichen Regelungen von Telekommunikationsgesetz, Überwachungsverordnung und Überwachungskostenverordnung beschrieben. Der zweite Teil des Kapitels handelt von jenen europäischen Ländern, in denen bereits Regelungen bezüglich der Vorratsdatenspeicherung vorhanden sind. In Frankreich und Spanien ist die Data Retention für die Anbieter von Telekommunikationsdiensten verpflichtend, in Großbritannien erfolgt sie auf freiwilliger Basis. Eine verpflichtende und umfassende Vorratsdatenspeicherung, wie sie in der EU-Richtlinie geplant ist, wird allerdings in keinem Land praktiziert.

Kapitel 4 (Data Retention) handelt von der kürzlich beschlossenen EU-Richtlinie bezüglich Vorratsdatenspeicherung. Zu Beginn werden die Entstehungsgeschichte, Anlass und Ziele sowie Befürworter und Gegner der Richtlinie abgehandelt. Danach werden die Details, also die Regelungen der Richtlinie beschrieben. Da die EU-Direktive in einigen Punkten vage formuliert ist und wichtige Details überhaupt nicht

behandelt wurden, werden diese im folgenden Unterpunkt ausführlich diskutiert. Die Ergebnisse dessen werden dann in „Risiken und Probleme bei der Umsetzung“ besprochen. Durch den Beschluss der Richtlinie werden einige bestehende Rechtstexte, österreichische sowie europäische, verletzt. Dass die Direktive sowohl auf Wirtschaft als auch auf die Gesellschaft hat Auswirkungen, wird ebenfalls behandelt. Im zweiten Teil des Kapitels werden Möglichkeiten besprochen, welche Umgehensmöglichkeiten der umfassenden Vorratsdatenspeicherung durch die EU-Bürger wahrgenommen werden können.

An dieser Stelle möchte ich mich ganz herzlich bei meinen Interviewpartnern bedanken, die mit mir sehr interessante Gespräche geführt haben. Ich möchte ihnen auch dafür danken, dass ich mich jederzeit mit Fragen an sie wenden konnte.

Außerdem möchte ich auch meiner Familie und meinen Freunden für ihre Unterstützung, für Anregungen und Ideen danken.

IV Inhalt

V Verzeichnis der Tabellen

VI Abkürzungsverzeichnis

ADSL ***A***symmetric ***D***igital ***S***ubscriber ***L***ine

BMVITBundes***m***inisterium für ***V***erkehr, ***I***nnovation und ***T***echnologie

ETSI ***E***uropean ***T***elecommunications ***S***tandards ***I***nstitute

FTP ***F***ile ***T***ransfer ***P***rotocol

GPRS ***G***eneral ***P***acket ***R***adio ***S***ervice

GSM ***G***lobal ***S***ystem for ***M***obile Communication

IMEI ***I***nternational ***M***obile ***E***quipment ***I***dentity

IMSI ***I***nternational ***M***obile ***S***ubscriber ***I***dentity

IP ***I***nternet ***P***rotocol

ISDN ***I***ntegrated ***S***ervices ***D***igital ***N***etwork

ISPA ***I***nternet ***S***ervice ***P***roviders ***A***ustria

IRC ***I***nternet ***R***elay ***C***hat

KMU ***K***lein- und ***M***ittel***u***nternehmen

LEA ***L***aw ***E***nforcement ***A***gencies

MMS ***M***ultimedia ***M***essaging ***S***ervice

P2P ***P***eer to ***P***eer

PSTN ***P***ublic ***S***witched ***T***elephone ***N***etwork (Festnetz)

SMS ***S***hort ***M***essage ***S***ervice

SPoC ***S***ingle ***P***oint ***o***f ***C***ontact

P2P ***P***eer to ***P***eer

TETRA ***Te***rrestrial ***Tr***unked ***Ra***dio

TKG ***T***ele***k***ommunikations***g***esetz

ÜKVO ***Ü***berwachungs***k***osten***v***erordnung

UMTS ***U***niversal ***M***obile ***T***elecommunications ***S***ystem

URL ***U***niform ***R***escource ***L***ocator

ÜVO ***Ü***berwachungs***v***er***o***rdnung

VPN ***V***irtual ***P***rivate ***N***etwork

WKO ***W***irtschafts***k***ammer ***Ö***sterreich

1 Einleitung

Ausgangspunkt

In der heutigen Zeit verläuft ein Großteil der privaten und geschäftlichen Kommunikation über elektronische Medien. Durch das Nutzen von Telekommunikationsdiensten fallen große Mengen an Daten an, die von verschiedenen Stellen erzeugt, verarbeitet oder gespeichert werden – so genannte Verkehrsdaten. Sie sind keine Inhaltsdaten, geben aber trotzdem Aufschluss über unsere Aktivitäten, Lebensweise und Dienst-Nutzung. Der Staat hat einerseits durch Gesetze, wie das Telekommunikationsgeheimnis, der Datenschutz, das Briefgeheimnis und die Achtung der Privatsphäre, Regelungen getroffen, um die Interessen der Bürger zu wahren. Andererseits hat die Exekutive ein besonderes Interesse daran, Zugang zu diesen Verkehrsdaten zu erhalten, um diese Datenquelle für die Strafverfolgung nutzen zu können. In diesem Spannungsfeld liegt die von der EU kürzlich beschlossene Richtlinie über Data Retention.

Ziel

Im Zuge dieser Arbeit möchte ich herausfinden, welche Auswirkungen die EU-Richtlinie haben wird. Dies gilt sowohl für die Bürger der EU als auch für die Wirtschaft und für die rechtliche Situation in den EU-Ländern, insbesondere in Österreich.

Dabei bin ich von folgenden Hypothesen ausgegangen: Die Vorratsdatenspeicherung von Ruf- und Verkehrsdaten bedeutet einen tiefen Eingriff in die Privatsphäre der Bürger. Die fehlenden Regelungen über den Kostenersatz bedeutet eine zusätzliche massive finanzielle Belastung für die Anbieter von Telekommunikationsdiensten.

Vorgehensweise

Für den „State of the art" habe ich vor allem österreichische und später auch europäische Rechtstexte analysiert. Hierzu zählen unter anderem Abschnitt 12 des Telekommunikationsgesetzes, die Überwachungsverordnung, die Überwachungskostenverordnung, das Staatsgrundgesetz über das Fernmeldegeheimnis und die Strafprozessordnung über die Verhältnismäßigkeit auf österreichischer Ebene. Auf europäischer Ebene waren es Artikel 8 der Europäischen Menschenrechtskonvention, die Europäische Datenschutzrichtlinie und die EU-Richtlinie über die Vorratsdatenspeicherung. Aber auch Medienberichte und Websites von Gegnern und Befürwortern der Richtlinie sind in meine Arbeit eingeflossen.

Meine Diplomarbeit ordne ich den wissenschaftlichen Disziplinen Medienwissenschaften und Rechtswissenschaften zu.

Bei meiner Arbeit habe ich eine kompilatorische Vorgehensweise gewählt, da hier bereits bekannte Arbeiten einander gegenübergestellt und verglichen werden. Bei der Literaturauswertung habe ich alle relevanten, mir zugänglichen Quellen ausgeschöpft und die gewonnenen Informationen unter dem Gesichtspunkt meiner Themenstellung neu strukturiert.

Da Data Retention noch ein sehr junges Thema ist und es in den Medien – abgesehen von einigen Computer-Fachzeitschriften – kaum Berichterstattungen gegeben hat, wissen viele Bürger noch gar nichts von der bevorstehenden Vorratsdatenspeicherung. Aus diesem Grund war es mir auch nicht möglich, eine quantitative Methode einzusetzen sodass ich mich entschlossen habe, Leitfadeninterviews durchzuführen. Meine Interviewpartner Herrn Georg Chytil und Herrn

Ing. Martin Prager hat mir mein Betreuer vermittelt, wofür ich ihm sehr dankbar bin. Außerdem konnte ich mit Frau Mag. Judith Leschanz und Herrn Mag. Gert Paulhart von der mobilkom Austria sehr interessante Gespräche führen.

Weitere Interviewpartner zu finden war mir leider nicht möglich, da die arge daten (österreichische Gesellschaft für Datenschutz) und Quintessenz (Organisation zur Wiederherstellung der Bürgerrechte im Informationszeitalter) leider keine Zeit für mich hatten. Von vibe.at (Verein für Internet-Benutzer Österreichs), von der österreichischen Datenschutzkommission, die dem Bundeskanzleramt unterstellt ist, von Nicholas Hauser von der Gewerkschaft der Privatangestellten, von Michael Vesely, Präsident des „future network" der Österreichischen Plattform für IT-Entscheider und von Public Netbase (Institut für neue Kulturtechnologien) habe ich keine Antwort auf meine Anfrage bekommen.

Aufbau

Diese Diplomarbeit gliedert sich in fünf Kapitel, wobei das erste Kapitel die Einleitung darstellt. Im zweiten Kapitel werden die grundlegenden Begriffe erörtert, die in dieser Diplomarbeit häufiger verwendet werden und dienen zum Verständnis des Lesers.

Der inhaltliche Teil dieser Arbeit gliedert sich in zwei Hauptkapitel Kapitel 3 (Derzeitige rechtliche Lage) und Kapitel 4 (Data Retention). Da es in Österreich keine Bestimmungen zur Vorratsdatenspeicherung gibt, wurden Regelungen im Telekommunikationsgesetz, die Überwachungsverordnung und die Überwachungskostenverordnung erlassen, um im Ausnahmefall Überwachungsmaßnahmen treffen zu können. Dies wird im Kapitel 3 (Derzeitige rechtliche Lage) beschrieben. Kapitel 3.2 behandelt jene EU-Länder, in denen bereits

Data Retention durchgeführt wird. Frankreich und Spanien haben die Anbieter von Telekommunikationsdiensten dazu verpflichtet, Verbindungsdaten auf Vorrat zu speichern, in Großbritannien erfolgt dies auf freiwilliger Basis. Eine bindende und umfangreiche Vorratsdatenspeicherung, wie sie in der EU-Richtlinie vorgesehen ist, wird in keinem EU-Mitgliedsland praktiziert.

Kapitel 4 (Data Retention) behandelt in erster Linie die EU-Richtlinie über Vorratsdatenspeicherung. Es werden die Entstehungsgeschichte, Anlass und Ziele sowie treibende Kräfte und Gegner erörtert. Danach werden die eigentlichen Bestimmungen der Direktive behandelt. In einigen Punkten ist die Richtlinie nicht oder unzureichend definiert, sodass es zu Problemen bei der Umsetzung kommen wird. Weiters werden einige bestehende Rechtstexte – österreichische und europäische – verletzt. Die Umsetzung der Richtlinie wird sowohl Auswirkungen auf die Wirtschaft, als auch auf die Gesellschaft haben, weshalb im Kapitel 4.2 aufgezeigt wird, wie Private die Vorratsdatenspeicherung umgehen können.

Kapitel 5 legt abschließend nochmals die Ergebnisse dieser Arbeit dar.

2 Begriffserklärungen[1]

Dieser Abschnitt soll im Vorfeld grundlegende Begriffe zur Vorratsdatenspeicherung erklären, die in dieser Diplomarbeit öfter verwendet werden.

Anbieter stellen öffentliche Kommunikationsdienste zur Verfügung. Anbieter werden im Bereich des Internets häufig auch ***Provider*** genannt.

Benutzer nutzen laut Telekommunikationsgesetz einen öffentlichen Dienst entweder privat oder geschäftlich, *„ohne diesen Dienst zwangsläufig abonniert zu haben."*

Benutzerkennung oder ***Nutzerkennung*** ist laut EU-Richtlinie eine eindeutige Kennnummer, die einem Teilnehmer bei der Registrierung oder Abschließung eines Abonnements zugeordnet wird.

Betreiber unterhalten öffentliche Kommunikationsnetze.

Data Freeze oder ***Data Preservation***, darunter versteht man die Konservierung oder Bewahrung von Daten. Diese ***anlassbezogene Speicherung*** hat nach Axel Heyer zum Ziel, einzelne (potentiell) verdächtige User zu überwachen, also deren Kommunikationsdaten abzufangen und zu speichern. Die Daten, die bei Data Freeze gespeichert werden, würden im Normalfall baldigst gelöscht werden.

Daten sind nach der EU-Richtlinie Verkehrs- und Standortdaten und alle Informationen, die damit in Zusammenhang stehen und nötig sind, um den Teilnehmer oder Nutzer festzustellen. Inhaltsdaten wurden in der EU-Richtlinie gesondert definiert.

---

1 Die meisten Definitionen stammen aus dem Lexikon der Kommunikations- und Informationstechnik von Niels Klußmann.

Dienste oder ***Services*** sind nach Niels Klußmann im Bereich der Telekommunikation die Fähigkeiten des Netzes, Nachrichten zu übertragen und einem anderen Nutzer bereit zu stellen. Beispiele hierfür sind Telefonie, Fax, Internet oder E-Mail. ***Öffentliche Dienste*** und ***Netze*** sind für jedermann gegen eine angemessene Gebühr zugänglich.

Dienste mit Zusatznutzen oder ***Mehrwertdienste*** sind Dienste, die erfordern, dass Verkehrs- oder Standortdaten über die normale Nutzung hinaus verarbeitet oder erhoben werden. Ziel dabei ist es immer, dem Kunden einen erhöhten Nutzen zu bringen. Beispiele hierfür sind R-Gespräche oder die Auskunft.

Domain bezeichnet nach Jürgen Weinknecht „die eindeutige, einmalige Adresse im Internet, unter der ein physikalischer oder virtueller Server erreichbar ist. Vor allem durch letzteres Merkmal [...] unterscheidet sich die Domain von den URLs (Unique bzw. Uniform Resource Locators), die zwar in ihrer Gesamtzusammestellung ebenfalls einmalig sein müssen, aber auch einzelne Verzeichnisse oder HTML-Seiten auf einem Server bezeichnen können." z.B. fh-burgenland.at

Erfolglose Anrufversuche sind nach EU-Richtlinie Telefonanrufe, bei denen eine Verbindung zu Stande gekommen ist, der Anruf blieb aber unbeantwortet, oder das Netzwerkmanagement hat eingegriffen. Ein Beispiel hierfür ist, dass der Anruf zur Mobilbox umgeleitet wird, wo der Anrufer eine Nachricht hinterlassen kann.

Funkzellen oder ***Zellen*** sind die Bereiche, die von Sendemasten, so genannten Basisstationen eines Mobilfunknetzes, abgedeckt werden. Normalerweise überlappen die Zellen von benachbarten Sendemasten und das Endgerät sucht nach dem Sender mit dem stärksten Signal. Die Übergabe von einer Zelle zur nächsten wird als ***Handover*** bezeichnet. Durch die Einbuchung in eine Zelle lässt sich die Position des Endgeräts feststellen, da jede Funkzelle durch eine eindeutige ***Cell-ID*** gekennzeichnet ist.

IMEI-Nummer: „***I***nternational ***M***obile ***E***quipment ***I***dentity", ist die internationale Geräteseriennummer des Mobiltelefons, die am Gerät gespeichert wird. Die IMEI besteht aus bis zu 15 Ziffern, die aus Typzulassung, Endfertigungsnummer und Seriennummer bestehen.

IMSI-Catcher (Fox 2002) lesen die IMSI auf der SIM-Karte des Mobiltelefons aus. Für das Handy simuliert der Catcher eine Funkzelle und Mobiltelefone buchen sich auf dem Catcher ein. Dadurch lässt sich der Standort eines Mobiltelefons innerhalb einer Funkzelle eingrenzen. Die Catcher werden hauptsächlich zum Mithören von Telefondaten verwendet.

IMSI-Nummer: „***I***nternational ***M***obile ***S***ubscriber ***I***dentity", also die internationale Kennummer des Nutzers, ist auf der SIM-Karte des Mobiltelefons gespeichert. Dies ist nicht die Telefonnummer. Die IMSI besteht ebenfalls aus bis zu 15 Ziffern, bestehend aus Mobile Country Code, Mobile Network Code und Mobile Subscriber Identity Number.

Inhaltsdaten sind laut EU-Richtlinie die Inhalte der Nachricht, also das Gespräch selbst, der Text einer SMS oder E-Mail, der Inhalt einer MMS oder Ähnliches.

Inhaltsüberwachung umfasst das *„Mithören, Abhören, Aufzeichnen oder sonstige Überwachen"* von Inhaltsdaten.

IP-Adressen (Internet Protocol Adressen) dienen zur logischen Adressierung von Geräten in Netzwerken. Ein Host (z.B. Computer, Router, Switch ...) besitzt mindestens eine IP-Adresse, die eindeutig ist. Dadurch können die Geräte im Netzwerk miteinander kommunizieren.

Juristische Personen sind durch einen Rechtsakt geschaffene Rechtssubjekte. Im öffentlichen Recht sind dies Bund, Land oder Gemeinden und im Privatrecht beispielsweise Stiftungen, Aktiengesellschaften, Gesellschaften mit beschränkter Haftung oder Genossenschaften.

Natürliche Personen sind nach dem Allgemeinen Bürgerlichen Gesetzbuch (ABGB) Menschen, deren Rechtsfähigkeit mit der Geburt anfängt und mit dem Tod endet.

Peer to Peer (P2P) bezeichnet die Kommunikation unter gleichgestellten, anonymen Usern. In diesen Netzwerken können alle PCs Dienste sowohl in Anspruch nehmen als auch zur Verfügung stellen. P2P-Netzwerke sind vor allem durch Tauschbörsen bekannt, wo User untereinander Dateien austauschen.

Phishing setzt sich aus ***P***assword, ***H***arvesting und F***ishing*** zusammen und bedeutet wörtlich das Abernten oder Abfischen von Passwörtern. Dieses Abfragen von Passwörtern oder anderen geheimen Daten wird insbesondere bei Zugangsdaten zu Online-Banking-Applikationen angewandt.

Proxy oder ***Proxyserver*** dienen zur Vermittlung und zur Steigerung der Effizienz des Datenverkehrs in Netzwerken. Für einen Server verhält sich der Proxy wie ein Client, für einen Client wie ein Server.

Rufdatenrückerfassung bezeichnet die Auswertung von Verbindungsdaten und stellt fest, welche Teilnehmeranschlüsse Ursprung oder Ziel der Kommunikation waren. Auch die Zusammenführung von IP-Adresse und Stammdaten ist ein Teil der Rufdatenrückerfassung.

Stammdaten, Bestandsdaten oder ***Grunddaten*** sind Daten, die für das Abschließen, Ändern oder Beenden eines Vertrages zwischen Anbieter und Benutzer erfasst werden. Die Daten umfassen nach TKG den akademischen Grad, den vollständigen Namen, die aktuelle Adresse, Informationen über den Vertrag und die Liquidität des Kunden und die Teilnehmernummer, also die Telefonnummer oder statische IP-Adresse oder andere Identifizierungsnummern, die zur Zustellung der Nachricht benötigt werden.

Standortbestimmung oder ***Standortpeilung*** ist die Lokalisierung des Endgeräts. In der EU-Richtlinie wird die Standortkennung als Kennung der Funkzelle definiert, von der aus eine Verbindung aufgebaut wird, oder in der sie beendet wird.

Standortdaten geben Aufschluss über den geografischen Standort des Endgeräts.

Teilnehmeranschluss ist die technische Einrichtung, die Ursprung oder Ziel einer Kommunikation ist. Über den Teilnehmeranschluss wird das Endgerät mit dem Netz verbunden.

Telefondienste sind nach EU-Richtlinie Anrufe inklusive Mail-Boxen, Konferenzschaltungen und Daten. Zu Telefondiensten zählen auch Zusatzdienste wie Rufumleitung, Mitteilungs- sowie Multimediadienste.

Übernahmeschnittstelle ist die ***Schnittstelle***, über die der Betreiber die Überwachungs-Maßnahme für die Strafverfolgungsbehörde technisch ermöglicht. Sie ist somit der technische Übergabepunkt beim Betreiber zur Strafverfolgungsbehörde. Hier wird die zu überwachende Kommunikation bereitgestellt.

Uniform Resource Locator (URL) dient zur eindeutigen Adressierung von jeglicher Ressource im World Wide Web. URLs bestehen aus der Angabe des Protokolls (http, ftp,...), des Trennzeichens „:“, „//“, Hostname des Servers und bei Bedarf :Port, wenn nicht der Standard-Port verwendet wird und dann die Pfadangabe. (http://<host> :<port>/<pfad>?<parameter>) z.B.: https://mail.fh-burgenland.at/

Verkehrsdaten umfassen sämtlichen Daten, die für die Weiterleitung einer Nachricht in einem Kommunikationsnetz benötigt werden, das sind Verbindungs- und Standortdaten. Welche dynamische IP verwendet und welche Website aufgerufen wurde, wird ebenfalls erfasst. Sie werden auch für die Verrechnung verwendet.

Vorratsdatenspeicherung oder ***Data Retention*** bedeutet die pauschale Speicherung von *„Stammdaten, Verbindungsdaten und Standortdaten, jedoch keine Inhaltsdaten“* auf Vorrat zum Zweck der Vorbeugung, Untersuchung und Verfolgung von strafbaren Handlungen.

Wireless Local Area Network (***WLAN***) ist ein kabelloses lokales Funknetzwerk. Durch Wireless LANs ist es innerhalb eines begrenzten Raums möglich, mehrere Geräte über Funk zu vernetzen und mit dem Internet zu verbinden. Für den Aufbau von WLANs benötigt man eine WLAN-Karte auf dem Rechner, falls diese nicht bereits im Laptop vorhanden ist, und eine zentrale Basisstation (Access Point). ***Hotspots*** sind öffentliche, zumeist kostenpflichtige Access Points.

3 Derzeitige rechtliche Lage[2]

3.1 Rechtslage in Österreich

Jeder österreichische Staatsbürger hat das verfassungsrechtlich gewährleistete Recht auf das Fernmeldegeheimnis (StGG 1867:Art. 10a), das nicht verletzt werden darf. Das bedeutet eine freie Wahl des Kommunikationspartners, ohne dass der Staat die Kommunikation mithören darf.

Die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten sichert ebenfalls die Vertraulichkeit der Kommunikation. Weiters gibt es das Recht auf informationelle Selbstbestimmung, welches gewährleistet, dass jeder Bürger selbst bestimmen darf, wann er personenbezogene Daten weitergeben will. Dabei wird nicht unterschieden, ob es sich um sensible Daten handelt oder nicht.

Dennoch ist es notwendig, dass die gespeicherten Daten den Strafverfolgungsbehörden zur Verfügung gestellt werden können, um schwere Straftaten aufzuklären. Da es in Österreich keine verpflichtende Vorratsdatenspeicherung gibt, bestehen gesetzliche Regelungen, wobei das schützenswürdige Interesse des Einzelnen hinter das Interesse des Staates gestellt wird, um eine Aufklärung zu ermöglichen. Dieses Prinzip der Verhältnismäßigkeit ist im §29 Sicherheitspolizeigesetz geregelt.

[2] Viele dieser Informationen wurden im Zuge von Leitfadeninterviews mit Frau Mag. Judith Leschanz, Head of Legal Expert Center der mobilkom Austria AG & Co KG, und Herrn Georg Chytil, Präsident des Verbandes ISPA, erarbeitet und vertieft.

3.1.1 Überwachungsmöglichkeiten in Österreich

In Österreich gibt es zurzeit keine Regelungen zur Vorratsdatenspeicherung, die für die Strafverfolgung oder für die Gewährleistung der nationalen Sicherheit genutzt werden könnten. Dennoch existieren Bestimmungen bezüglich der Telekommunikationsüberwachung für die Inhalts- beziehungsweise Verkehrsdatenüberwachung. Die gesetzliche Grundlage findet sich in der Strafprozessordnung (StPo 1975: §149a-149p), die genau definiert, was Überwachung ist, in welchen Fällen sie angeordnet werden darf, wer sie anordnen darf und welchen Inhalt dieser Beschluss haben muss.

Sämtliche Überwachungen bedürfen eines richterlichen Beschlusses eines Untersuchungsrichters oder eines Gerichtshofs; ein Beschluss eines Bezirksrichters ist nicht ausreichend. Die Richter können sich dabei von Gutachtern beraten lassen, und zwar entweder von Vertretern der Betreiber oder von gerichtlich beeideten Gutachtern. Weiters darf eine Überwachung nur angeordnet werden, wenn das Verbrechen, das aufgeklärt werden soll, mit mehr als einem Jahr Freiheitsstrafe geahndet wird. Beispielsweise darf wegen eines Diebstahls keine Überwachung angeordnet werden, da hier das Strafmaß im Normalfall maximal sechs Monate beträgt. Die Anordnung für die Rufdatenrückerfassung beziehungsweise für eine Standortpositionierung muss schriftlich erfolgen. Sie hat den Namen, die Anschrift sowie die Rufnummer oder sonstige Kennung der zu überwachenden Person zu enthalten. Auch muss die Art, die Dauer und der Umfang der Maßnahme festgelegt werden. Bei Gefahr im Verzug kann eine Überwachung auch ohne diesen Beschluss angeordnet werden. Dann muss die richterliche Anordnung allerdings umgehend nachgereicht werden.

3.1.1.1 Telefonie

Im Bereich der Telefonie gibt es derzeit die Rufdatenrückerfassung, die Kommunikationsüberwachung und die Standortpeilung.

Die ***Rufdatenrückerfassung*** bezieht sich nur auf Daten aus der Vergangenheit. Es werden daher nur vorhandene Verkehrsdaten ausgewertet, zum Beispiel, wer mit wem wie lange telefoniert hat. Das Leitfadeninterview mit Frau Mag. Judith Leschanz, Rechtsexpertin der mobilkom austria AG & Co KG, hat ergeben, dass hauptsächlich Daten aus den letzten drei Monaten abgefragt werden. Daten, die zwischen drei und sechs Monate alt sind, werden selten, ein Jahr alte Daten kaum beauskunftet, da diese für Ermittlungen nicht mehr relevant sind.

Im Gegensatz dazu erfolgt die ***Kommunikationsüberwachung*** in Echtzeit, also dann, wenn die überwachte Person tatsächlich telefoniert.

Außerdem kann zusätzlich noch eine ***Standortpeilung*** durchgeführt werden, mit deren Hilfe die Funkzelle ermittelt werden kann, in welcher der Teilnehmer telefoniert oder das Mobiltelefon eingebucht ist. Die Peilung kann ebenfalls nur in Echtzeit erfolgen. Zur Standortbestimmung wird an das Endgerät eine für den Nutzer nicht erkennbare Aufforderung zur Identifizierung gesandt. Dieser Vorgang wird auch *„stealthy ping"* genannt. Wenn das Handy eingeschalten ist, antwortet es der Basisstation ebenfalls für den Benutzer unbemerkt. Die Basisstation wird dann über die Cell-ID identifiziert und das Endgerät kann so lokalisiert werden. Diese Standortpeilung ist in größeren Städten genauer, da hier mehr Sender für die Netzabdeckung zur Verfügung stehen als in weniger besiedelten oder landwirtschaftlich genutzten Gegenden, wo eine Funkzelle mehrere Quadratkilometer abdeckt. Daher ist die Standortbestimmung im Mobilfunk immer von der Reichweite der Funkzelle abhängig.

Die folgende Tabelle zeigt die Relevanz von Rufdatenrückerfassung in Österreich auf. Darin ist ersichtlich, dass die Zahl von Rückerfassungen und Inhaltsdaten rasant angestiegen ist. Dies könnte möglicherweise auf das enorme Wachstum des Marktes zurückgeführt werden. Wie viele dieser Anfragen wirklich für den Erfolg der Ermittlung ausschlaggebend waren, ist nicht öffentlich bekannt. Eine Statistik über die Anzahl von Abfragen von Bestandsdaten liegt ebenfalls nicht vor.

Tabelle 1: Verfahren, bei denen Rufdatenrückerfassung stattfand.

Jahr	Verfahren	Betroffene Anschlüsse	Davon nur Rufdaten-rückerfassung	Davon Inhaltsüber-wachung
1997	444	751	509	141
1998	493	804	618	k.A.
1999	496	1228	932	275
2000	759	1479	1069	410
2001	787	1721	1257	464
2002	993	2964	1423	641

Quelle: Wik-Consult Studie 2004

Festnetz-Telefone sind im Gegensatz zu Mobiltelefonen drahtgebunden, also durch eine eigene physikalische Leitung an einen örtlich festgelegten Anschluss angebunden. Die Weitergabe der Gespräche innerhalb des Netzes erfolgt über Vermittlungsstellen. Die Ortsvermittlungsstelle vermittelt die Gespräche der Teilnehmer und speichert Daten über den jeweiligen Anschluss, wie beispielsweise die Anschlussart (ISDN, ASDL, ...), die gebuchten Services und Informationen zur Abrechnung. Nachdem nun ein Festnetz-Telefon fest mit dem Netz verbunden ist und dem Teilnehmer eine eindeutige Nummer zugewiesen ist, kann der Anschluss leicht identifiziert werden.

Bei internationalen Anfragen zur Beauskunftung von Stammdaten, sowohl im Bereich Internet als auch bei Mobil- und Festnetz-Telefonie, ist ein Amtshilfeverfahren notwendig. Das bedeutet, dass das ausländische Gericht ein österreichisches Gericht anrufen muss. Der österreichische Richter erlässt nach Prüfung den nötigen Beschluss, um die Weitergabe der Daten zu veranlassen. Das betroffene Unternehmen gibt die angefragten Informationen regulär an das Bundesministerium für Inneres weiter und verrechnet die entstandenen Kosten dem beauftragenden Gericht. Amtshilfeverfahren sind meist sehr zeitintensiv und häufig wurden die angefragten Daten vom Provider bereitsgelöscht, bevor die Anfragen bei ihnen einlangen.

3.1.1.2 Internet

Wenn ein Kunde eines ISPs in kriminelle Handlungen verwickelt ist oder derer verdächtigt wird, müssen die Provider sämtliche vorhandenen Stammdaten und Verkehrsdaten des beschuldigten Kunden an die Strafverfolgungsbehörden weitergeben. Sowohl Durchleitungs- als auch Host Provider müssen auf Grund eines richterlichen Beschlusses jene Daten übermitteln, die zur Bekämpfung oder Aufklärung von Straftaten dienen. Zumindest sind die Stammdaten, also Name und Wohnanschrift des Nutzers, zu beauskunften.

Computer sind über die zugewiesene IP-Adresse identifizierbar. Um den Rechner des Urhebers einer Kommunikation festzustellen, ist es nötig, die Uhrzeit mitaufzuzeichnen, um herausfinden zu können, wem welche IP zu einem bestimmten Zeitpunkt zugeordnet war und welche Websites der Inhaber der IP wann aufgerufen hat. In einigen Netzwerken sind allerdings unterschiedliche Zeiten auf den Rechnern eingestellt, was Unschärfen bei der Auswertung nach sich ziehen kann. Um das Ziel einer Kommunikation festzustellen, wird die Zieladresse der Nachricht ermittelt.

Wird dem Kunden dieselbe IP-Adresse permanent zugeordnet (statische IP), zählt dies zu den Stammdaten und muss bei einer Beauskunftung von Stammdaten mit angegeben werden. Dynamische IP-Adressen werden dem Kunden bei jeder Anmeldung ins Netz neu zugewiesen und müssen im Zusammenhang mit den Zugangsdaten des Kunden ausgewertet werden.

Da dynamische IPs dem Telekommunikationsgesetz (TKG 2003:§92 Abs.3) nach Verkehrsdaten sind, dürfen sie nicht gespeichert werden, sondern müssen nach Erbringung des Dienstes sofort gelöscht oder anonymisiert werden. Nach Auskunft der Wirtschaftskammer Österreich sind ältere IP-Adressen oftmals gar nicht mehr verfügbar. Der Tatsache, dass dynamische IP-Adressen laut Telekommunikationsgesetz umgehend gelöscht werden müssen, widerspricht ein Urteil des Obersten Gerichtshofs von 26. Juli 2005 (11 Os 57/05z). Darin wird ausgeführt, dass Access-Provider in Fällen von Urheberrechtsverletzungen Auskunft über den Inhaber einer IP erteilen müssen, und zwar unabhängig davon, ob es sich dabei um eine statische oder dynamische IP-Adresse handelt.

In der Praxis erfolgt die Beauskunftung so, dass ein Techniker die angefragten Daten auswertet und ein Polizist ein Protokoll aufnimmt. Die Anfragen bei Providern sind sehr unterschiedlich, so Georg Chytil. Es erfolgt also keine elektronische Übermittlung der Daten.

3.1.2 Regelungen des Telekommunikationsgesetzes

Der Abschnitt 12 des Telekommunikationsgesetzes über *„Kommunikationsgeheimnis und Datenschutz"* regelt die Rechte und Pflichten der Betreiber. Demnach sind alle Betreiber verpflichtet, an einer Überwachung mitzuwirken (TKG 2003:§94) und die technischen Einrichtungen dafür bereit zu halten. Das bedeutet, dass die erfassten Daten beim Provider gespeichert werden und im Bedarfsfall von den Strafverfolgungsbehörden abgefragt werden können. Für die Mithilfe bei Überwachungen ist ein *„angemessener Kostenersatz"* vorgesehen.

Weiters sind alle Betreiber zur Geheimhaltung (TKG 2003:§93) verpflichtet. Dieses Kommunikationsgeheimnis umfasst alle Inhaltsdaten, Verkehrsdaten und Standortdaten. Das bedeutet auch, dass die Anbieter Nachrichten nicht überwachen dürfen. Auch das Aufzeichnen von den damit zusammenhängenden Standort- und Verkehrsdaten sowie die Weitergabe von Informationen ist untersagt. Für den Fall, dass ein Betreiber gegen das Kommunikationsgeheimnis verstößt und Daten weitergibt, die Nachricht in irgendeiner Form verfälscht oder *sie „unbefugt dem Empfangsberechtigten vorenthält"*, kann vom Gericht eine Freiheitsstrafe von bis zu drei Monaten und eine Geldstrafe von bis zu 180 Tagessätzen verhängt werden.

Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten dürfen nur für die Diensteerbringung verwendet werden und müssen auf das absolute Minimum beschränkt werden. Die Frage, die sich diesbezüglich stellt ist, in wieweit die Planung und Instandhaltung der Systeme zur Diensteerbringung zählen. Immerhin müssen die Betreiber die vorhandenen Daten auswerten, um eine optimale Netzauslastung und Netzabdeckung zu ermöglichen.

Die Betreiber dürfen (TKG 2003:§97) nur Stammdaten erfassen und verarbeiten, die notwendig sind, um Verträge abzuschließen, sie zu ändern oder sie zu beenden. Sie dürfen diese Datenart auch nur zur Rechnungslegung verwenden oder um Auskünfte an Notrufe erteilen zu können. Stammdaten müssen spätestens nach Vertragsende gelöscht werden (TKG 2003:§97 (2)). Dem wiederum widerspricht allerdings das Steuerrecht (BAO 2005:§132), das besagt, dass alle Bücher und Aufzeichnungen sowie die dazugehörigen Belege sieben Jahre lang aufzubewahren sind. Dazu gehören alle Informationen, die für die Steuererhebung von Bedeutung sind, wie beispielsweise alle Rechnungen, Verträge, Leistungsverzeichnisse und Korrespondenzen. Für die Rechnung muss auch festgehalten werden, wie die Leistung berechnet wurde. Das bedeutet in diesem Fall, wie viele Einheiten verrechnet wurden.

Zudem werden derzeit nur Daten über Kommunikation aufgezeichnet, die tatsächlich statt gefunden hat, erfolglose oder nicht zustande kommende Gespräche werden nicht erfasst, da diese Daten nicht für die Rechnungslegung relevant sind.

Inhaltsdaten dürfen von Providern nicht aufgezeichnet werden, es sei denn, es ist für die Erbringung eines Dienstes unbedingt nötig. In diesem Fall müssen die Daten unmittelbar nach Diensteerbringung gelöscht werden. Das Problem dabei ist, dass ein Teil der URL der besuchten Websites Verbindungsdaten und ein anderer Teil bereits Inhaltsdaten sind. Dies könnten beispielsweise dynamische Teile oder Informationen aus Formularen sein. Herr Georg Chytil, Präsident des Verbandes ISPA, meint hierzu, dass beim Surfen im Internet die besuchten Websites in Logfiles bei einigen Anbietern aufgezeichnet werden, die zu den Verbindungsdaten zählen. Da allerdings die gesamte Kommunikation nachvollziehbar ist, kann man durchaus

auch von Inhaltsdaten sprechen. Dadurch ist es möglich, auch ohne das Aufzeichnen der Inhalte die gesamte Kommunikation der User zu reproduzieren.

Auch werden bei E-Mails normalerweise die Header mitgeloggt, allerdings ohne die Betreffzeile, um den Datenschutz zu gewährleisten. Stattdessen wird eine eindeutige Message-ID, Sender und Empfänger des Mails und die Eingangs- und Ausgangszeit mitgeloggt, um die E-Mail später leichter auffindbar zu machen.

Bestandsdaten dürfen für Marketingzwecke oder für das Anbieten von Mehrwertdiensten verwendet werden, wenn der Teilnehmer dem ausdrücklich zugestimmt hat. Diese „Anmeldung" wird auch als opt-in bezeichnet. Der Benutzer muss jederzeit die Möglichkeit haben, diese Zustimmung zu widerrufen.

Die Informationen, die für die Rechnungslegung verwendet werden, müssen möglichst gering gehalten werden. Einzelentgeltnachweise dürfen die Angaben über Telefonnummern, die angerufen wurden, nur in verkürzter Form darstellen, um den Datenschutz zu gewährleisten. Bei vielen Betreibern kann man auch einen unverkürzten Einzelentgeltnachweis bestellen, wenn der Nutzer versichert, die Mitbenutzer und die angerufenen Teilnehmer darüber zu informieren, dass die Teilnehmernummern vollständig und nicht anonymisiert dargestellt werden.

3.1.3 Regelungen der Überwachungsverordnung

Basierend auf dem Telekommunikationsgesetz wurden 2001 vom Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) die Überwachungsverordnung und 2004 die Überwachungskostenverordnung erlassen, um die Regelungen des TKG zu spezifizieren. Die Überwachungsverordnung regelt die von den Betreibern zur Verfügung zu stellenden Funktionen und technischen Einrichtungen im Detail. Die Überwachungskostenverordnung regelt den Kostenersatz für den durch die Überwachungsverordnung entstandenen Aufwand.

3.1.3.1 Technische Schnittstelle

Nach der Überwachungsverordnung müssen die Anbieter in ihren Anlagen Funktionen bereithalten, die eine aktive Mitarbeit an einer Überwachung ermöglichen. Sie müssen im Einzelfall die Kommunikation überwachen können und sonstige für die Überwachung relevanten Informationen zur Verfügung stellen. Es ist jedoch nicht geregelt, ob die übertragenen Kundendaten vom Anbieter weiterverarbeitet oder gespeichert werden dürfen.

Die Überwachung erfolgt über eine Schnittstelle, die auf dem ETSI-Standard ETSI TS 101 331 V1.1.1[3] basiert und entweder als Wähl- oder Festverbindung realisiert werden kann. Dieser Standard trägt den Titel Telecommunications Security; Lawful Interception; Requirements of Law Enforcement Agencies (LEAs) und definiert Normen für Anforderungen an die Übergabeschnittstelle für legale Telekommunikations-Überwachung. Der ETSI-Standard definiert somit die Zugriffsmöglichkeiten auf GSM, GPRS, ISDN, PSTN (Festnetz), TETRA und UMTS-Netzwerke.

[3] Diese Norm basiert auf dem umstrittenen Enfopol 98 Dokument und orientiert sich an den "International User Requirements". Die User sind in diesem Fall die Strafverfolgungsbehörden (LEAs).

Im Bereich des Internets gibt es derzeit de-facto-Standards zur Speicherung von Daten, so Georg Chytil. So werden E-Mail Logfiles meist so gespeichert, wie sie in der Applikation Sendmail aussehen, Web Logfiles so wie in den Applikationen Appache oder Internet Information Server. Dies kann ein Problem bei der Zusammenführung von Daten darstellen, wenn sie in unterschiedlichen Formaten vorliegen. Dann müssen sie zunächst in ein einheitliches Format übertragen werden, um sie dann korrelieren und auswerten zu können. Außerdem ist häufig auf den Rechnern nicht dieselbe Uhrzeit eingestellt, sodass es zu Unschärfen bei der Auswertung der Aufzeichnung kommen kann.

Weiters muss die Schnittstelle technisch die folgenden Anforderungen erfüllen:

- Sie darf nur die Kommunikation der überwachten Stelle bereitstellen.
- Die Qualität muss die gleiche sein, wie sie der überwachten Stelle geboten wird.
- Übertragen wird das Ergebnis der Überwachung über *„genormte, allgemein verfügbare Übertragungswege und Protokolle"*.
- Der Standard ETSI TS 101 331 V1.1.1 muss eingehalten werden.

Außerdem muss das System so gestaltet sein, dass weder die Beteiligten der Kommunikation, also der Angerufene und der Anrufer, noch Dritte, die nicht an der Überwachungsmaßnahme beteiligt sind, dies feststellen können. Der Zugang zum Netz ist ebenfalls ein Bestandteil der Schnittstelle. Sie ist durch aktuelle technische Maßnahmen vor dem Zugriff oder der Kenntnisnahme zu schützen. Zur Übertragung der überwachten Kommunikation muss eine Festverbindung oder eine ISDN-Wählverbindung verwendet werden. Wenn dies nicht möglich ist, muss auf ein ähnlich schnelles Übertragungsnetz zurückgegriffen werden. Falls Inhaltsdaten und andere Daten übermittelt werden müssen, so muss dies auf von einander getrennten Wegen geschehen.

3.1.3.2 Bereitzuhaltende Funktionen

Die Überwachungsverordnung schreibt die Funktionen vor, die von den Betreibern bereitzuhalten sind. Die Verpflichtungen betreffen die Anbieter nur, wenn ihnen dies wirtschaftlich und technisch zumutbar ist.

Im Einzelfall muss die Kommunikation eines Anschlusses aufgezeichnet werden können. Die Anbieter müssen ebenfalls jene Daten speichern können, die an einen Datenspeicher, also Voice- und Mail-Boxen, gesandt werden, beziehungsweise aus ihm abgerufen werden. Außerdem müssen sie Leistungen bereitstellen, um die Inhaltsdaten und die damit zusammenhängenden Daten zur Verfügung stellen zu können. Zu diesen Daten zählen:

- die Adresse des überwachten Teilnehmeranschlusses. Unter Adresse versteht man in diesem Fall alle Elemente, die zur Festlegung des Ziels einer Verbindung benötigt werden. Dies können die Rufnummer, IMEI, IMSI, IP (bei dynamischen IPs inklusive der genauen Uhrzeit) oder sonstige Adressierungselemente sein,
- die gewählten (eventuell unvollständigen) Adressen, auch bei erfolglosen Verbindungsversuchen,
- der technische Grund für den Abbruch oder Nichtzustandekommen der Verbindung,
- bei Um- oder Weiterleitung die Ziel-Adresse und bei virtuellen Anschlüssen die jeweiligen Teilnehmeranschlüsse, die auch als physikalische Anschlüsse bezeichnet werden,
- die angeforderten Dienste oder das Dienstemerkmal,
- im Mobilfunk die Cell-ID.

Falls die oben genannten Daten nicht erhoben werden können, so müssen zumindest Beginn, Ende und Dauer der Verbindungen erfasst werden.

3.1.4 Regelungen der Überwachungskosten-verordnung

Grundsätzlich ist im TKG vorgesehen, dass die anfallenden Kosten einer Überwachung den Betreibern ersetzt werden. Außerdem ist es laut Urteil des Verfassungsgerichtshofs aus dem Jahr 2003 unzulässig, nur die Betriebskosten zu ersetzen. Deshalb haben vor Erlassung der Verordnung eingehende Diskussionen zwischen dem Bundesministerium für Justiz und dem Fachverband der TK- & Rundfunkunternehmer statt gefunden. Nach der Wik-Consult Studie für BITKOM[4] (2004:72) hat der Fachverband *„erreicht, dass die Frage des Kostenersatzes für die Investitionen in die Überwachungseinrichtungen nicht in der ÜKVO geregelt wurde, vielmehr wird diese Frage in gesonderten Verhandlung mit den beteiligten Ministerien beraten. Somit besteht in Österreich die Aussicht auf eine Entschädigung der Kapitalkosten."*

Daraufhin wurde im Jahr 2004 korrespondierend zur Überwachungsverordnung die Überwachungskostenverordnung erlassen, um den Providern den Aufwand, der durch die Überwachung entsteht, erstatten zu können. Insbesondere sind die Tarife für den Kostenersatz festgelegt. Dieser Ersatz deckt zwar nicht sämtliche anfallenden Kosten, doch wird zumindest ein Teil davon beglichen.

[4] Bitkom: deutscher Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Die Kosten, die geltend gemacht werden können, umfassen die Instandhaltung und die Kontrolle der Überwachungseinrichtungen sowie die Beauskunftung an das Gericht beziehungsweise an die Sicherheitsstelle. Wenn für die Überwachung zusätzliche Geräte transportiert werden müssen, können auch diese Belastungen geltend gemacht werden. Außerdem wird den Providern eine so genannte *„Sekretariatspauschale"* gewährt, das bedeutet, dass Kosten für die Aufbereitung und Übermittlung der Daten ebenfalls vergütet werden. Investitionskosten werden den Betreibern nicht ersetzt. Wenn Leistungen zwischen 22.00 und 6.00 Uhr oder am Wochenende oder an Feiertagen erbracht werden müssen, dann erhält der Anbieter einen Zuschlag von 100%.

In der Praxis ist die Abwicklung des Kostenersatzes aufwändig, so Wik-Consult. Die Rechnungslegung erfolgt dezentral, was bedeutet, dass eine Einzelfallabrechnung an jenes Gericht gestellt wird, das die Überwachung angeordnet hat. Der Richter entscheidet dann auf Basis der Tarife der Überwachungskostenverordnung (ÜKVO) über die Höhe des Ersatzes. Dies bedeutet einen hohen Aufwand bei der Kostenerstattung sowohl für die Unternehmen, als auch für die Gerichte. Daher gibt es von beiden Seiten den Wunsch nach einer Standardisierung.

3.2 EU-Länder mit verbindlicher Vorratsdatenspeicherung[5]

Im Gegensatz zu Österreich bestehen in einigen EU-Mitgliedsländern gesetzliche Regelungen zur Vorratsdatenspeicherung beziehungsweise zur Data Preservation. Eine verpflichtende und umfassende Vorratsdatenspeicherung, wie sie in der EU-Richtlinie geplant ist, wird allerdings in keinem Land praktiziert (ISPA Positionspapier 2005:2).

In Frankreich und Spanien ist die Vorratsdatenspeicherung für die Anbieter von Telekommunikationsdiensten verpflichtend, hingegen wird in Großbritannien Data Retention auf freiwilliger Basis durchgeführt. Diese drei Staaten haben oft auch andere zusätzliche Regelungen als die übrigen EU-Mitgliedsstaaten, wie beispielsweise bei der Verwendung von Daten für unternehmenseigene Zwecke.

3.2.1 EU-weite Regelungen

Nach Umsetzung der Europäischen Datenschutzrichtlinie müssen in allen EU-Ländern die Verkehrsdaten anonymisiert oder gelöscht werden, sobald sie für die Diensterbringung, die Gewährleistung der Netzsicherheit oder die Rechnungslegung nicht mehr benötigt werden. Ansonsten dürfen sie bis zum Ende der Einspruchsfrist auf die Rechnung gespeichert werden. Diese beträgt zumeist sechs Monate. In Großbritannien dürfen die gespeicherten Daten dann gelöscht oder anonymisiert werden, wenn sie nicht mehr für geschäftliche Zwecke verwendet werden.

[5] Die Grundlage für dieses Kapitel bildet die Wik-Consult Studie für BITKOM „Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich". Die enthaltenen Informationen wurden geprüft und unter dem Gesichtspunkt der Themenstellung neu strukturiert.

Die erfassten Daten dürfen nur zweckbezogen verwendet werden und dürfen auch nur mit Zustimmung des Nutzers wiedergegeben werden. Zudem müssen Teilnehmer in der Regel zustimmen, dass ihre Daten für Marketingzwecke und für das Anbieten von Mehrwertdiensten verwendet werden (opt-in). Das Versenden von unerwünschten Werbe-Mails ist ebenfalls untersagt. In Spanien ist elektronische Werbung grundsätzlich verboten, außer sie wird innerhalb eines Vertragsverhältnissens angewandt, was einen Widerspruch in sich darstellt.

In vielen Mitgliedesländern gibt es auch Ausnahmeregelungen für die Auskunftserteilung an im Einsatz befindliche Notrufdienste.

In den Niederlanden dürfen alle gespeicherten Daten zur Missbrauchsbekämpfung verwendet werden. Ferner müssen die Bestandsdaten erst ein Jahr nach Beendigung des Vertragsverhältnisses gelöscht werden.

3.2.2 Frankreich

In Frankreich wird die ***Data Retention*** im Gesetz zur Alltagssicherheit aus dem Jahr 2001 geregelt. Außerdem ist der Gebrauch von Kryptografie in Frankreich beschränkt. Daher müssen Produkte, die Verschlüsselung erlauben, staatlich lizenziert werden. Nutzen darf man den Schlüssel nur dann, wenn er bei staatlichen Stellen, wie dem Service Central de la Sécurité des Systèmes d'Information, registriert wurde. Somit ist sichergestellt, dass die Strafverfolgungsbehörden im Bedarfsfall verschlüsselte Daten entschlüsseln und somit lesen können.

Alle Anbieter von Kommunikationsdiensten sind zur Speicherung all jener Daten, die der Aufklärung von Straftaten und der Gewährleistung der nationalen Sicherheit dienen, verpflichtet. Die Daten werden grundsätzlich für die Nutzeridentifizierung, für die technische Charakterisierung des Dienstes und die Lokalisierung des Endgeräts gespeichert. Die Dauer der Speicherung ist abhängig von der Art der Daten und des Unternehmens und beträgt maximal ein Jahr. Internet Service Provider speichern die Daten maximal sechs Monate, Cache Server im Durchschnitt drei bis fünf Tage und Web Hosting Provider maximal drei Monate.

Weiters gibt es im Strafgesetzbuch Regelungen zur ***anlassbezogenen Speicherung*** von Daten. Für die Veranlassung einer solchen Speicherung benötigt die Kriminalpolizei einen richterlichen oder staatsanwaltlichen Beschluss, der den Betreiber verpflichtet, entsprechende Maßnahmen zu treffen, um Inhalte der Kommunikation eines Teilnehmers bis zu einem Jahr zu speichern.

Auf die erfassten Daten aus Data Retention und Data Preservation haben der Zoll, verschiedene Verwaltungsbehörden, die Börsenaufsicht und die Justiz, also Gerichte, aber auch Polizei und Gendarmerie, während laufender Ermittlungen ***Zugriff***.

Auch ist ein ***Kostenersatz*** für operative Kosten im Strafgesetzbuch vorgesehen, der von der Staatskasse getragen wird. Über die Höhe der Entschädigungen gibt es allerdings keine öffentlichen Informationen. Außerdem werden Investitionskosten nicht ersetzt, was ein Problem für kleinere Anbieter darstellt, da ihnen wenige Anfragen gestellt werden und somit der Kostenersatz gering ist.

3.2.3 Spanien

In Spanien sind die Maßnahmen zur ***Vorratsdatenspeicherung*** im Allgemeinen Datenschutzgesetz 2002 und das Fernmeldegeheimnis in der Verfassung und im Strafgesetzbuch geregelt. Die Daten dürfen maximal 12 Monate gespeichert werden. In der Praxis werden sie allerdings auf Grund der hohen Kosten für Speicherung und Verarbeitung zumeist schon nach 12 Stunden überschrieben, weshalb sie für die Strafverfolgung nicht relevant sein können.

Art und Umfang der zu speichernden Daten variieren je nach Anbieter. So müssen Netzbetreiber, Service Provider und Access Provider jene Daten speichern, die es ermöglichen, Endgeräte zu lokalisieren. Housing Provider hingegen müssen nur jene Daten speichern, die zur Bestimmung der Datenherkunft nötig sind sowie das Datum und die Zeit des Nutzungsbeginns. Zudem dürfen keine Daten gespeichert werden, die dem Fernmeldegeheimnis unterliegen. Die Daten, die durch die Vorratsdatenspeicherung entstehen, dürfen nicht für unternehmenseigene Zwecke verwendet werden, auch wenn die Erfassung der Daten nach dem Datenschutzgesetz gestattet wäre.

Wie in Frankreich gibt es auch in Spanien Regelungen zur ***Data Preservation***, die in der Strafprozessordnung festgehalten sind. Zur Anordnung dieser anlassbezogenen Speicherung bedarf es einer richterlichen oder staatsanwaltlichen Anordnung, die nur im Rahmen eines Strafprozesses oder zur Aufrechterhaltung der öffentlichen beziehungsweise nationalen Sicherheit erteilt werden darf. In der Praxis wird Data Preservation kaum eingesetzt, stattdessen werden im Bedarfsfall Echtzeit-Überwachungen durchgeführt.

Auf die erfassten Daten dürfen Gerichte, Staatsanwälte und das Finanzministerium ***zugreifen***. Wenn die allgemeinen Datenschutzregelungen eingehalten werden, so darf die Exekutive auch ohne richterliche Anordnung auf die Daten zugreifen. Für Anfragen an die Betreiber gibt es keine festgelegten Formalitäten, üblicherweise erfolgt die Anfrage per Fax oder Telefon.

In Spanien gibt es keinerlei Regelungen über den ***Kostenersatz*** für Betreiber. Das bedeutet, dass die Telekommunikations-Unternehmen sämtliche Kosten für Abhörmaßnahmen alleine tragen müssen.

3.2.4 Großbritannien

In Großbritannien ist die ***Vorratsdatenspeicherung*** für Strafverfolgungszwecke im 2001 verabschiedeten Anti-Terrorism, Crime and Security Act geregelt. Das Gesetz über Ermittlungsbefugnisse (RIPA[6]) regelt den Gewinn und die Weitergabe von Verbindungs- und Standortdaten. Allerdings gibt es auch hier sehr strenge Datenschutz-Regelungen.

Die Vorratsdatenspeicherung ist nicht verpflichtend. Sie basiert auf freiwilligen Vereinbarungen zwischen Betreibern von öffentlichen Telekommunikations-Dienstleistungen und dem Home Office[7]. Diese Vereinbarungen sollen die Unternehmen dazu motivieren, die Daten von sich aus zu speichern. Wie viele Anbieter tatsächlich Data Retention betreiben, unterliegt der Geheimhaltung. Laut Wik-Consult Studie gehen Experten allerdings davon aus, dass die Bereitschaft zur Speicherung groß sei. Die kooperierenden Unternehmen speichern Verkehrs- und Bestandsdaten für die nationale Sicherheit.

---

[6] ***R***egulation of ***I***nvestigatory ***P***owers ***A***ct 2000

[7] Das Home Office ist das britische Innenministerium

Die Unternehmen, die Vorratsdatenspeicherung betreiben, dürfen Logfiles über die Webaktivität maximal vier Tage und Telefon-Verbindungsdaten und Bestandsdaten maximal ein Jahr speichern. SMS, EMS, MMS und sonstige Internet-Daten müssen nach sechs Monaten gelöscht werden.

Es gibt keine detaillierten Anforderungen an Hard- und Software sowie die Administration, die Auswertung und Aufbereitung der gespeicherten Daten. Bei Anfragen werden die ohnehin vorhandenen Daten, so wie sie sind, weitergegeben. Die ***Anfrage*** an die Betreiber muss verhältnismäßig und notwendig sein, außerdem muss sie detailliert formuliert sein. Die Anbieter dürfen nur die angeforderten Daten extrahieren und weitergeben.

Die ***anlassbezogene Speicherung*** erfolgt ebenfalls auf freiwilliger Basis, sie kann aber von den Strafverfolgungsbehörden verlangt werden und nötigenfalls können auch Durchsuchungen von Servern durchgeführt werden. In der Praxis wird Data Preservation allerdings kaum angewandt. Nach Wik-Consult ist es *„nach RIPA [grundsätzlich] für einen dazu berechtigten Mitarbeiter einer LEA[8] gestattet, Daten auf jede Art und Weise zu gewinnen beziehungsweise Zugang zu diesen zu erlangen. Voraussetzung ist, dass die Schritte dazu verhältnismäßig und notwendig sind."*

[8] Law Enforcement Agency

Zugriff auf die Data Retention und die Data Preservation Daten haben verschiedene Police Forces und Intelligence Services[9], welche die Daten zur Gewährleistung der nationalen Sicherheit, zum Schutz und zum Aufdecken von Straftaten im Zusammenhang mit der Gefährdung der nationalen Sicherheit abfragen dürfen. Streng genommen dürfen die Daten daher nicht für die Strafverfolgung verwendet werden. Die Unternehmen müssen für die Abfragen einen speziell geschulten Mitarbeiter benennen, einen so genannte Single Point of Contact (SPoC). Es werden zirka 500.000 Abfragen pro Jahr durchgeführt. Hauptsächlich wird eine Auflistung aller Anrufe oder eine Identifizierung von Teilnehmern auf Basis von Telefonnummern, E-Mail-Adressen, Websites oder IPs angefordert.

Auch in Großbritannien ist grundsätzlich eine ***Entschädigung*** für die entstandenen ***Kosten*** vorgesehen, allerdings sind keine Details geregelt. Die Höhe der Entschädigung liegt im Ermessen der Regierung und die Tariflisten unterliegen der Geheimhaltung.

Laut Herrn Ing. Martin Prager[10] zeichnet Großbritannien seit den 1980er-Jahren auch jegliche Kommunikation auf, die über das United Kingdom erfolgt oder dort verfügbar ist.

---

[9] Intelligence Services sind Geheimdienste und Spionagedienste

[10] Ing. Martin Prager ist Leiter der Expertsgroup IT-Security des Fachverbandes Unternehmensberatung und Informationstechnologie (UBIT) der Wirtschaftskammer Österreich

3.2.5 Niederlande

In den Niederlanden gibt es ***keine Verpflichtung zur Vorratsdaten-speicherung***. Es gibt allerdings einen Sonderfall für die Speicherung von Verbindungs- und Standortdaten zur Identifizierung von Teilnehmern, bei denen keine Stammdaten vorliegen. Diese Regelung betrifft besonders Kunden von Prepaid-Karten im Mobilfunk. In diesen Fällen werden in der Praxis Bestands- und Verkehrsdaten für drei Monate gespeichert.

Alle Netzbetreiber und Anbieter von öffentlichen Telekommunikations-Dienstleistungen sind zur Kooperation mit Strafverfolgungsbehörden ausnahmslos verpflichtet. Nach der Wik-Consult Studie sind die erfassten Daten so zu speichern, dass sie jederzeit von der dazu berechtigten *„Zentralstelle der Behörden, der so genannten CIOT „Central Information System for Telecommunication Investigation" abgerufen werden können [...]."* Die Zentralstelle kann dadurch täglich auf aktualisierte Bestandsdaten zurückgreifen. Es gibt keinerlei technische Standards, auf denen dieses automatisierte System basieren muss.

Einerseits müssen die Betreiber Bestandsdaten, also Name, Adresse, Rufnummer und die Art des genutzten Dienstes, speichern und automatisch weitergeben. Das bedeutet, dass die Anbieter zum Monitoring und zur Speicherung von Bestandsdaten verpflichtet sind. Andererseits sind Mobilfunk-Unternehmen zur Speicherung von Verkehrsdaten, die sich auf Prepaid-Karten, also Wertkarten-Handys, beziehen, für die Dauer von drei Monate verpflichtet. Diese müssen auch auf Anfrage weitergeben werden. Auch jene Daten, die für unternehmenseigene Zwecke gespeichert werden, müssen bei einer Anfrage beauskunftet werden, wenn sie für die Strafverfolgung relevant sind.

Die ***Speicherfrist*** für Verkehrsdaten im Bereich Festnetz-Telefonie beträgt sechs Monate, die für E-Mails zirka eine Woche und jene im Mobilfunk ungefähr fünf Monate. Bestandsdaten müssen spätestens ein Jahr nach Vertragsende gelöscht werden. Daten, die bei der Nutzung von Chat, IRC oder News Groups entstehen, werden nicht gespeichert.

Eine ***Besonderheit*** der niederländischen Gesetzgebung ist, dass es durch das Gesetz *„über besondere Befugnisse bei Ermittlungsverfahren"* aus dem Jahr 2001 gestattet ist, die Telekommunikation in einem geschlossenem Netzwerk zu überwachen. Dies gilt auch für Unternehmensnetzwerke. Zu diesem Zweck darf ein Computer „verwanzt" werden. Beispielsweise dürfen technische Einrichtungen verwendet werden, um E-Mails abzufangen. Auch Scanner dürfen in Netze implementiert werden, um Mobilkommunikation mithören zu können.

4 Data Retention[11]

Als Vorratsdatenspeicherung wird die bald verpflichtende pauschale Speicherung aller Daten, die bei Internet- und Telekommunikations-Providern bei der Nutzung der Dienste anfallen, bezeichnet. Immer wenn ein Kunde einen Telefonanruf über Festnetz, Mobilnetz oder Voice-over-IP ins Festnetz tätigt, eine SMS, MMS oder E-Mail versendet, eine Website aufruft oder Daten von einem FTP-Server abruft, werden diese Informationen für einen begrenzten Zeitraum für Strafverfolgungsbehörden gespeichert und auf Anfrage herausgegeben. Es werden allerdings keine Inhaltsdaten aufgezeichnet.

Da heutzutage ein großer Teil der Kommunikation bereits über elektronische Medien verläuft, bedeutet diese Richtlinie für die Bürger einen massiven Eingriff in ihre Privatsphäre. Schon allein die Speicherung von Verkehrsdaten ermöglicht im Mobilfunk das Erstellen von Bewegungsprofilen oder das Ermitteln von Kommunikationsnetzwerken, also wer mit wem kommuniziert hat. Datenschützer und Vertreter der Telekommunikations-Branche sprechen von einer Verdächtigung aller Teilnehmer, kriminelle Handlungen zu planen oder durchführen zu wollen.

[11] Viele dieser Informationen wurden im Zuge eines Leitfadeninterviews mit Ing. Martin Prager erarbeitet und vertieft. Er ist Leiter der Expertsgroup IT-Security des Fachverbandes Unternehmensberatung und Informationstechnologie (UBIT) der Wirtschaftskammer Österreich

Alternativ zur Vorratsdatenspeicherung besteht die von Experten angeratene Möglichkeit von Data Preservation, da hier nicht so große Mengen an Daten anfallen. Bei der anlassbezogenen Speicherung kann beim Verdacht auf schwere oder terroristische Straftaten eine Speicherung der Verkehrsdaten für eine einzelne Person veranlasst werden. Dadurch würden in erster Linie Kosten für Investitionen und Speicherung sowie Auswertung der Daten eingespart werden können. Auch der Eingriff in die Privatsphäre der Bürger wäre nicht so tief greifend wie bei einer pauschalen Vorratsdatenspeicherung.

4.1 EU-Richtlinie bezüglich Vorratsdaten-speicherung

Mitte Dezember 2005 hat das Europäische Parlament und der Europäische Rat eine Richtlinie bezüglich Vorratsdatenspeicherung beschlossen, welche die Mitgliedstaaten verpflichtet, Ruf- und Verkehrsdaten für mindestens 6 Monate und maximal zwei Jahre zu speichern. Die Dauer der Speicherung innerhalb dieses Rahmens ist jedem Mitgliedsland freigestellt. Für die Anbieter von Mobil- und Festnetz-Telefonie und Internetservice Provider bedeutet die Vorrats-datenspeicherung einen enormen Kosten- und Administrations-Aufwand.

Der Kostenersatz ist nicht in der EU-Richtlinie geregelt, sondern kann auf nationaler Ebene beschlossen werden. Daher sind die Mitgliedslän-der auch nicht verpflichtet, Regelungen für die Erstattung der Kosten einzuführen. Falls die Kosten gar nicht oder nur begrenzt ersetzt würden, könnte dies einen Wettbewerbsnachteil für kleinere Provider darstellen. Größere Anbieter könnten die Kosten auf ihre Kunden abwälzen. Dennoch sind die Bürger der Europäischen Union diejenigen, die für anfallende Kosten aufkommen müssen, sei es über erhöhte Kosten für die Nutzung der verschiedenen Dienste oder über Steuern.

Data Retention ist ein sehr brisantes Thema, das von Datenschutzexperten und Anbietern von Telefonie und Internet abgelehnt, aber von Strafverfolgungsbehörden befürwortet wird, da es ihrer Ansicht nach eine wesentliche Erleichterung für ihre Ermittlungen bedeutet. Durch die Vorratsdatenspeicherung wird man von allen 450 Millionen Bürgern der EU wissen, wer wann mit wem wohin und auch relativ viel worüber er kommuniziert hat.

4.1.1 Entstehungsgeschichte der Richtlinie

Erstmals wurde im August 2002 auf europäischer Ebene über Data Retention diskutiert. Dänemark hatte zu diesem Zeitpunkt die Ratspräsidentschaft inne und legte einen Entwurf für eine Richtlinie vor. Die Dauer der Speicherung sollte mit zwölf Monaten begrenzt sein. Der Entwurf wurde allerdings mehrheitlich abgelehnt.

Am 25. März 2004 hat der Europäische Rat die *„Erklärung des Rats zum Kampf gegen den Terrorismus"* (Ratsdokument 7764/04) verabschiedet, die auch die Erarbeitung von Rechtsnormen für die langfristige Speicherung von Kommunikationsdaten von Anbietern und Betreibern verlangt. Der Europäische Rat beauftragte den Ministerrat bis Juni 2005 zu überprüfen, welche Rechtsvorschriften zur Data Retention erlassen werden sollen.

Daraufhin haben Vertreter aus Frankreich, Irland, Schweden und Großbritannien am 30. April 2004 einen Entwurf für einen Rahmenbeschluss zur Vorratsspeicherung von Telekommunikationsdaten dem Ministerrat vorgelegt (Ratsdokument 8958/04). Der Rat hielt eine einheitliche Politik bezüglich der Vorratsdatenspeicherung auf Grund der steigenden Anzahl von Terroranschlägen und zunehmender grenzüberschreitender Kriminalität für angemessen. In dem Entwurf war eine Vorratsspeicherung von zwölf bis 36 Monaten vorgesehen.

Im Unterschied zu dem 2002 abgelehnten Entwurf sollte die Data Retention auch zur Verhinderung von Straftaten eingesetzt werden. Die Beschränkung auf schwere Straftaten und Terrorismus wurde aufgehoben.

Durch die Übernahme der Ratspräsidentschaft durch Großbritannien und die Anschläge in London bekamen die Befürworter der Richtlinie neue Energie. Die EU-Kommission legte am 21. September 2005 einen eigenen Entwurf für eine Richtlinie vor. Internetdaten sollten zumindest sechs Monate und Telefoniedaten mindestens zwölf Monate lang gespeichert werden. Die Kommission erhoffte sich dadurch Möglichkeiten zur Prävention, Aufklärung und Verfolgung von schweren Straftaten. Das Parlament begrüßte den Vorschlag der Kommission, kürzte allerdings die Liste der zu speichernden Datenarten.

Der Ministerrat ergriff die Initiative und verhandelte ohne das Wissen des Berichterstatters mit EU-Parlamentariern. Zu diesem Zeitpunkt versuchten verschiedene Interessensvertreter über den LIBE-Ausschuss[12] zu erklären, an welchen Punkten Probleme auftreten können.

Dem Europäischen Parlament wurde erneut ein Kompromissentwurf vorgelegt, der am 14. Dezember 2005 mit 378 zu 197 Stimmen beschlossen wurde. Der Ministerrat stimmte am 21. Feber 2006 ebenfalls mehrheitlich für den Entwurf. Die Slowakei und Irland stimmten aus formalen Gründen gegen die Richtlinie, da sie der Auffassung waren, dass Regelungen zur Data Retention auf Basis eines Rahmenbeschlusses beschlossen werden sollten.

[12] Der Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und Innere Angelegenheiten (LIBE).

4.1.2 Anlass und Ziele der Richtlinie

Ziel der beschlossenen Richtlinie (PE-CONS 3677/05) ist es, die Pflichten für Betreiber und Anbieter zur Vorratsdatenspeicherung zu harmonisieren, sodass die Strafverfolgungsbehörden der EU auf das gleiche Datenreservoir zurückgreifen können. Laut Vorschlag zur Richtlinie (A6-0365/2005) bestehen bereits in einigen Mitgliedsländern Regelungen zur Data Retention. Durch die unterschiedlichen Regelungen in den Ländern können die Daten nicht effizient verwendet werden. Die Harmonisierung soll gewährleisten, dass die gespeicherten Daten auf internationaler Ebene zur *„Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten"* verwendet werden können. Stammdaten und Verkehrsdaten zusammen können wichtige Informationen für die Strafverfolgung bringen.

Die ISPA (Positionspapier 2005:2) widerspricht dem, da in keinem europäischen Land eine verpflichtende und umfassende Vorratsdatenspeicherung praktiziert wird. Selbst Großbritannien, eine treibende Kraft der Vorratsspeicherung, hat die Data Retention nur auf freiwilliger Basis eingeführt und auch in den USA bestehen derzeit nur Regelungen zur Data Preservation. Daher besteht laut ISPA kein Harmonisierungsbedarf. Zudem ist in Österreich wie in einigen anderen EU-Mitgliedsländern die Speicherung von Verkehrsdaten verboten (TKG 2003:§99).

Für die pauschale Speicherung der Verkehrsdaten sprechen einige Gründe, wie die Bekämpfung von Kinderpornografie, die Beschränkung der Verbreitung von rassistischen Inhalten oder die Bekämpfung und Vorbeugung der organisierten Kriminalität. Seit den Anschlägen in den USA am 11. September 2001, dem Anschlag in Madrid am 11. März 2004 und den Anschlägen in London am 7. Juli 2005 zählt der *„Kampf gegen Terrorismus"* zu den Hauptargumenten der Befürworter.

Dennoch bedeutet die Speicherung der Kommunikationsdaten auf Vorrat die Möglichkeit einer langfristigen Kontrolle und Überwachung der Telekommunikationsteilnehmer durch den Staat, da die Daten nicht schnellstmöglich anonymisiert oder gelöscht werden, sondern langfristig erhalten bleiben. Dies bedeutet auch ein großes Missbrauchspotential für die gespeicherten Daten.

4.1.3 Treibende Kräfte und Gegner

Immer mehr Anbieter bieten Flatrates, also Pauschaltarife, für die Nutzung ihrer Dienste an, daher besteht für sie kaum noch die Veranlassung, Verkehrsdaten für die Rechnungslegung zu speichern. Die Strafverfolgungsbehörden könnten dann auch nicht mehr auf diese Daten für die Aufklärung von Verbrechen zurückgreifen.

Durch die Vorratsdatenspeicherung stehen EU-weit sämtliche Verbindungsdaten der Teilnehmer zur Verfügung, wodurch im Nachhinein festgestellt werden kann, wer kommuniziert hat. Strafverfolgungsbehörden erhoffen sich dadurch Informationen über Verbrechen.
Auf ***EU-Ebene*** hat sich besonders Großbritannien für den Beschluss der Richtlinie eingesetzt, wo es ja bereits Regelungen zur Data Retention auf freiwilliger Basis gibt (siehe Kapitel 3.3). Auch Frankreich, Irland, Schweden und Deutschland haben sich sehr für den Beschluss der Richtlinie eingesetzt. Dies geschah auch unabhängig von der amtierenden Partei. Jörg Zierke, Präsident des Deutschen Bundeskriminalamtes, gab in einem Interview mit der BITKOM im Dezember 2004 an: *„Das Argument, dass auch die Daten Unschuldiger gespeichert werden, interessiert mich nicht."*

Nur Irland und die Slowakei stimmten im Ministerrat gegen den Beschluss der Richtlinie, da sie die Rechtsgrundlage als falsch erachteten. *„Sie waren gegen eine Beteiligung des Europa-Parlaments an der Entscheidung",* so die IT-News Website "futurezone".

Österreich zählte nicht zu den treibenden Kräften, obwohl das Bundesministerium für Inneres sich klar für die EU-Richtlinie aussprach, da ihm die Strafverfolgungsbehörden unterstellt sind. Diese erhoffen sich eine Erleichterung bei der Verfolgung von Straftaten. Das Bundesministerium für Justiz zeigte auf Beamtenebene ein klares Verständnis für das Einhalten der Europäischen Menschenrechtskonvention, so Ing. Martin Prager. Das Bundeskanzleramt sprach sich ebenfalls gegen die beschlossene Richtlinie aus, da dem Bundeskanzleramt die Datenschutzkommission untersteht, die sich für den Schutz der Konsumenten einsetzt. Die Datenschutzkommission ist der Ansicht, dass jeder der 450 Millionen EU-Bürger durch die Vorratsdatenspeicherung verdächtigt wird, kriminelle Handlungen zu setzen oder zu planen. Außerdem seien die freie Meinungsäußerung und der freie Informationsaustausch gefährdet.

Von Österreichs politischen Parteien sprachen sich vor allem das Bündnis Zukunft Österreich (BZÖ) und die Freiheitliche Partei Österreichs (FPÖ) für die Data Retention aus, aus dem Lager der Grünen und der Sozialdemokratische Partei Österreich (SPÖ) kamen die häufigsten Gegenstimmen.

Die deutschen Grünen haben bereits eine Klage vor dem Europäischen Gerichtshof gegen die beschlossene Richtlinie angekündigt.

Auch Vertreter der Musik- und Filmindustrie haben sich für die verpflichtende Vorratsdatenspeicherung ausgesprochen, da sie sich davon offenbar versprechen, diese Daten auch für die Verfolgung von Schwarzkopierern und Tauschbörsenbetreibern nutzen zu dürfen.

Insbesondere technische Experten, Menschenrechtsvertreter, Datenschutzexperten und Branchenvertreter sprechen sich gegen die Data Retention aus, da sie einen enormen technischen und finanziellen Aufwand sowie einen tiefen Eingriff in die Privatsphäre befürchten. Derzeit werden pro User und Monat durchschnittlich 50 Megabyte an Daten übertragen. Bei circa 4 Millionen Nutzern sind dies ungefähr 20 Terabyte pro Monat, die gefiltert und aufgezeichnet werden müssen.

4.1.4 Details der Richtlinie

In den EU-Mitgliedsländern sind alle Anbieter von öffentlichen Diensten und Betreiber von öffentlichen Netzen dazu verpflichtet, Verkehrs- und Standortdaten und jene Daten, die damit in Zusammenhang stehen, für die *„Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten"* dauerhaft zu speichern. Daten, die über den Inhalt einer Kommunikation Aufschluss geben könnten, dürfen nicht gespeichert werden. Ob und wie die Data Retention zur Verhütung von Straftaten eingesetzt werden kann, ist umstritten.

Da es keine Ausnahme bei der Data Retention gibt, werden nicht nur die Daten von natürlichen Personen, sondern auch die von juristischen Personen gespeichert. Auch könnte dies einen Eingriff in die ärztliche Schweigepflicht bedeuten, da die Kommunikationswege der Ärzte aufgezeichnet werden. Bereits die Tatsache, dass überhaupt ein Behandlungsverhältnis zwischen Arzt und Patient besteht, unterliegt der Schweigepflicht. Auch Mandanten von Rechtsanwälten und Steuerberatern sind schützenswert, sodass der Inhalt von Beratungen ebenfalls einer Geheimhaltungspflicht unterliegt.

Des Weiteren müssen auch erfolglose Anrufversuche aufgezeichnet werden, wenn die Daten bei der Bereitstellung der Dienste verarbeitet oder erzeugt und gespeichert beziehungsweise protokolliert werden. Anrufe, bei denen keine Verbindung zustande kommt, müssen nicht gespeichert werden. Dieser Punkt ist einer der am meisten kritisierten Teile der Richtlinie. Frau Mag. Judith Leschanz hat in unserem Gespräch angegeben, dass im Mobilfunk die Anzahl der erfolglosen Anrufversuche weit höher ist als jene, bei denen tatsächlich ein Gespräch zu Stande kommt. Die Menge dieser Daten könnte die Effizienz der Strafverfolgung wesentlich beeinträchtigen.

Die EU-Mitgliedsstaaten müssen entsprechende Richtlinien erlassen, die den Zugang zu den Daten begrenzen. Der Zugriff auf die gespeicherten Daten darf nur in bestimmten Fällen geschehen und zwar nur dann, wenn sie mit dem nationalen Recht in Einklang stehen. Außerdem muss bei der nationalen Umsetzung auf die Bestimmungen des Gemeinschaftsrechts oder des Völkerrechts, insbesondere auf dieEuropäische Menschenrechtskonvention Rücksicht genommenen werden. Der Zugang zu den gespeicherten Daten muss den Anforderungen der Verhältnismäßigkeit und Notwendigkeit entsprechen. In welcher Form der Zugriff genau beschränkt werden muss und welche Behörden auf die Daten Zugriff haben dürfen, ist nicht in der Richtlinie definiert.

Keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, dürfen aufgezeichnet werden. Eine Trennung von Inhalts- und Verbindungsdaten ist allerdings bei SMS, MMS und E-Mail schwer realisierbar, da diese Dienste die Datenformen schon auf Protokollebene vermischen. Nach der Online-Zeitschrift „heise.de" sind Providerverbände der Ansicht, dass somit P2P- und FTP-Transfers und Chat-Sitzungen selbst nicht erfasst werden müssen. Auch im Web ist es schwierig, Verbindungs- und Inhaltsdaten zu trennen, da oft in der URL nicht nur die Domain, sondern auch die Unterseite oder dynamische Inhalte enthalten sind.

Bei den zu speichernden Datenkategorien wird grundsätzlich zwischen Anbietern von Festnetz- und Mobiltelefonie und Anbietern von Internetdiensten unterschieden. Im Internet-Bereich beschränkt sich die Speicherung auf Verbindungsdaten auf Internetzugang, E-Mail und Internet-Telefonie. Im Groben umfassen die zu speichernden Daten Angaben wie Rufnummer, Benutzerkennung oder IP-Adresse, den Namen und die Anschrift der Teilnehmer, Datum und Uhrzeit sowie die Dauer der Kommunikation. Außerdem müssen die Art der (mutmaßlichen) Endeinrichtung und die Art des in Anspruch genommenen Dienstes aufgezeichnet werden.

Folgende Tabelle zeigt detailliert die zu speichernden Datenarten, getrennt nach Telefonie und Internet, auf. „Teilnehmer" steht dabei für „Teilnehmer oder registrierter Benutzer".

Tabelle 2: Zu speichernde Datenarten (EU-Richtlinie 2005:Art. 5)

Zur Rückverfolgung & Identifizierung der Quelle von Nachrichten benötigte Daten	
Telefonfestnetz & Mobilfunk	**Internetzugang, Internet-E-Mail & -Telefonie**
• Rufnummer des anrufenden Anschlusses • Name & Anschrift des Teilnehmers	• zugewiesene Nutzerkennung(en) • Nutzerkennung und Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden • Name & Anschrift des Teilnehmers, dem IP, Nutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war
Zur Identifizierung des Adressaten der Nachricht benötigte Daten	
Telefonfestnetz & Mobilfunk	**Internet-E-Mail & -Telefonie**
• angewählte Rufnummer(n) & bei Zusatzdiensten (z.B. Rufweiterleitung / Rufumleitung) die Nummer(n), an die der Anruf geleitet wird • Namen & Anschriften der Teilnehmer	• Nutzerkennung / Rufnummer des vorgesehenen Empfängers eines Anrufes (Internet-Telefonie) • Namen & Anschriften der Teilnehmer und Nutzerkennung des vorgesehenen Empfängers einer Nachricht
Zur Bestimmung von Datum, Uhrzeit & Dauer einer Nachrichtenübermittlung benötigte Daten	
Telefonfestnetz & Mobilfunk	**Internetzugang, Internet-E-Mail & -Telefonie**
• Datum & Uhrzeit des Beginns & Endes der Kommunikation	• Datum & Uhrzeit der An- & Abmeldung beim Internetzugangsdienst (Grundlage: bestimmte Zeitzone), mit der vom Access Provider zugewiesenen dynamischen / statischen IP-Adresse & Nutzerkennung des Teilnehmers • Datum & Uhrzeit der An- und Abmeldung für Internet-Email-Dienst / Internet-Telefonie-Dienst (Grundlage: bestimmte Zeitzone)
Zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten	
Internet-E-Mail & -Telefonie	
• in Anspruch genommener Dienst	

Zur Bestimmung der (vorgeblichen) Endeinrichtung oder von Nutzern benötigte Daten		
Telefonfestnetz	**Mobilfunk**	**Internetzugang, Internet-E-Mail & -Telefonie**
• Rufnummern des anrufenden & des angerufenen Anschlusses	• Von anrufenden & angerufenem Anschluss: IMSI&IMEI • bei vorbezahlten anonymen Diensten: Datum & Uhrzeit erster Aktivierung & Cell-ID, wo Dienst aktiviert wurde	• Rufnummer (anrufender Anschluss) für Zugang über Wählanschlüsse • digitale Teilnehmeranschluss oder anderer Endpunkt des Urhebers der Kommunikation
Zur Bestimmung des Standorts mobiler Geräte benötigte Daten		
• Standortkennung (Cell-ID) bei Beginn der Verbindung • Daten zur geographischen Ortung von Funkzellen durch Bezugnahme auf Standortkennung (Cell-ID) während des Zeitraums, in dem Vorratsspeicherung der Kommunikationsdaten erfolgt		

Die Vorratsdaten müssen so gespeichert werden, dass die Daten unverzüglich an die zuständigen Behörden weitergegeben werden können. Die oben genannten Datenarten müssen mindestens sechs Monate und maximal zwei Jahre gespeichert werden. Die EU-Länder müssen innerhalb von achtzehn Monaten Rechts- und Verwaltungsvorschriften erlassen und den Text dieser Bestimmungen an die Kommission übermitteln.

Wenn ein Mitgliedsstaat eine Verlängerung der maximalen Speicherfrist rechtfertigen kann, so können die notwendigen Maßnahmen gesetzt werden. Die Kommission und die anderen EU-Länder müssen darüber informiert werden. Innerhalb von sechs Monaten kann die Kommission die Verlängerung ablehnen. Außerdem kann die Umsetzung der Richtlinie um weitere achtzehn Monate zurückgestellt werden. Auch hiervon ist die Kommission zu unterrichten.

In Bezug auf Datenschutz und Datensicherheit müssen die Mitgliedsländer zumindest folgende Richtlinien einhalten:

Zunächst muss die Qualität der gespeicherten Daten gleich sein. Diese unterliegen auch *„der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten."* Außerdem müssen die Vorratsdaten vor Zerstörung, Verlust, Abänderung sowie vor zufälliger oder unrechtmäßiger Speicherung, Verarbeitung oder Weitergabe geschützt werden.

Zudem dürfen nur besonders ermächtigte Personen Zugang zu den gesicherten Daten haben. Bisher hatten nur eine begrenzte Zahl an Mitarbeitern Zugang zu den Logfiles. Diese waren über den Dienstvertrag hinaus zur Verschwiegenheit verpflichtet.

Es muss sichergestellt werden, dass die Vorratsdaten nach Ablauf der Speicherfrist vernichtet werden. Davon ausgenommen sind jene Daten, die abgerufen und gesichert wurden. Frau Mag. Leschanz geht davon aus, dass jene Daten nicht zu löschen sind, die im Zuge eines Verfahrens gesichert werden müssen. Beispielsweise gibt es einen Gerichtsbeschluss, der besagt, dass Daten gespeichert werden müssen, diese werden aber erst zu einem späteren Zeitpunkt gebraucht, ähnlich dem Data Freeze.

Jeder Mitgliedsstaat muss eine oder mehrere unabhängige Stellen benennen, die für die Kontrolle zuständig sind. Auch müssen Sanktionen inklusive verwaltungsrechtlicher und strafrechtlicher Sanktionierungen für den Verstoß gegen die Richtlinien festgelegt werden. Diese müssen *„wirksam, angemessen und abschreckend"* sein.

Außerdem soll jährlich eine Statistik erstellt werden, die aufzeigt, in welchen Fällen Daten weitergegeben wurden, welcher Zeitraum zwischen der Speicherung und der Anfrage liegt und wie viele der Anfragen ergebnislos geblieben sind. In der Statistik dürfen keinerlei personenbezogene Daten ausgewiesen werden.

Spätestens drei Jahre nach Umsetzung der Richtlinie wird die Kommission dem Europäischen Parlament eine Bewertung der Auswirkungen auf Wirtschaft und Verbraucher vorlegen. Besondere Aufmerksamkeit wird dabei auf die festgelegten Datenarten und die Dauer der verpflichtenden Speicherung unter Berücksichtigung des technischen Fortschrittes gelegt werden.

4.1.5 Ungeklärte Punkte der Richtlinie

Viele Gegner kritisieren an der beschlossenen Richtlinie, dass sie sehr vage formuliert ist und viele Punkte nicht oder nicht ausreichend geregelt wurden. Die Regelung zur Data Retention soll die nationalen Gesetze der Mitgliedsländer harmonisieren. Durch die unzureichenden oder fehlenden Definitionen beziehungsweise durch den Handlungsspielraum bei der Umsetzung kommt es allerdings wieder zu unterschiedlichen Gesetzgebungen.

In erster Linie mangelt es an Regelungen über einen ***Kostenersatz*** für die anfallenden Kosten bei den Anbietern von Telekommunikationsdiensten. Dies wird vor allem von Branchenvertretern und den Anbietern selbst kritisiert. Sie fordern deshalb einen angemessenen Ersatz für die entstandenen Kosten, auch für Investitionskosten und die laufenden Kosten, da es nicht verständlich sei, wieso die Wirtschaft für die Erfüllung von Staatsaufgaben aufkommen solle. Klein- und Mittelunternehmen könnten durch einen mangelnden Investitions-Kostenersatz in Zahlungsschwierigkeiten kommen. Herr Georg Chytil vermutet, dass die Betriebskosten für Internet Service Provider um 10-20% steigen werden. Laut Herrn Ing. Martin Prager schätzt die WKO den Investitionsaufwand für Mittel- und Großbetriebe, wie beispielsweise große Telekom- und Mobilfunkunternehmen, auf mehrere Millionen Euro. Innerhalb der Wirtschaftskammer gäbe es

Diskussionen, ob es sich dabei um zwei- oder dreistellige Millionenbeträge handelt. Die Schätzungen liegen zwischen 80 und 200 Millionen Euro.

Die variablen Kosten sind laut Ing. Martin Prager nicht abschätzbar. Hierzu zählen sämtliche Aufwendungen, um die Technik am Laufenden zu halten und sie zu betreiben, um Datenschutzmaßnahmen zu setzen, um die Datenflut zu sortieren oder um für die Auswertung der Daten zu sorgen. KMUs müssten extra Personal einstellen, da die Entscheidungsträger und die Überwachenden nicht die gleichen Personen sein dürfen. Herr Georg Chytil nimmt an, dass große Provider für die Verarbeitung der Anfragen durch die Exekutive *„eine halbe Person"* benötigen, im Bereich des Mobilfunks wesentlich mehr. Laut Parlamentsberichterstatter Alexander Alvaro könnte die verpflichtende Data Retention und die damit einhergehenden Mehrkosten auch einen Verstoß gegen die Gewerbefreiheit darstellen.

Die ***Dauer*** der Vorratsspeicherpflicht ist mit sechs bis 24 Monaten geregelt, wodurch es in den unterschiedlichen EU-Mitgliedsländern zu verschiedenen Fristen kommen wird. Dies könnte für international tätige Anbieter ein Problem darstellen. Sie werden zudem für die entstandenen Kosten unterschiedlich entschädigt. Das österreichische Bundesministerium für Inneres möchte die maximale Speicherfrist von zwei Jahren ausreizen, das Justizministerium beharrt auf sechs Monaten. Die Wirtschaft hofft, dass die Daten maximal für sechs Monate zu speichern sind. Herr Ing. Martin Prager schätzt die tatsächliche Speicherdauer auf 12-24 Monate, Frau Mag. Judith Leschanz auf ein Jahr und Herr Chytil hofft, dass die Daten nur für maximal sechs Monate gespeichert werden müssen.

Wie bereits in Kapitel 3.1.2 (Überwachungsmöglichkeiten in Österreich) erwähnt, werden hauptsächlich Daten von Strafverfolgungsbehörden abgefragt, die nicht älter als drei Monate sind. Branchenvertreter kritisieren deshalb, dass durch die Vorratsdatenspeicherung große Datenfriedhöfe entstehen.

Die Vorratsdatenspeicherung ist besonders für Internet Service Provider und Anbieter von Festnetz-Telefonie Neuland, Anbieter von Mobiltelefonie speichern bereits einige Verkehrsdaten für die Rechnungslegung (siehe Kapitel 3.1.2.1. Regelungen des TKG).

Ebenso wenig festgelegt wurde, was unter „schweren Verbrechen" zu verstehen ist. Nur im Falle von schweren Straftaten dürfen Ermittler auf die gespeicherten Daten ***zugreifen***. Die Begriffsbestimmung von *„schweren Verbrechen"* wird in der EU-Richtlinie nur mit der Definition *„wie beispielsweise Terrorakte und kriminelle Handlungen im Rahmen des organisierten Verbrechens"* eingegrenzt. Eine genaue Definition muss von jedem Mitgliedstaat in dessen nationaler Legislatur geregelt und werden kann deswegen stark variieren. Empfohlen wird allerdings der EU-Strafenkatalog für internationale Haftbefehle. In Österreich soll der Zugriff auf die Daten weiterhin nur ermöglicht werden, wenn ein richterlicher Beschluss vorliegt. Anfragen von anderen EU-Ländern sollen nur über Amtshilfeverfahren bearbeitet werden (siehe Kapitel 3.1.3.1. Telefonie). Wenn es zur Regelungen bezüglich eines Kostenersatzes kommt, können die Anbieter die Kosten für die Abfrage und Auswertung an das jeweilige Gericht weiterverrechnen. Ob und wie ein österreichisches Gericht die Kosten von dem anfragenden EU-Land ersetzt bekommt, ist nicht geklärt.

Auch wurde nicht geregelt, wer die Daten ***auswerten*** und ***abfragen*** darf und wo die Daten gespeichert werden sollen. Österreich plant, dass die Daten weiterhin bei den Anbietern gespeichert werden und im Bedarfsfall von den zuständigen Gerichten angefordert werden. Das Bundesministerium für Inneres setzt sich allerdings für eine zentrale Speicherung der Daten ein.

Besonders von Datenschützern wird kritisiert, dass in der Richtlinie keine genauen Angaben über ***Datenschutz und Datensicherheit*** enthalten sind. Die Anbieter müssen lediglich sicherstellen, dass *„geeignete technische und organisatorische Maßnahmen getroffen [werden], um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung"* zu schützen. Auch für den Zugang zu den Daten sind *„geeignete technische und organisatorische Maßnahmen"* zu treffen, sodass nur besonders ermächtigte Personen auf die gespeicherten Daten zugreifen können. Was genau „geeignete technische und organisatorische Maßnahmen" sind, ist nicht definiert und muss wiederum in der nationalen Gesetzgebung der Mitgliedsländer festgehalten werden.

Auch wird die Richtlinie innerhalb der EU zu unterschiedlichen ***Zeitpunkten*** umgesetzt. Ungefähr die Hälfte der Mitgliedstaaten, darunter auch Österreich, machen von der Möglichkeit Gebrauch, die Umsetzungsfrist auf 36 Monate zu erstrecken. Frankreich hat die Richtlinie sofort per Dekret umgesetzt.

4.1.6 Risiken und Probleme bei der Umsetzung

Durch die ungenauen oder fehlenden Definitionen der Richtlinie kann es bei der Umsetzung zu Problemen kommen. Auch wurden einige Regelungen beschlossen, die aus ***technischen Gründen*** so nicht umsetzbar sind.

Einerseits sind in der Mobilkommunikation die IMSI und die IMEI der angerufenen Anschlüsse aufzuzeichnen. Diese Informationen sind für den Anbieter während des Anrufs nicht ersichtlich, da diese indirekt abgehandelt werden. Die IMEI und die IMSI werden nur während der Einwahl ins Netz an den Betreiber übermittelt und ausgewertet. Genauso wenig kann der Anbieter des Nutzers, der jemanden anruft oder eine E-Mail schreibt, den Namen, die Anschrift sowie die Nutzerkennung inklusive der IMEI und IMSI des Adressaten speichern, da diese Informationen nur beim Anbieter des Empfängers vorliegen.

Außerdem wird eine enorme Menge an Daten anfallen, die von den Anbietern zu speichern sind. Laut Schätzungen von Herrn Ing. Martin Prager wird die ***Datenmenge*** um ein zehn bis 100-faches ansteigen.

Die Provider werden vor allem mit Filterproblemen konfrontiert werden. In der Richtlinie ist nicht geregelt, wie die Auswertung und Filterung der Daten erfolgen soll. Wird bei kurzer Inaktivität des Routers die Verbindung rasch ab- und dann wieder aufgebaut, wird jeweils der Zeitpunkt von An- und Abmeldung mehrfach aufgezeichnet. Laut Online-Zeitschrift „futurezone" sind Breitband-Kunden entweder dauernd online oder wählen sich im Achtstunden-Rhythmus automatisch ein. Auch bei E-Mail-Programmen kann man einstellen, wie oft die E-Mails vom Server abgerufen werden sollen. Auch dann muss jede Anfrage an den Mail-Server aufgezeichnet werden. Auch die große Menge an Spam-Mails stellt ein Problem beim Filtern der Datenmenge dar.

Überhaupt nicht erwähnt wird, wie nicht zugestellte oder geblockte E-Mails behandelt werden sollen.

Unklar ist auch, wie die Anbieter die Datenflut filtern sollen. Insbesondere für Betreiber von E-Mail-Servern tritt die Frage auf, wie sie die Absender- beziehungsweise die Empfänger-Adressen aus dem Datenstrom filtern sollen.

Um die gespeicherten Daten sinnvoll verwenden zu können, müssen sämtliche Anbieter in Europa dieselbe Uhrzeit, abhängig von der jeweiligen Zeitzone in der sie sich befinden, auf allen ihren Rechnern einstellen und synchron halten.

Durch Trojaner[13] oder durch Ausspähen oder Phishen von Passwörtern oder anderer persönlicher Daten kann es zu falschen Beschuldigungen gegenüber den Usern kommen, wenn deren Accounts oder Daten für kriminelle Tätigkeiten verwendet werden. Denn dann müssen unschuldige User beweisen, dass ihre Daten ausgespäht wurden, was in der Praxis schwierig ist.

[13] Trojaner sind unerwünschte oder schädliche Programme, dies sich als nützliche Programme. Sie erfüllen allerdings ohne das Wissen des Anwenders im Hintergrund ganz andere Funktionen.

4.1.7 Unvereinbarkeit mit bestehenden Rechtstexten

Die Richtlinie wurde auf Basis der ersten ***Säule der EU*** beschlossen. Der Europäische Rat hat sich hierbei auf alleinige Gesetzgebungsbefugnisse berufen. Sein juristischer Dienst, die EU-Kommission und der Rechtsausschuss des EU-Parlaments vertreten allerdings die Auffassung, dass der Rat keine Allein-Befugnis hatte, sondern auf die Mitbestimmung der EU-Mitgliedstaaten im Wege nationaler Gesetzgebung angewiesen war und der Rat somit seine Befugnisse überschritten hatte. Der Austausch und Zugriff auf die gespeicherten Daten stellen Maßnahmen auf Basis der dritten Säule dar. Ein Beschluss auf der dritten Säule wäre notwendig gewesen, damit die Mitgliedsländer die erfassten Daten auch tatsächlich unter einander aus den anderen Ländern abgefragt werden dürfen. So müssen die EU-Mitgliedsländer Regelungen auf nationaler Ebene treffen, wodurch es wiederum zu unterschiedlichen Gesetzgebungen kommen wird.

Auch der Grundsatz der ***Unschuldsvermutung*** wird verletzt. Die Data Retention ist keine Einzelfallmaßnahme, sondern eine pauschale Überwachung aller 450 Millionen EU-Bürger. Außerdem besteht kein konkreter Verdacht, aufgrund dessen eine Überwachungsmaßnahme angeordnet werden könnte. Die Data Retention ist eine pauschale Überwachungsmaßnahme gegenüber allen EU-Bürgern

Datenschützer geben an, dass die Richtlinie tief greifende Auswirkungen auf bereits bestehende Rechtstexte haben wird, die den Nutzer schützen sollen. Insbesondere ***Artikel 8 der Europäischen Menschenrechtskonvention*** (EMRK 1950: Art. 8) soll dadurch massiv eingeschränkt werden. Dieser besagt, dass das Privat- und Familienleben, die Wohnung und der Briefverkehr sowie die Verkehrs- und Zugangsdaten zu Kommunikationsnetzen und -Diensten geschützt werden müssen. Ein Eingriff in dieses Recht muss *„im Sinne eines konkreten Ausnahmetatbestandes geregelt"* sein, so Franz Schmidbauer. Eine richterliche Genehmigung ist dafür nicht erforderlich. Durch das Umsetzen der Richtlinie wird somit ein Teil dieser Konvention zum Schutz der Menschenrechte und Grundfreiheiten außer Kraft gesetzt. Da die Konvention in der österreichischen ***Verfassung*** garantiert ist, müsste die Verfassung dementsprechend angepasst werden, so Ing. Martin Prager.

Auch das ***Fernmeldegeheimnis***, das in Artikel 10a des Staatsgrundgesetzes festgelegt ist und das Grundrecht auf Datenschutz (DSG 2000:§1) werden verletzt. Die EU-Richtlinie ist nicht mit der ***EU-Datenschutzrichtlinie*** und dessen Umsetzung ins ***österreichische Datenschutzgesetz*** vereinbar. Der Datenschutz verbietet grundsätzlich das Aufbewahren und Auswerten von Daten, hingegen ist in der Richtlinie zur Data Retention genau das für die Dauer von sechs bis 24 Monaten vorgesehen. Die EU-Datenschutzrichtlinie ermöglicht eine ausnahmsweise Vorratsdatenspeicherung für einen begrenzten Zeitraum, falls dies notwendig, angemessen und verhältnismäßig sowie im öffentlichen Interesse ist. Die umfassende Vorratsspeicherung darf nicht der Regelfall sein. Sie ist bei Bedarf auf nationaler Ebene zu beschließen. Weiters widerspricht die Richtlinie einem der Hauptprinzipien des Datenschutzgesetzes, der Datenvermeidung.

Zudem wird das ***Recht auf informationelle Selbstbestimmung*** und das ***Recht auf Richtigstellung*** beeinflusst. Auch das Recht, Auskünfte zu verlangen, wird durch mangelnde Bestimmungen über Informationspflichten der Strafverfolgungsbehörden gegenüber den Bürgern außer Acht gelassen.

Das ***Telekommunikationsgesetz*** wird ebenfalls durch die Richtlinie beeinflusst. Es besagt, dass die Daten sofort nach Erbringung des Dienstes gelöscht oder anonymisiert werden. Stammdaten müssen spätestens ein Jahr nach Beendigung des Vertragsverhältnisses gelöscht werden. Verkehrsdaten dürfen nur für Abrechnungszwecke gespeichert werden, die ebenfalls nach der Einspruchsfrist gelöscht werden müssen. (siehe Kapitel 2.1.2.1 Regelungen des TKG)

4.1.8 Mögliche Auswirkungen auf Wirtschaft und Gesellschaft

Welche Auswirkungen die Richtlinie tatsächlich auf Wirtschaft und Gesellschaft haben wird, ist jetzt noch nicht abschätzbar, da die Richtlinie in Österreich voraussichtlich erst im Jahr ***2007*** in nationales Recht umgesetzt wird.

Für die ***Wirtschaft*** könnte die Richtlinie zu einem Wettbewerbsnachteil führen, wenn kein angemessener Kostenersatz beschlossen wird. Laut Herrn Ing. Martin Prager überlegen bereits einige Firmen, den Standort ihrer Systeme in Länder zu verlagern, in denen keine Regelungen bezüglich Data Retention bestehen. Außerdem könnten Klein- und Mittelunternehmen in finanzielle Schwierigkeiten kommen, falls der Kostenersatz nicht auch die Investitionskosten umfasst. Keine Bank würde ein Darlehen für die Anschaffungskosten der Systeme gewähren, wenn keine Zusage der öffentlichen Hand vorliegt, die besagt, dass die Kosten den Betreibern ersetzt werden. Zudem haben die Anbieter nicht nur die Regelungen der Richtlinie einzuhalten, sondern

auch ihre Verantwortung ihren Kunden gegenüber wahrzunehmen.

Herr Georg Chytil denkt, dass die Kosten für die Internetnutzung europaweit um 10 bis 20 Prozent steigen werden. Dies könnte die Kunden dazu veranlassen, zu Anbietern außerhalb der EU abzuwandern. Das wiederum würde zu einem Gewinnrückgang bei den Providern führen. Dadurch könnten weitere Unternehmen ihren Standort in ein Nicht-EU-Land verlagern.

Die ISPA gibt in ihrem Positionspapier zur Data Retention an, dass die Umsetzung der Richtlinie zu einem Aufweichen des Fernmeldegeheimnisses führen wird. Dadurch würden die Kunden das Vertrauen in die Anbieter verlieren. Die geringere Nutzung des Internets und die daraus resultierenden Gewinneinbußen könnten dazu führen, dass die Forschung und Entwicklung auf diesem Sektor beeinträchtigt würden.

Gegner der Richtlinie sind der Ansicht, dass der Beschluss der Data Retention ein weiterer Schritt in Richtung Überwachungsstaat ist, und dass die ***Bürger*** der EU immer mehr zu „gläsernen Menschen“ werden.

Laut Herr Ing. Martin Prager ist die Missbrauchsgefahr wegen der großen Menge sensibler Daten sehr groß. In Österreich gilt die in der Verfassung festgelegte Unschuldsvermutung, was bedeutet, dass die Exekutive dem beschuldigten Bürger beweisen muss, dass seine Handlungen illegal waren. Herr Ing. Martin Prager gibt zu bedenken, dass unbescholtene Bürger nicht geschützt würden und die Richtlinie zur Beweislastumkehr führen könnte, also dazu, dass unbescholtene Bürger ihre Unschuld beweisen werden müssen. Herr Georg Chytil vermutet daher, dass die Richtlinie dazu führen wird, dass die Kunden die Dienste bewusster nutzen werden, da sie wissen, dass sämtliche Kommunikationen aufgezeichnet werden.

4.2 Umgehensmöglichkeiten

Es gibt verschiedene Möglichkeiten zu verhindern, dass die Kommunikation der User in der Data Retention nicht oder nur verzerrt aufgezeichnet werden kann.

Die einfachste Möglichkeit, um im Internet anonym zu bleiben, ist wahrscheinlich die ***Angabe falscher Daten*** oder das Verwenden von falschen ***Identitäten***. Dies ist vor allem beim Ausfüllen von Anmeldeformularen oder sonstigen Formularen, die persönliche Daten abfragen, eine weit verbreitete Methode.

Auch durch das Telefonieren in ***öffentlichen Telefonzellen*** oder das Surfen in ***Internet-Cafes*** bleiben die Nutzer weitgehend anonym. Um auch wirklich unerkannt zu bleiben, wird man im Internet-Cafe nicht mit Bankomat- oder Kreditkarten bezahlen. Durch die Benützung dieser Zahlungsmittel können der Zeitpunkt, der Ort und die bezahlte Leistung zurückverfolgt werden.

Für den Zugang zum Internet über ***Wireless LAN*** können ***ungeschützte*** oder ***offene Hotspots*** verwendet werden. In Wien beispielsweise gibt es einige Lokale, die den Gratis-Zugang über offene Hotspots ermöglichen. Einige Internet-User mit Flatrate-Tarifierung lassen absichtlich ihre Hotspots unverschlüsselt, um anderen Nutzern das Surfen in ihrem Netz zu ermöglichen, so Herr Georg Chytil.

Auch durch den Zugang zum Internet über ***gehackte Rechner*** bleiben die Urheber von Kommunikation unerkannt. Dies stellt allerdings ein großes Problem für den Besitzer des gehackten Rechners da, wenn Illegales über seinen Computer geschieht. Dann muss er beweisen, dass nicht er selbst, sondern ein Hacker dafür verantwortlich ist.

In Österreich können ***Prepaid-Handys***, die auch als Wertkartenhandys bezeichnet werden, ohne Angabe der Identität erworben werden. Dies ist nicht in allen EU-Mitgliedsländern möglich. Bei der ersten Aktivierung eines Prepaid-Handys werden der genaue Zeitpunkt und die Cell-ID aufgezeichnet. Um völlig anonym zu bleiben, könnte das Endgerät in einem kleinen Geschäft ohne Kameraüberwachung gekauft und erst einige Monate nach Erwerb und nicht nahe dem Wohnort erstmals aktiviert werden. Diese Wertkartenhandys können sowohl für das Telefonieren, als auch für die Einwahl ins Internet verwendet werden.

Da beim Versenden von E-Mails Teile der Stammdaten des Nutzers und des Adressaten aufgezeichnet werden müssen, können E-Mails über Anbieter für ***Webmail*** versandt werden, die außerhalb der EU agieren. Auch beim Anmelden zu Webmail-Diensten geben die Nutzer häufig falsche Identitäten an, wodurch sie zusätzlich geschützt werden. Durch das Verwenden von Diensten, die nach der EU-Richtlinie nicht erfasst werden müssen, können Informationen auch anonym übertragen werden. Anstelle von E-Mails können ***Messaging-Dienste*** oder Chat-Programme verwendet werden. Über Instant Messaging können die User in Echtzeit mit einander kommunizieren, also chatten, und Daten austauschen. Außerdem können Informationen und Dateien ebenfalls über ***File-Sharing***-Programme ausgetauscht werden. Weiters ist die ***Internet-Telefonie***, auch Voice-over-IP genannt, von der Vorratsspeicherungspflicht ausgenommen, so die IT-News Website „futurezone". Einzig Voice-over-IP-Anrufe, die im Telefonfestnetz enden, müssen am Verbindungsknoten zum Festnetz aufgezeichnet werden. Erfasst werden können dann nur die angerufene Nummer und der Verbindungsknoten, über den der Anruf weitergeleitet wurde. Der Gesprächsursprung und die Identität des Anrufers können nicht oder nur sehr schwer festgestellt werden.

Außerdem gibt es verschiedene ***Anonymisierungstechniken***, um die Identität des Nutzers zu verschleiern. Anonymizer sind nach der Online-Zeitschrift „heise.de" Software oder Dienste, die den User anonymisieren und verhindern, dass er anhand der IP-Adresse identifiziert werden kann.

Kai Billen nennt als einfachste Methode die Verwendung von ***Rewebbern***. Hierbei wird die Homepage des Rewebbers im Internet Explorer aufgerufen und in einem Formular die URL der zu besuchende Website eingegeben. Der User wird daraufhin auf die eigentlich gewünschte Homepage weitergeleitet. Man kann auch Personal Firewalls, also Paketfilter, als einfachste Form von Anonymizern ansehen. Sie simulieren einen lokalen Proxyserver, der allerdings die wahre IP-Adresse des Absenders nicht verschleiern kann, sondern nur Begleitinformationen, wie Informationen über das Betriebssystem oder den Webbrowser versteckt. Bei echten ***anonymisierenden Proxys*** wird eine Anfrage nicht direkt zwischen dem User und dem Webserver ausgetauscht, sondern über eine so genannte Mix Proxy Kaskade weitergeleitet. Dies ist eine Kette mehrerer Proxy-Rechner, die bei einer Anfrage hintereinander geschalten werden. Die Verbindungen des Benutzers zur ersten Kaskade und jene zwischen den Mixproxys der Kaskade sind zumeist verschlüsselt.

Anonymous Remailer sind nach André Bacard Dienste, die E-Mails *„ent-personalisieren"*. Dadurch können E-Mails oder Usenet-Beiträge anonym versendet werden und weder der Name noch die E-Mail-Adresse können identifiziert werden. Beim Versenden von E-Mails über Remailer werden der echte Name und die Adresse aus dem Mail-Header gelöscht und durch eine Tarnadresse ersetzt und an den Adressaten weitergeleitet.

Eine weitere eher unbekannte Möglichkeit Informationen zu verschleiern, ist die ***Steganographie.*** Kai Billen schreibt hierzu auf seiner Homepage: *„Über steganografische Algorithmen ist es möglich, die Bits einer Datei zwischen den Bits einer Bild- oder Tondatei zu verstecken. Äußerlich betrachtet ergibt sich zwischen der Rohdatei und der steganografische behandelten Bild- oder Tondatei (...) kein erkennbarer Unterschied."* Da bei elektronischen Daten eine gewisse unmerkliche Fehlertoleranz vorliegt, können in digitalisierten Bildern und Audio-Dateien Informationen versteckt werden, ohne dass sich das Gesamtbild beziehungsweise der Ton verändert. Steganographie kann vor allem dort verwendet werden, in denen der Austausch verschlüsselter Daten verboten ist, wie beispielsweise in Frankreich, aber auch in Ländern wo die Kommunikation sehr streng überwacht oder gar Informationen zensiert werden. Die Steganographie ist nur als Ergänzung, nicht aber als Ersatz der Kryptografie anzusehen.

5 Ergebnisse

Ziel dieser Diplomarbeit war es herausfinden, welche Auswirkungen die EU-Richtlinie auf die Bürger der EU, die Wirtschaft und die rechtliche Situation haben wird.

Dabei bin ich von folgenden Hypothesen ausgegangen: Die Vorratsdatenspeicherung von Ruf- und Verkehrsdaten bedeutet einen tiefen Eingriff in die Privatsphäre der Bürger. Ein mangelnder Kostenersatz bedeutet eine zusätzliche massive finanzielle Belastung für die Anbieter von Telekommunikationsdiensten.

In Österreich gibt es keine gesetzlichen Bestimmungen über Vorratsdatenspeicherung. Es gibt verschiedene Regelungen, um die Interessen der Bürger zu schützen. Es besteht das Recht auf das Fernmeldegeheimnis, das nicht verletzt werden darf und das Recht auf informationelle Selbstbestimmung. Artikel 8 der Europäischen Menschenrechtskonvention sichert die Vertraulichkeit der Kommunikation. Das Datenschutzgesetz und Abschnitt 12 des Telekommunikationsgesetzes legen fest, in welchen Fällen welche Daten zu welchem Zweck wie lange gespeichert werden dürfen. Grundsätzlich sind die Anbieter zur Geheimhaltung verpflichtet. Sie müssen jene Daten, die durch die Diensteerbringung entstehen unverzüglich löschen oder anonymisieren, soweit sie für die Rechnungslegung nicht mehr benötigt werden. Die Betreiber dürfen nur jene Stammdaten erfassen, die für einen Vertragsabschluss, deren Änderung oder Beendigung benötigt werden. Diese Bestandsdaten müssen spätestens nach Vertragsende gelöscht werden.

Trotz allem ist es nötig, dass die gespeicherten Daten von der Exekutive genutzt werden können, um schwere Straftaten aufzuklären. Es bestehen daher gesetzliche Regelungen, wobei das schützenswürdige Interesse des Einzelne hinter das Interesse des Staates gestellt wird. Diese Bestimmungen werden in der Überwachungsverordnung und der korrespondierenden Überwachungskostenverordnung geregelt.

Das Europäische Parlament und der Europäische Rat haben Mitte Dezember 2005 eine Richtlinie bezüglich Vorratsdatenspeicherung beschlossen. Sie besagt, dass alle Anbieter von öffentlichen Diensten und Betreiber von öffentlichen Netzen in den Mitgliedstaaten verpflichtet sind, Ruf- und Verkehrsdaten für mindestens 6 Monate und maximal zwei Jahre zu speichern. Es wird grundsätzlich zwischen Anbietern von Festnetz- und Mobiltelefonie und Anbietern von Internetdiensten unterschieden. Im Groben umfassen die zu speichernden Daten Angaben wie Rufnummer, Benutzerkennung oder IP-Adresse, den Namen und die Anschrift der Teilnehmer, Datum und Uhrzeit sowie Dauer der Kommunikation. Außerdem müssen die Art der (mutmaßlichen) Endeinrichtung und die Art des in Anspruch genommenen Dienstes aufgezeichnet werden. Die verpflichtende Speicherung umfasst auch erfolglose Anrufversuche. Es dürfen keinerlei Daten gespeichert werden, die Aufschluss über den Inhalt der Kommunikation geben können. Regelungen bezüglich Datenschutz und Datensicherheit sowie über den Zugang zu den Daten müssen von den EU-Ländern in den nationalen Gesetzgebungen festgelegt werden.

Gegner der Richtlinie kritisieren, dass es keine Regelungen über einen angemessenen Kostenersatz, weder für die laufenden Kosten noch für die Investitionskosten gibt. Dies kann, muss aber nicht in der Legislative der Mitgliedsländer geregelt werden. Werden keine solchen Bestimmungen getroffen, bestätigt sich meine Hypothese, dass es zu einer massiven finanziellen Belastung der Anbieter kommen wird.

Die Richtlinie kann außerdem aus einigen technischen Gründen so nicht umgesetzt werden. Auch die enorme Menge an zu speichernden Daten konfrontiert die Anbieter mit Filterproblemen.

Die Richtlinie ist unvereinbar mit einigen bestehenden Rechtstexten, sowohl auf österreichischer, als auch auf europäischer Ebene. Zunächst hätte die Direktive auf Basis der dritten Säule der EU beschlossen werden müssen, um einen Austausch der gespeicherten Daten zwischen den Ländern zu ermöglichen. Auch der Artikel 8 der Europäischen Menschenrechtskonvention, der in der österreichischen Verfassung garantiert wird, wird durch die Richtlinie massiv eingeschränkt. Das Fernmeldegeheimnis, das österreichische Datenschutzgesetz, das Telekommunikationsgesetz, das Prinzip der Unschuldsvermutung und das Recht auf informationelle Selbstbestimmung werden ebenfalls verletzt. Da alle diese Regelungen zum Schutz der Bürger erlassen wurden und nun durch die Umsetzung der Richtlinie verletzt werden, bestätigt sich auch meine zweite Hypothese, die besagt, dass die Richtlinie einen massiven Eingriff in die Privatsphäre der EU-Bürger darstellt.

Einige Länder haben aus diesen Gründen bereits eine Klage vor dem Europäischen Gerichtshof angekündigt. Wenn sie Recht bekommen sollten, wird das EU-Parlament die Richtlinie überarbeiten und eine neue verabschieden müssen. In der Zwischenzeit werden allerdings einige EU-Länder, beispielsweise Frankreich, gesetzliche Regelungen getroffen haben, die dann wiederum aktualisiert werden müssen. Die Betreiber in diesen Ländern werden ihre Systeme an die Richtlinie erneut anpassen werden müssen.

Offen bleibt die Frage, welche Auswirkungen die EU-Richtlinie tatsächlich auf die Gesellschaft haben wird. Dies kann erst nach der Umsetzung in nationales Recht beurteilt werden.

6 Bibliographie

- Bacard A. (1995). The Computer Privacy Handbook. California: Peachpit Press
- Bericht A6-0365/2005 über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden und zur Änderung der Richtlinie 2002/58/EG
- Bleich H., Heidrich J. (2002). Ach wie gut, dass niemand weiß... c't Magazin für Computertechnik. Nr. 19, Seite 124
- *Brandl E., Mayer-Schönberger V.* (2006). Datenschutzgesetz. Wien: Linde Verlag.
- Bundesgesetz über die Organisation der Sicherheitsverwaltung und Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG). idF. BGBl. Nr. 566/1991 ST0205
- *Klußmann N. (2001). Lexikon der Kommunikations- und* Informationstechnik. Telekommunikation, Internet, Mobilfunk, Multimedia, Computer, E-Business. Heidelberg: Hüthing Verlag.
- *Parschalk M., Otto G., Weber J., Zuser A.* (2006). Telekommunikationsrecht. Wien: Linde Verlag.
- Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).
- 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
- Richtlinie PE-CONS 3677/05 des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG
- *Ritz Ch.* (2005). Bundesabgabenordung. Wien: Linde Verlag.

- Strafprozessordnung 1975. BGBl. Nr. 631/1975 (WV)., idF. BGBl. I Nr. 119/2005
- Verordnung der Bundesministerin für Justiz über den Ersatz der Kosten der Betreiber für die Mitwirkung an der Überwachung einer Telekommunikation (Überwachungskostenverordnung - ÜKVO). idF. BGBl. II Nr. 322/2004
- Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung – ÜVO). idF. BGBl. II Nr. 418/2001

Online-Literatur

- *Billen, K.* „Steganographie mit F5, Guess und Steghide". Retrieved April 2006, from http://kai.iks-jena.de/stego/stego.html
- *Billen, K.* „Sicher und anonym im Internet mit Proxys". Retrieved April 2006, from http://kai.iks-jena.de/bigb/asurf.html#a1
- *Büllingen F., Gillet A., Gries Ch., Hillebrand A., Stamm P.* (2004). Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich. Retrieved November 2005, from http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf
- Entschließung des Rates der Europäischen Union über die rechtmäßige Überwachung des Telekommunikationsverkehrs in Bezug auf neue Technologien (Enfopol 98). Retrieved Jänner 2006, from http://www.heise.de/tp/r4/artikel/6/6326/2.html
- *Fox. D.* Der IMSI-Catcher. Retrieved Dezember 2005, from http://www.secorvo.de/publikationen/imsicatcher-fox-2002.pdf
- *Heyer A.* (2002). Datenfass ohne Boden. Die Kernfragen zu Data Retention in Europa. Retrieved März 2006, from http://www.politik-digital.de/econsumer/datenschutz/retent2.shtml
- *Internet Service Providers Austria* (2005). Positionspapier Vorratsdatenspeicherung. Retrieved Dezember 2005, from http://www.ispa.at/downloads/86dad947a09f_ISPA_Positionspapier_Data-Retention.pdf
- *Internet Service Providers Austria (2005).* Allgemeine Regeln zur Haftung und Auskunftspflicht des ISP. Retrieved Oktober 2005, from http://www.ispa.at/downloads/1937e3c02fb2_Allgemeine_Regeln_zur_Haftung_und_Auskunftspflicht_des_ISP.pdf

- *Krempl S.* (2006). Fragen und Fakten zur Vorratsspeicherung von Telefon- und Internetdaten. Retrieved März 2006, from http://www.heise.de/ct/aktuell/meldung/69995
- *Matthaei R. (2005).* Der URL. Retrieved Mai 2006, from http://home.arcor.de/fredrik.matthaei/HTML/URL.htm
- *Moechel E.* (2006). EU-Minister segnen Datenspeicherung ab. Retrieved Feber 2006, from http://futurezone.orf.at/it/stories/91017
- *Moechel E.* (2006). EU-Richtlinie von Technik überholt. Retrieved April 2006, from http://futurezone.orf.at/it/stories/101686
- *Office of Public Sector Information* (2002-2005). Regulation of Investigatory Powers Act 2000. Retrieved Jänner 2006, from http://www.opsi.gov.uk/acts/acts2000/20000023.htm
- *Schmidbauer F.* (2006). Staatsgrundgesetz vom 21. Dezember 1867, über die allgemeinen Rechte der Staatsbürger für die im Reichsrate vertretenen Königreiche und Länder - StGG. Retrieved Feber 2006, from http://www.internet4jurists.at/gesetze/stgg.htm
- *Schmidbauer F.* (2006). Auskunft über Kundendaten. Retrieved Jänner 2006, from http://www.internet4jurists.at/provider/auskunft1a.htm
- *Schmidbauer F.* (2006). Entscheidungen zur Auskunftspflicht (Ö). Retrieved März 2006, from http://www.internet4jurists.at/provider/entsch4a.htm
- *Schmidbauer F.* (2006). Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, BGBl. 1958/210 samt Zusatzprotokoll vom 20.3.1952, GBBl 1958/210 und österreichischer Vorbehalt zur MRK. Retrieved Jänner 2006, from http://www.internet4jurists.at/gesetze/emrk.htm#Artikel_8
- *Weinknecht J.* (2003). Schutz von Domains - Was ist eigentlich eine Domain? Retrieved Mai 2006, from http://www.weinknecht.de/ojr/index.html?/ojr/1996/2.htm

VII Anhang

VII.1 Interviewpartner

Chytil Georg, am 21.02.1006

Präsident der ISPA - Internet Service Provider

Verband der österreichischen Internet-Anbieter
1090 Wien, Währingerstrasse 3/18
Telefon: 01 4095576, E-Mail: Georg.Chytil@nextlayer.at

Mag. Leschanz Judith, am 16.02.2006

head of legal expert center

mobilkom austria AG & Co KG
1020 Wien, Obere Donaustraße 29
Telefon: 0664 3312170, E-Mail: j.leschanz@mobilkom.at

Mag. Paulhart Gert, am 16.02.2006

business devolpment, interconnection manager

mobilkom austria AG & Co KG
1020 Wien, Obere Donaustraße 29
Telefon: 0664 3312021, E-Mail: g.paulhart@mobilkom.at

Ing. Prager Martin, am 13.03.2006

Leiter der Expertsgroup IT-Security des Fachverbandes Unternehmensberatung und Informationstechnologie (UBIT)

Wirtschaftskammer Österreich
A-1045 Wien, Wiedner Hauptstraße 63
Telefon: 0699 17520908, E-Mail: Prager@Prager.at

VII.2 Fragenkatalog für Leitfadeninterviews

- Was verstehen Sie unter Rufdatenerfassung?
- Welche Daten werden erfasst? Was genau sind Verbindungsdaten? Was sind Stammdaten? Gehört dazu auch, welche Internetseiten aufgerufen wurden?
- Wie ist Ihre persönliche Meinung bezüglich Data Retention?

- Wird auch Kommunikation via SMS / WAP überwacht? Wenn ja, werden auch Inhalte der Kommunikation aufgezeichnet?
- Was werden Experten mit den erfassten Daten über die überwachte Person herausfinden können? Was können sie derzeit über die User herausfinden?
- Werden die zusätzlichen Informationen, die über Data Retention erfasst werden den Experten auch qualitativ hochwertigere Informationen liefern oder wird nur die Menge an Daten über mehr User steigen?
- Welche technischen Möglichkeiten stehen zur Überwachung von Mobiltelefonen zur Verfügung?
- Wenn nur das Mobiltelefon identifiziert werden kann, wie wird der Besitzer eines Wertkartenhandys ermittelt?
- Könnten die erfassten Daten über eine Person nicht verfälscht werden?
- In welcher Form werden die Daten gespeichert? Wird es einen EU-weiten Standard geben? Wo werden die Daten gespeichert werden (bei Providern oder zentral)?
- Welche Menge an Daten wird anfallen? Wie viel ist es zurzeit?
- Wie werden die gespeicherten Daten geschützt? Welche Auswirkungen wird Data Retention noch auf die Anbieter haben? Welche organisatorischen Maßnahmen werden sie setzen müssen?
- Werden die Daten auch noch nach einigen Jahren verwertbar sein?

- Wer wird auf die Daten zugreifen können?
- Werden die erfassten Daten in irgendeiner Form verschlüsselt / vor dem Zugriff von Dritten / Missbrauch geschützt?
- Wie wird sichergestellt werden, dass die Unternehmen, die Data Retention durchführen werden, nicht selbst auf die Daten zugreifen können, sie für eigene Zwecke verwenden oder an Dritte verkaufen können?
- Werden diese Unternehmen Zugriff auf anonymisierte Daten haben?

- Wer darf zurzeit erfasste Daten auswerten? Wird sich daran nach der Umsetzung der Richtlinie etwas ändern?
- Wie werden die Daten dem Auswertenden übermittelt?
- Wie können diese Mengen zusammengeführt und ausgewertet werden?
- Wie sinnvoll ist die Auswertung?

- Welche technische Maßnahmen zur Umsetzung der EU-Richtlinie sind sinnvoll / möglich?
- Welche Kosten fallen durch die Speicherung der Daten an und wer muss sie tragen?

- Werden die Kosten den ISPs ersetzt? Wie können die ISPs ihren Anspruch geltend machen? Wie wird dieser Kostenersatz errechnetet werden?
- Wenn beispielsweise eine Deutsche Firma Daten aus England speichert und an diese beauskunftet, wer übernimmt die Kosten?
- Kosten-Nutzen-Faktor?

- Wie ist die derzeitige rechtliche Lage?
- Welche Daten werden zurzeit erfasst?
- Welche Daten müssen beauskunftet werden?
- Was ist der Unterschied zwischen der Überwachungs-Verordnung und Data Retention?

- Die Auslieferung und in Folge dessen die Auswertung der Daten erfolgt auf richterliche Anweisung, wie wird die Kompetenz des Richters sichergestellt? Wer kommt als Gutachter in Betracht?
- Wie lange dürfen Verkehrsdaten momentan gespeichert werden?
- Wie lange werden sie vermutlich in Österreich gespeichert werden müssen? (nach Umsetzung der Richtlinie)
- Wer wird in Österreich die Umsetzung der Richtlinie durchführen?
- Welche Auswirkungen hat die EU-Richtlinie auf das österreichische Recht? Welche Gesetze müssen angepasst werden?
- Dürfen die EU-Staaten Data-Retention-Daten untereinander austauschen?

- Welche Risiken bestehen für die Konsumenten durch die Speicherung der Ruf- und Verkehrsdaten?
- Geht Österreich in Richtung Überwachungsstaat?
- Welche Auswirkungen könnte Data Retention auf die Gesellschaft haben?
- Welche wirtschaftlichen Auswirkungen könnten durch die Umsetzung der Richtlinie entstehen?
- Könnte Data Retention Firmen bei der Wahl Österreichs oder der EU als Wirtschaftsstandort beeinträchtigen?
- Welche Kettenreaktionen könnten von einer Überwachung ausgelöst werden? Werden Kommunikationspartner des Überwachten mit-überwacht? Wie werden unbescholtene Bürger geschützt?
- Sind einige Personen von Data Retention ausgenommen?
- Drittländer könnten sehr an den erfassten Daten interessiert sein. Werden sie Zugriff auf die Daten haben können?
- Wie könnte die Rufdatenerfassung umgangen werden?

- Gibt es einen internationalen Vorreiter bezüglich Data Retention?
- Wer war in Österreich die treibende Kraft? Wer war international die treibende Kraft?

- Was war die Motivation? Gab es eine politische Motivation für die Entscheidung?
- Hat Österreich aktiv bei der Entwicklung der Richtlinie mitgewirkt?
- Welche Argumente gab es für bzw. gegen die Richtlinie? Von wem kamen sie?
- Welche der österreichischen Vorschläge wurden umgesetzt (wenn auch abgeändert)? Welche konnten nicht umgesetzt werden?
- Wer sind die Gegner von Data Retention? Was sind deren Argumente?
- Die Kommission wurde von Experten beraten. Was haben diese der Kommission geraten? Deckt sich die Expertenmeinung mit jener der Verordnungserlasser?
- Warum wurde die Richtlinie trotz Abraten von Experten beschlossen?
- Was war das entscheidende Argument für die Richtlinie, dass die Expertenmeinung außer Acht gelassen wurde?

7 Lebenslauf

Karin Larnhof

Geboren am 8. Juli 1983 in Oberpullendorf (Burgenland)

Schulbildung:

2002-2006	Fachhochschule für Informationsberufe, Eisenstadt
1997 – 2002	HWL Theresianum Eisenstadt Matura 2002
1994 – 1997	Hauptschule Theresianum Eisenstadt
1993 – 1994	Gymnasium Wolfgarten Eisenstadt

Berufspraxis:

Juni bis Aug. 2000	Pflichtpraktikum im Hotel Lengauerhof, Saalbach-Hinterglemm
Aug. 2001	Ferialpraxis bei BEGAS, Eisenstadt
Juli bis Aug. 2002	Ferialpraxis bei Kelemen & Mollatz Wirtschaftstreuhand, Eisenstadt
Sommersemester 2003	Projekt mit Knowledge Management Austria, Wien: Entwicklung einer Wissensstrategie
Juli 2003	Berufsorientierungspraktikum bei Well.COM Datahighway Burgenland, Eisenstadt
Aug. 2003	Ferialpraxis bei Kelemen & Mollatz Wirtschaftstreuhand, Eisenstadt
Sommer- und Wintersemester 2003/04	Projekt mit dem Verein KIBu - Komponisten und Interpreten im Bgld.: Entwicklung von Maßnahmen zur Verbesserung der Öffentlichkeitsarbeit
Aug. 2004	Ferialpraxis bei Well.COM Datahighway Burgenland, Eisenstadt
Wintersemester 2005	Projekt mit Mag. Burkhard Neumayer: Entwicklung einer virtuellen Galerie
Aug. bis Feber 2005/06	Berufspraktikum bei INVARIS Informationssysteme GmbH