wik-Consult • Bericht

Studie für
BITKOM Servicegesellschaft mbH

Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich

Franz Büllingen
Aurélia Gillet
Christin-Isabel Gries
Annette Hillebrand
Peter Stamm

Bad Honnef, Oktober 2004

wik CONSULT

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AFA	Access providers association
AFA	l'Association des Fournisseurs d'Accès et de services (Internet Access Provider Association)
AFORM	Association Francaise des Opérateurs de Réseaux Multiservices
AFORM	Association Française des Opérateurs Multiservices
APD	Agencia de Protección de Datos
ATCSA	Anti-Terrorism, Crime And Security Act 2001
BGBl.	Bundesgesetzblatt
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BOE	Boletín Oficial del Estado
BOS	Behörden mit Sicherheitsaufgaben
CALEA	Communications Assistance for Law Enforcement Act
CGVoP	Carrier Grade Voice over Packet
CIOT	Central Information System for Telecommunication Investigation
CNIL	Commission Nationale de l'Informatique et des Libertés
CSP	Communications Service Provider
DC	Conseil Constitutionnel
DC	decision relative au contrôle de la constitutionnalité des normes
DR	Data Retention
ECPA	Electronic Communications Privacy Act
EMS	Electronic Mail Service
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission

GCHQ	Government Communications Headquarters
IMEI	International Mobile Equipment Identification
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IRC	Internet Relay Chat
ISP	Internet Service Provider
LCE	Loi N°2004-669 sur les communications électroniques
LEA	Law Enforcement Agency
LOPD	Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal (Gesetz 15/1999 vom 13. Dezember über den Schutz persönlicher Daten)
LSQ	Loi N°2001-1062 sur la Sécurité Quotidienne
LSQ	Loi N°2001-1062 sur la Sécurité Quotidienne
LSSI	Ley 34/2002 de 11 de julio, se servicios del sociedad de la información y de comercio electrónico (Gesetz 34/2002 vom 11. Juli über Dienste der Informationsgesellschaft und Electronic Commerce)
MI5	The Security Service
MI6	The Secret Intelligence Service
MMS	Multimedia Messaging Service
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Station/Subscriber ISDN Number
NHS	National Health System
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
P&EC Code	Posts and Electronics Communications Code
P&EC Code	Posts and Electronics Communications Code (übergeordnetes Gesetz zum LSQ)
PR/TT	Pen Register/Trap and Trace

PSFND	Packet Surveillance Fundamental Needs Document
RIPA	Regulation of Investigatory Powers Act 2000
SIS	Secret Intelligence Service
SMS	Short Message Service
SPoC	Single Point of Contact
StPO	Strafprozessordnung
SW	Software
TIA	Telecommunications Industry Association
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
Tw	Telecommunicatiewet
ÜKVO	Überwachungskostenverordnung
URL	Uniform Ressource Locator
USC	United States Code
ÜVO	Überwachungsverordnung
VfGH	Verfassungsgerichtshof
Wet BOB	Wet Bijzondere opsporingsbevoegdheden
WKO	Wirtschaftskammer Österreich

Zentrale Ergebnisse der Studie

- Eine gesetzliche Verpflichtung zur Vorratsdatenspeicherung ist in den wenigsten TK-Märkten implementiert.
- Eine Speicherung „sämtlicher Verkehrsdaten“, wie sie der EU-Rahmenbeschlussentwurf vorsieht, findet in keinem der untersuchten Länder statt.
- Der Umfang der EU-weit geplanten Vorratsdatenspeicherung geht weit über die Daten hinaus, die bisher durch TK-Unternehmen für Unternehmenszwecke gespeichert werden. Die Speicherung erfolgt bislang hauptsächlich zu Abrechnungszwecken und für die Bereitstellung von Diensten.
- Aus datenschutzrechtlichen Gründen hätten Unternehmen keine Möglichkeiten, die zu speichernden Daten nutzbringend für eigene Zwecke zu verwenden, so dass eine Vorratsdatenspeicherung ausschließlich geschäftsfremden Zwecken mit entsprechend hohen Kosten dienen würde.
- Der Bedarf zur Einführung der geplanten Vorratsdatenspeicherung ist zweifelhaft. Systematische Studien zur Wirksamkeit konnten nicht identifiziert werden. Vorhandene Statistiken belegen, dass in den allermeisten Fällen nur auf die ohnehin vorhandenen Bestandsdaten zugegriffen wird.
- Verkehrsdaten, die älter als 3-6 Monate sind, werden von den Law Enforcement Agencies (LEAs) kaum angefordert. Daher sind Speicherungen, die über die derzeit praktizierte Dauer für Unternehmenszwecke hinausgehen, kaum zu rechtfertigen.
- Kostentreiber einer Vorratsdatenspeicherung wären vor allem die Anpassung der Systemtechnik zur Generierung und Speicherung der zusätzlichen Daten und die Anpassung der betrieblichen Abläufe zur Sicherung sowie zur Bearbeitung und Auswertung der Daten.
- Kostenentschädigungsregelungen finden sich in beinahe allen untersuchten Ländern. Damit Unternehmen in einzelnen Mitgliedstaaten keine Nachteile im internationalen Wettbewerb entstehen, erscheinen EU-weite Regeln für eine umfassende Kostenerstattung, die auch Investitionen berücksichtigt, erforderlich.
- ITK-Unternehmen, Daten- und Verbraucherschützer in allen EU-Ländern kritisieren den Rahmenbeschlussentwurf vehement, da die Effektivität einer Vorratsdatenspeicherung, die zu erwartende Kostenbelastung und Datenschutzaspekte bisher nicht ausreichend diskutiert wurden.
- Die Anhörung der EU-Kommission hat gezeigt, dass aus Sicht der EU-Kommission der Bedarf einer Vorratsdatenspeicherung bisher nicht hinreichend dargelegt und Kostenfragen nicht angemessen berücksichtigt wurden.

- Formalisierte Prozesse und Personalschulungen bei den Strafverfolgungsbehörden können in erheblichem Umfang dazu beitragen, die Effizienz zu erhöhen und Kosten bei den Unternehmen zu senken.

1 Management Summary

Gegenstand und Zielsetzung

Die vorliegende Vergleichsanalyse umfasst die aktuellen Regelungen (bis einschließlich September 2004) und wesentlichen Rahmendaten zur Vorratsdatenspeicherung[1] in den Ländern Frankreich, Italien, Niederlande, Österreich, Schweden, Spanien, Vereinigtes Königreich und den USA. Sie basiert zum einen auf Desk-Research und der Auswertung aller wesentlichen Dokumente. Zum anderen wurden Face-to-Face-Interviews mit einschlägigen Experten und Repräsentanten der zuständigen Behörden durchgeführt.

Die Ergebnisse sollen zu den anstehenden Diskussionen sowohl auf EU-Ebene wie auf nationaler Ebene beitragen, die im Zusammenhang mit dem EU-Rahmenbeschlussentwurf der Länder Frankreich, Irland, Vereinigtes Königreich und Schweden zur Harmonisierung der Vorratsdatenspeicherung innerhalb der EU angestoßen worden sind.[2] Der Rahmenbeschlussentwurf sieht vor, dass sämtliche Verkehrsdaten (einschließlich Standortdaten) sowie Bestandsdaten (Teilnehmer- und Nutzerdaten)[3] in den Bereichen der klassischen Telefonie (Festnetz und Mobilfunk) und des Internets für einen Zeitraum von mindestens 12 bis maximal 36 Monaten gespeichert werden müssen.

Hintergrund

Der Europäische Rat wurde in der vom Rat am 25. März 2004 angenommenen „Erklärung zum Kampf gegen den Terrorismus“ beauftragt, bis Juni 2005 Maßnahmen für die Erarbeitung von Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch TK-Diensteanbieter zu prüfen, damit diese für Zwecke der Strafverfolgung genutzt werden können. Dabei ist offen geblieben, ob eine generelle Regelung getroffen werden wird und wie diese ausgestaltet sein könnte.

Im Rahmen einer von den Generaldirektionen Informationsgesellschaft sowie Justiz und Inneres inzwischen durchgeführten schriftlichen Konsultation[4] sowie einer öffentlichen Anhörung am 21.09.04 in Brüssel haben ITK-Anbieter, Daten- und Verbraucherschützer aus Europa den Entwurf vehement kritisiert und zahlreiche Fragen aufgeworfen, deren Beantwortung durch öffentliche Institutionen und Behörden im wesentlichen noch aus-

---

1 Unter Vorratsdatenspeicherung wird in der Studie die Speicherung von bei der Erbringung von TK-Diensten anfallenden Daten (z.B. Bestandsdaten, Verkehrsdaten) zum Zweck der Strafverfolgung und Gewährleistung der nationalen Sicherheit verstanden.

2 Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus v. 28.04.2004.

3 Analog zu der Begriffsdefinition im deutschen TKG werden in der Studie unter Verkehrsdaten Verbindungsdaten und Standortdaten verstanden. Bestandsdaten sind diejenigen Daten, die einem Teilnehmer oder Nutzer zuzuordnen sind und die für das Vertragsverhältnis bedeutsam sind (z.B. Name, Rechnungsanschrift, Zahlungsart (z.B. Kontoverbindung), Rufnummer u.ä.). Sollten in den einzelnen Ländern andere Begriffsdefinitionen gebräuchlich sein, wird jeweils darauf hingewiesen.

4 Die Stellungnahmen zur Konsultation sind nicht öffentlich.

steht. Diese Fragen beziehen sich insbesondere auf folgende Aspekte, die bei einer Abwägung der Verhältnismäßigkeit zu berücksichtigen sind:

1. die Prüfung alternativer Lösungen wie z.B. Data Preservation,[5] die weniger aufwändig und grundrechtsschonender sind, und die ebenso geeignet sind, die berechtigten Interessen der Strafverfolgungsbehörden zu befriedigen wie die mit hohem finanziellen, organisatorischen und prozeduralen Aufwand verbundenen Maßnahmen zur Vorratsdatenspeicherung;

2. die bestehenden, vielfachen Möglichkeiten von Straftätern, eine Nachverfolgung der Kommunikation zu vereiteln;

3. der tatsächliche Bedarf der Behörden, auf Daten, die älter als 3-6 Monate zurückliegen, zuzugreifen. In der Regel werden Daten angefragt, die bis zu 3 Monate zurückliegen. Nur sehr selten werden Daten angefordert, die älter als 6 Monate sind;

4. die künftigen Veränderungen im Nutzerverhalten und die dadurch zusätzlich verursachte Kostenbelastung durch die breitere und intensivere Nutzung von Telekommunikationsdiensten insbesondere auch für kleine und mittlere Unternehmen;

5. die Ermittlung der durch die Einführung von Vorratsdatenspeicherung verursachten Kosten für die TK-Unternehmen unter Berücksichtigung des Aspekts, inwieweit Unternehmen im Einklang mit den jeweiligen Datenschutzregelungen die gespeicherten Daten auch für unternehmenseigene Zwecke nutzen können;

6. der Aufwand, der durch die Einführung von Vorratsdatenspeicherung verursachten Kosten für die einzelnen nationalen Anbietergruppen unter Berücksichtigung der jeweiligen Datenschutzregelungen und deren negative Implikationen für die Nutzung der gespeicherten Daten für unternehmenseigene Zwecke;

7. die Prüfung der durch organisatorische und prozedurale Erfordernisse verursachten Kosten sowie der durch mangelnde Effizienz verursachten Transaktionskosten;

8. die Bestimmung von geeigneten Maßnahmen zur Sicherstellung einer möglichst effizienten Zusammenarbeit zwischen Unternehmen und Behörden sowohl national als auch grenzüberschreitend etwa durch die Einrichtung sog. “Single Points of Contact“ (SPoC), durch Personalschulungen oder standardisierte Anforderungen;

---

5 Bei Data Preservation werden die Daten einer bestimmten verdächtigen Person ab einem bestimmten Zeitpunkt gespeichert (sog. „Data Freeze“).

9. der Eingriff in das Grundrecht des Fernmeldegeheimnisses und die Auswirkungen auf die Akzeptanz und das Vertrauen der Bürger bei der Nutzung von Telekommunikationsdiensten als Voraussetzung für die Entwicklung der Informationsgesellschaft.

In den Diskussionen um den Beschlussentwurf wird deutlich, dass eine Verpflichtung zur Vorratsdatenspeicherung in den wichtigsten TK-Märkten i.d.R. nicht implementiert ist und es zeigt sich, dass der Umfang der EU-weit geplanten Vorratsdatenspeicherung weit über das hinaus geht, was bislang durch Telekommunikationsunternehmen für Unternehmenszwecke (insbesondere für Zwecke der Rechnungserstellung) gespeichert wird. Dies hat u.a. zur Folge, dass die intendierte Vorratsspeicherung von Telekommunikationsdaten für Strafverfolgungszwecke über einen Zeitraum von bis zu drei Jahren nicht nur die Telekommunikationsindustrie mit hohen Kosten belasten würde, sondern den Unternehmen in einzelnen Mitgliedstaaten auch Nachteile im europäischen Wettbewerb bescheren könnte, falls keine einheitlichen Regelungen für die Erstattung der erforderlichen Aufwendungen geschaffen würden.

Vor diesem Hintergrund hat WIK-Consult im Auftrag von BITKOM - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. im Zeitraum von August bis September 2004 die folgenden Aspekte untersucht:

- Gesetzliche Grundlagen und Praxis der Vorratsdatenspeicherung, Data Preservation und Datenspeicherung für unternehmenseigene Zwecke,
- Wirksamkeit bestehender Regelungen und Effektivität des Zugriffs der berechtigten Stellen (Law Enforcement Agencies – LEAs) auf Vorratsdaten,
- Kostenentschädigungsregelungen für Vorratsdatenspeicherung.

Wichtigste Ergebnisse der Studie

Gesetzliche Grundlagen und Praxis von Vorratsdatenspeicherung, Data Preservation und Datenspeicherung für Zwecke der Unternehmen

- Der Vergleich der verschiedenen Regelungen in den wichtigsten TK-Märkten der EU und in den USA zeigt insgesamt, dass eine verpflichtende Vorratsdatenspeicherung für Zwecke der Strafverfolgung und nationalen Sicherheit wenig verbreitet ist. Eine Verpflichtung zur Speicherung „sämtlicher“ Verkehrsdaten, wie sie der EU-Rahmenbeschlussentwurf vorsieht, findet sich in keinem der untersuchten Länder.
  Die USA verzichten gänzlich auf eine Vorratsdatenspeicherung, da den nationalen Behörden eine fallbezogene Datenspeicherung (Data Preservation) ausreichend erscheint. Die Vergleichsländer UK, Schweden oder Österreich verfügen über keine gesetzlichen Verpflichtungen zur Vorratsdatenspeicherung. In UK basiert die Vorratsdatenspeicherung seit 2001 auf einer freiwilligen Vereinba-

rung, nach der die Unternehmen Daten, die diese bereits zu unternehmenseigenen Zwecken speichern, für einen längeren Zeitraum (je nach Datentyp zwischen 4 Tagen und 12 Monaten) speichern sollen. Die Niederlande haben ausschließlich für sog. call records im Bereich der Prepaid-Karten im Mobilfunk eine Speicherverpflichtung von 3 Monaten erlassen. In Spanien wurde in 2002 zwar ein entsprechendes Gesetz verabschiedet, eine Verordnung, durch die die darin enthaltenen Vorschriften erst wirksam würden, fehlt jedoch bis heute. In Frankreich (2001) existieren gesetzliche Rahmenregelungen für eine Speicherung für die Dauer von einem Jahr. Eine diese Regelung umsetzende Verordnung, die den Umfang der zu speichernden Datentypen und die Kostenentschädigung regeln soll, wird zurzeit kontrovers diskutiert. In Italien ist seit 2003 ein Gesetz in Kraft, wonach Unternehmen Verkehrsdaten für einen Zeitraum von 2 Jahren speichern müssen. Die zu speichernden Datentypen wurden jedoch bisher nicht festgelegt. Die Verpflichtung bezieht sich derzeit auf den Bereich der Telefonie (fixed und mobile).

Gesetzliche Grundlagen und Praxis von Data Preservation

- Data Preservation ist in manchen Ländern als Alternative oder zusätzlich zu Vorratsdatenspeicherung eingeführt worden. Die USA verfügen über die umfassendste und detaillierteste Regelung in diesem Bereich und verstehen das Verfahren als Alternative zu Vorratsdatenspeicherung. Gesetzentwürfe zu Vorratsdatenspeicherung wurden in den letzten Jahren mehrfach durch den Kongress als zu weitgehend abgewiesen.
  In Frankreich ist eine gesetzliche Ermächtigungsgrundlage für die Einführung von Data Preservation in Kraft. Das Einfrieren der Daten kann auf Basis einer Anordnung für bis zu ein Jahr geschehen.
  Nach den jeweiligen Strafprozessordnungen ist auch in UK und Spanien Data Preservation möglich. In den Niederlanden ist im Rahmen der Ratifizierung der Cybercrime Convention ein entsprechendes Gesetz in Vorbereitung. Danach soll eine Anordnung für Data Freeze für 90 Tage erfolgen.

- Grundsätzlich ist anzumerken, dass ein Zugriff auf Verkehrsdaten in den untersuchten Ländern immer auch im Rahmen von Überwachungsmaßnahmen (Legal Interception) erfolgen kann, wobei die Daten in Echtzeit oder ggf. auch per Datenträger an die Strafverfolgungsbehörden übermittelt werden.

Gesetzliche Grundlagen und Praxis von Datenspeicherung für unternehmenseigene Zwecke

- Die Praxis der Datenspeicherung wird in den untersuchten Ländern von den sektorspezifischen Datenschutzregelungen bestimmt. Dies bedeutet, dass Daten nur zweckbezogen gespeichert werden, also z.B. für Billing-Zwecke und für die Bereitstellung der Dienste. Für Marketingzwecke gilt in den EU-Mitgliedsländern zumeist, dass das Einverständnis des Teilnehmers erforderlich

ist. Die Dauer der Speicherung der zweckbezogenen Daten wird prinzipiell aus Kostengründen so kurz wie möglich gehalten, d.h. sie ist faktisch auf wenige Monate beschränkt. Rechnungsdaten können bis zur Verjährung der Einspruchsfrist aufbewahrt werden; falls Einsprüche geltend gemacht werden, auch länger.

- In allen untersuchten Ländern - mit Ausnahme der USA und UK - können TK-Anbieter Daten nur unter eingeschränkten Bedingungen für eigene Zwecke (z.B. Billing, Marketing) speichern. Im Wesentlichen gelten in den EU-Ländern vergleichbare Regelungen entsprechend der EU-Rahmenrichtlinie 2002/58/EC zum Datenschutz. D.h., dass die Speicherfrist für Rechnungszwecke auf 6 Monate beschränkt ist und die Verwendung für Marketingzwecke nur unter bestimmten Bedingungen gestattet ist.

- In UK besitzen die TK-Anbieter relativ weitreichende Befugnisse in Bezug auf die Verwendung von Bestandsdaten für Direktwerbung. Hier gilt generell ein „opt-out" Prinzip, d.h., Teilnehmer müssen der Nutzung ihrer Daten für Direktwerbungszwecke widersprechen. Rechnungsdaten dürfen 6 Jahre bis zum Ende der Einspruchsfrist aufbewahrt werden. Im Vereinigten Königreich besteht somit eine Möglichkeit für die Unternehmen, Datensätze weit intensiver für eigene Zwecke auszuwerten, als dies in den übrigen Ländern der Fall ist. Somit dürfte die Kostenbelastung durch Regelungen zur Vorratsdatenspeicherung für Strafverfolgungszwecke erheblich geringer sein als z.B. für deutsche Unternehmen, die hier erst mit großem Aufwand entsprechende Investitionen und Vorkehrungen vornehmen müssen.

- In den USA sind im Privatsektor Datenschutzregelungen kaum vorhanden. Hier bleibt die Dauer der Speicherung von Bestands- und Verkehrsdaten der Entscheidung der Unternehmen überlassen.

Wirksamkeit bestehender Regelungen und Effektivität des Zugriffs der berechtigten Stellen (Law Enforcement Agencies) auf Vorratsdaten

- In den Ländern, in denen gesetzliche Regelungen zu Data Retention für Strafverfolgungszwecke existieren, erweisen sich nicht nur die spezifischen zusätzlichen Investitionen, sondern auch die Abwicklungs- und Durchführungsprozesse sowie Maßnahmen zur Sicherung der Daten als Kostentreiber für die Unternehmen. Auch die Anzahl der zur Abfrage berechtigten Stellen hat deutliche Auswirkungen auf die entstehenden Kosten.

- Als kritisch ist in diesem Zusammenhang auch zu bewerten, dass die TK-Anbieter zu ihrem eigenen Schutz prüfen müssen, ob sie die Daten an eine berechtigte Stelle weitergeben. Andernfalls laufen sie Gefahr, gegen Datenschutzbestimmungen oder gegen strafrechtliche Bestimmungen (Strafvereitelung oder Verletzen des Fernmeldegeheimnisses) zu verstoßen. Es hat sich gezeigt, dass

die Prozesse und Anfragen kaum formalisiert und standardisiert sind, was die Prüfung für die Unternehmen umso aufwändiger gestaltet. Ein SpoC, geschulte Behördenmitarbeiter, elektronische Übertragungsverfahren und standardisierte Abfrageformulare können in erheblichem Umfang dazu beitragen, sowohl für Unternehmen als auch für die Behörden Kosten zu senken und die Effektivität zu steigern.

- UK verfügt in diesem Zusammenhang über die detaillierteste Festlegung der Datenabfrageprozesse. Jede Behörde muss entsprechende Mitarbeiter schulen und einen SPoC festlegen. Nur ein entsprechend geschulter Accredited Officer (AO) ist zur Abfrage berechtigt. Die Schulungen werden zum Teil durch die TK-Unternehmen durchgeführt. Die Formalisierung der Anfragen trägt nach Angaben der befragten Experten sowohl auf Seiten der Behörden als auch der TK-Anbieter erheblich zu Rechtssicherheit und Prozesskosteneinsparungen bei. Auch in Frankreich sind entsprechende Prozesse geplant. Eine Arbeitsgruppe von ISP und spezialisierte Einheiten der Strafverfolgungsbehörden haben sich darauf verständigt, SPOCs zu etablieren sowie an der Vereinheitlichung der gerichtlichen Anordnungen zu arbeiten. Die TK-Industrie ist in das Training für LEA-Vertreter involviert. Einige ISP haben einen „Servicekatalog“ für die LEAs entworfen, in dem sie ihre technischen Spezifikationen darlegen und erläutern, welche Informationen sie nicht zur Verfügung stellen können.

- Die Daten sollen zumeist in der Form übergeben werden, in der sie den Unternehmen vorliegen. Faktisch ist nach Expertenaussagen mit der Übergabe dennoch ein erheblicher Aufwand bei der Extrahierung und Aufbereitung der Daten verbunden. Zum Teil muss gemeinsam vor Ort am Access-Point mit Vertretern der Behörden nach Daten recherchiert werden, was den Aufwand für beide Seiten deutlich nach oben treibt.

- Die Übermittlung der angeforderten Verkehrsdaten geschieht in der Regel nicht elektronisch. Die Abwicklung der Datenanfrage und –übergabe erfolgt häufig per Telefon oder Fax, ggf. auch per Datenträger. Dieser Medienbruch bei der Übertragung wird von den involvierten Stellen als unbefriedigend und aufwändig angesehen.

- Für die untersuchten Länder liegen keine systematischen Studien zur Wirksamkeit von Vorratsdatenspeicherung vor. Analysen von schwedischen TK-Anbietern zeigen jedoch, dass 85% der abgefragten Verkehrsdaten sich auf einen Zeitraum beziehen, der nicht länger als 3 Monate zurückliegt. 10% der angeforderten Daten nehmen auf einen Maximalzeitraum von einem halben Jahr Bezug. Auch in UK beziehen sich die Abfragen zu 80% auf Daten, die in den letzten 3 Monaten generiert wurden, obwohl den Sicherheitsbehörden bekannt ist, dass die Unternehmen Daten für eigene Zecke zumeist für 12 Monate vorhalten. Vor diesem Hintergrund erscheinen die in der Diskussion über Data Retention erhobenen Forderungen nach einer Speicherfrist von zwölf Monaten bis

zu drei Jahren insbesondere unter dem Gesichtspunkt der Verhältnismäßigkeit zwischen Aufwand und Nutzen als wenig praxisgerecht. Statistiken aus den Niederlanden und Österreich belegen, dass Verkehrsdaten grundsätzlich nur einen geringen Beitrag zur Strafverfolgung leisten. Von den Strafverfolgungsbehörden werden am häufigsten Bestandsdaten (Name, Adresse, Kennungen, etc.) abgefragt. Dies ist auch in Frankreich der Fall.

Kostenentschädigungsregelungen für Vorratsdatenspeicherung

- Kostenentschädigungsregelungen finden sich in beinahe allen untersuchten Ländern. In den Niederlanden schließen die TK-Anbieter jeweils Tarifverträge über Entschädigungssätze mit dem Justizministerium ab. Auch in UK und Frankreich existieren solche Tariflisten. In Schweden können Kosten für einzelne Datenabfragen den Behörden in Rechnung gestellt werden. Auch in den USA können die Unternehmen einzelfallbezogen ihre Kosten geltend machen. In Italien und Österreich wurden Gebührenverordnungen erlassen, die die Höhe der Entschädigungen festlegen, die dann jeweils im Einzelfall gegenüber der jeweiligen Behörde geltend gemacht werden können.

- Auch Investitionen werden teilweise bei den Entschädigungszahlungen berücksichtigt. In Italien bekommen die Unternehmen einen Anteil der Kapitalkosten erstattet, wenn sie zu einem bestimmten Zeitpunkt in die geforderte Technik investieren. In den USA und in UK existieren Fonds, aus denen Entschädigungen für Investitionen von TK-Anbietern gezahlt werden. Aus Sicht der befragten TK-Anbieter ist eine Erstattung zu fordern, die sowohl Kapital- als auch Betriebskosten umfassend berücksichtigt.

- Nach einem Urteil des Verfassungsgerichts vom 27.02.2003 ist in Österreich eine Entschädigungszahlung an die TK-Anbieter zu leisten. Am 1. September 2004 ist eine entsprechende Gebührenverordnung in Kraft getreten, die die TK-Anbieter für die operativen Kosten entschädigt, wenn sie eine sog. Rufdatenrückerfassung durchführen. Darüber hinaus werden die zuständigen Behörden mit den TK-Industrieverbänden demnächst über eine Entschädigungsregelung für Investitionen in Überwachungstechnik gesondert verhandeln. Auch in Frankreich hat im Jahr 2000 das Verfassungsgericht entschieden, dass der Staat zu Entschädigungszahlungen verpflichtet ist.

- Die Regel, wonach in manchen Ländern einzelfallbezogen mit den Behörden abgerechnet werden muss, führt nicht nur bei den TK-Anbietern, sondern auch bei den Behörden zu hohen Kosten für die Rechnungsstellung und -bearbeitung. Dies führt zum Teil sogar dazu, dass betroffene Unternehmen wegen des hohen Aufwandes auf eine Rechnungstellung gänzlich verzichten und dadurch Wettbewerbsnachteile erleiden. Die Einrichtung einer zentralen Abrechnungsstelle und eine Standardisierung der Prozesse wären daher aus Sicht aller TK-Anbieter dringend wünschenswert.

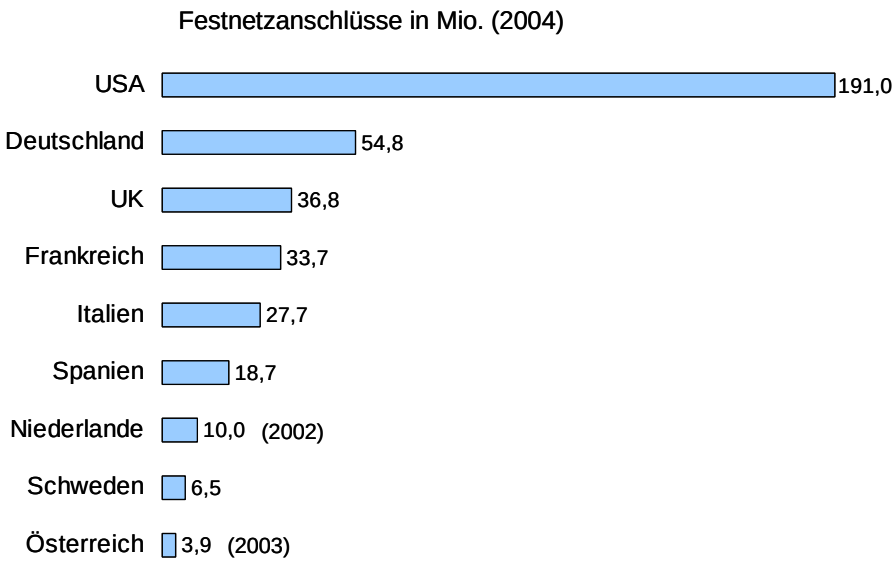
- Vorratsdatenspeicherung kann das Nutzerverhalten negativ beeinflussen, da ein Akzeptanz- und Vertrauensverlust der Bürger nicht ausgeschlossen werden kann. Eine vertrauliche Kommunikation ist jedoch eine wichtige Voraussetzung für die Nutzung innovativer Telekommunikationsdienste und damit für die Wachstumspotenziale der ITK-Industrie.

2 Marktüberblick

Die folgenden Abbildungen geben einen Überblick über die Anzahl der Anschlüsse im Bereich Festnetz, Mobilfunk und Internet in den in der Studie untersuchten Ländern.

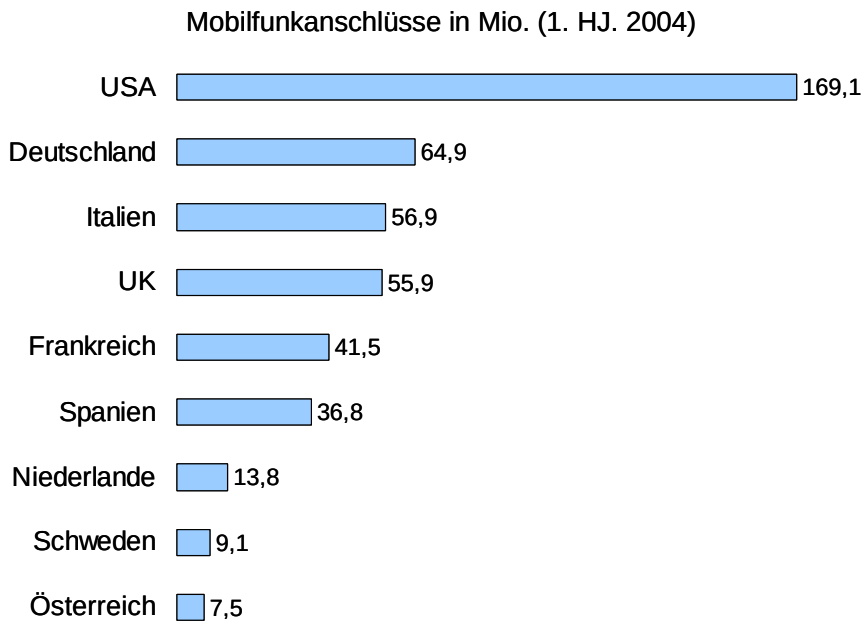
Es zeigt sich, dass Deutschland im Vergleich zu den übrigen europäischen Ländern in allen drei Bereichen über die höchsten Anschlusszahlen verfügt. Entsprechend ist davon auszugehen, dass in Deutschland weitaus mehr Bestandsdaten und Verkehrsdaten generiert werden, als in den Vergleichsmärkten.

Abbildung 2-1: Festnetzanschlüsse



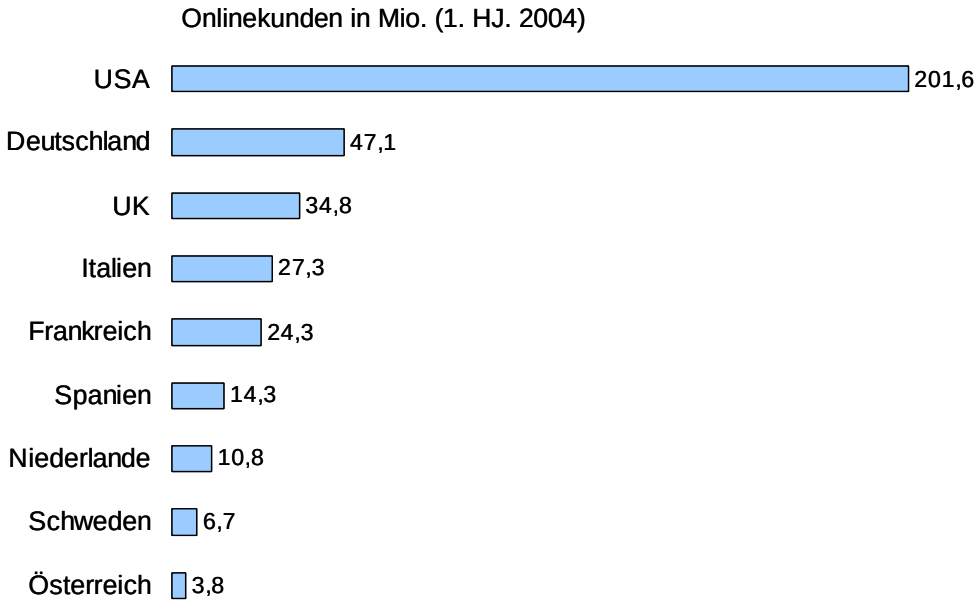
Quelle: EITO, CIA, Indexmuni.com

Abbildung 2-2: Mobilfunknutzer



Quelle: Mobile communications, CTIA

Abbildung 2-3: Internetnutzer



Quelle: Nielsen-Netratings, EITO, AIM

3 Frankreich

3.1 Gesetzliche Grundlagen[6]

3.1.1 Gesetzliche Grundlagen für Vorratsdatenspeicherung zum Zweck der Strafverfolgung

Die Vorratsdatenspeicherung der Verkehrsdaten von öffentlichen elektronischen Netzen, in Frankreich "conservation des données de connexion" genannt, wurde mit dem Gesetz zur Alltagssicherheit (Loi N°2001-1062 sur la Sécurité Quotidienne - LSQ) vom 15. November 2001 eingeführt.

Seither wird die Vorratsdatenspeicherung in Frankreich durch vier Gesetze geregelt:

- Loi N°2001-1062 sur la Sécurité Quotidienne (LSQ). Dieses Gesetz enthält Vorschriften zur Vorratsdatenspeicherung sowie zum Zugang der Regierung zu kryptografischen Schlüsseln.
- Loi N°2003-239 vom 18. März 2003 zur inneren Sicherheit.
- Loi N°2004-669 sur les communications électroniques (LCE) vom 9. Juli 2004, das die neue europäische Rahmenrichtlinie in französisches Recht umsetzt und mit einigen Modifikationen des LSQ einhergeht.
- Loi N°2004-801 vom 6. August 2004 zum Schutz der verarbeiteten Daten von natürlichen Personen. Dieses neue Datenschutzgesetz modifiziert das Gesetz N°78-17 vom 6. Januar 1978 zu Informationstechnologie, Datenspeicherung und Bürgerrechten.

Seit der kürzlich erfolgten Umsetzung des neuen europäischen Regulierungsrahmens in französisches Recht durch das Gesetz N°2004-669 vom 9. Juli 2004, das auch einige Änderungen zum LSQ und zum Gesetz N°2003-239 mit sich brachte, werden Verkehrsdaten im Code für Post und elektronische Kommunikation (P&EC)[7] erstmals erwähnt. Zuvor wurden diese Daten als „technische Daten" bezeichnet.[8]

Nach den Bestimmungen zur Vorratsdatenspeicherung von Verkehrsdaten in Artikel L34.1 P&EC, müssen grundsätzlich alle Verkehrsdaten gelöscht oder anonymisiert

---

6 Alle im Folgenden zitierten Gesetze sind unter www.legifrance.gouv.fr. verfügbar.

7 Gemeint sind mit Verkehrsdaten Verbindungs- und Standortdaten. Das Gesetz für Post und elektronische Kommunikation bildet den Kern der sektorspezifischen Regulierung bei Post und Elektronischer Kommunikation in Frankreich. Es ist in etwa vergleichbar mit dem deutschen TKG und kann durch Gesetz (wie im Falle des LCE) oder durch Dekret geändert werden.

8 S. Artikel 29 Gesetz N°2001-1062. Dieser Artikel setzt insbesondere Artikel 6 der Direktive 97/66/EC um.

werden. Diese Vorschrift gilt für alle Anbieter elektronischer Kommunikationsdienste, einschließlich ISP. Zu dieser Vorschrift existieren Ausnahmen, darunter die Verpflichtung zur Datenspeicherung für Zwecke der Strafverfolgung und Gewährleistung der nationalen Sicherheit

Bevor der Artikel L34.1 P&EC tatsächlich in Kraft treten kann, bedarf es eines Umsetzungsdekrets des französische Staatsrats (Conseil d'Etat). Ein solches Dekret soll auf Basis der Stellungnahme der französischen Datenschutzbehörde "Commission Nationale de l´Informatique et des Libertés" entworfen werden und soll enthalten:

- die Datenkategorien, die in die Vorratspeicherung einbezogen werden müssen, bzw. die innerhalb der Vorschriften des Artikels L34.1 (V) P&EC gespeichert werden dürfen,
- die Dauer der Vorratsdatenspeicherung, in Abhängigkeit vom Geschäftsfeld des Betreibers und der Art der Kommunikationsdienste sowie
- die Kostenentschädigungsregelungen im Zusammenhang mit den vorgeschriebenen Vorratsdatenspeicherungen.

Dieses Dekret wird bereits seit dem Gesetz zur Alltagssicherheit von 2001 erwartet. Die Verabschiedung dieses Dekrets wurde zum einen verzögert durch die späte Umsetzung des neuen europäischen TK-Regulierungsrahmens in französisches Recht im Juli 2004 und zum anderen durch die Änderung des Gesetzes N°78-17 im August 2004. Gegenwärtig steht ein Entwurf dieses Umsetzungsdekrets zur Diskussion.

In der Zwischenzeit speichern die Betreiber alle Daten, die ihnen relevant erscheinen und deren Speicherung innerhalb der Vorschriften des Artikels L34.1 (V) P&EC sowie des Gesetzes N°78-17 vom 6. Januar 1978 zu Informationstechnologie, Datenspeicherung und Bürgerrechten möglich ist.

Bis heute existieren noch keine konkreten Bestimmungen darüber, wie die Vorratsdatenspeicherung der Verkehrsdaten bei den Betreibern elektronischer Kommunikationsnetze und –dienste technisch durchzuführen ist.

3.1.2 Gesetzliche Grundlagen für anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung

Die Regelungen zur anlassbezogenen Datenspeicherung finden sich in Artikel 60-2 des Strafgesetzbuches, eingeführt durch Gesetz N°2003-239 sowie modifiziert durch Gesetz N°2004-204 vom 9. März 2004 zur Anpassung der Justiz an die Entwicklung der Kriminalität, durch Gesetz N°2004-575 vom 21. Juni 2004 zum Vertrauen in der digitalen Wirtschaft sowie durch Gesetz N°2004-801.

Ein Dekret des Staatsrates das die Stellungsnahme der “Commission Nationale de l´Informatique et des Libertés” berücksichtigt, soll die konkreten Modalitäten bezüglich Ermittlungsmethoden, Übermittlung und notwendigen Verarbeitung der Daten festlegen.

3.1.3 Gesetzliche Grundlagen der Datenspeicherung für unternehmenseigene Zwecke

Parallel zur Vorratsdatenspeicherung aus Strafverfolgungsgründen, wird auch die Datenspeicherung für andere Zwecke durch das LSQ und den Artikel L34.1 P&EC geregelt. Es bestehen zwei weitere Ausnahmen von der grundsätzlichen Verpflichtung zur Löschung oder Anonymisierung der Verkehrsdaten. Betreiber dürfen bestimmte, durch ein Dekret des Staatsrats festzulegende Kategorien von Verkehrsdaten speichern und zwar

- zur Durchführung der Abrechnung ist eine Speicherung bis zum Ende der Einspruchsfrist erforderlich (ein Jahr),[9]
- mit Einwilligung der Teilnehmer ist eine Speicherung für Marketingzwecke möglich,
- außerdem dürfen zur Gewährleistung der Netzsicherheit Daten gespeichert werden.

Diese Datenspeicherung und –verarbeitung darf nur innerhalb der Grenzen des Artikels L34.1 (V) P&EC sowie im Einklang mit den Vorschriften des Datenschutzgesetzes N°78-17 durchgeführt werden.

3.2 Praxis der Vorratsdatenspeicherung

3.2.1 Art, Umfang und Dauer

Artikel L34.1 (V) P&EC beschreibt die Datenkategorien, die durch die Betreiber gespeichert werden dürfen. Die gespeicherten Daten sollen ausschließlich der Identifikation der Nutzer der Dienste des jeweiligen Betreibers dienen sowie die technischen Charakteristika des Kommunikationsdienstes und die Lokalisierungsdaten des Endgerätes enthalten. Die Speicherung von Daten, die Rückschlüsse auf die übermittelten Inhalte der Kommunikation ermöglichen, ist nicht zulässig.

Gemäß Artikel 29 LSQ und Artikel L34.1 P&EC müssen die Betreiber die für die Strafverfolgung gespeicherten Daten maximal ein Jahr lang aufbewahren. Das oben er-

9 Diese Frist bezieht sich auf L126 des P&EC Code und betrifft den Public Operator France Telecom. Die Einspruchsfrist beträgt ein Jahr.

wähnte Dekret zur Einführung von Artikel L34.1 wird voraussichtlich weitere Konkretisierungen der prinzipiellen Vorschriften mit sich bringen und die Aufbewahrungsperiode für jede Datenkategorie festlegen.

Nach Auskunft von Betreiberverbänden müssen entsprechend dem jetzt diskutierten Verordnungsentwurf künftig folgende Informationen für maximal 365 Tage gespeichert werden:

- Name und Adresse des Teilnehmers,
- E-Mail-Adresse und Passwörter,
- Datum des Vertragsbeginns und Zahlungsweise,
- Nummernportierung,
- Dauer, Datum, Anfangs- und Endzeitpunkt des Kommunikationsdienstes,
- Nummer des Anrufers, angerufene Nummer,
- genutzter Dienst,
- Art des Kommunikationsdienstes,
- IP-Adresse,
- IP-Adressen von Sender und Empfänger,
- Datum und Zeit der Verbindung zu E-Mail-Konten.

Die Mitglieder des französischen ISP Verbandes (AFA)[10] haben sich als Reaktion auf gerichtliche Anordnungen in Bezug auf Bestands- und Verkehrsdatenabfragen bereits im Oktober 1998 auf eine gemeinsame Liste von Daten geeinigt, die sie als Minimum freiwillig speichern (vgl. Tabelle 3-1).

10 AFA wurde 1997 gegründet. Die Mitgliederunternehmen sind Internet Technical Provider auf dem Gebiet der IP-Netze, des professionellen und privaten Hosting sowie des professionellen und privaten Netzzugangs. Die Mitglieder im Einzelnen sind: 6 sens (Bouygues Telecom Group), AOL France, Aricia, Cario, Club-Internet, COLT France, InterPC, Magic On Line, MCI, Mobius, MSN France, NC Numéricable, neuf Telecom, Noos, Outremer Telecom, SFR Cegetel, Tiscali France, UPC France, Wanadoo and Yahoo! France. Vgl. www.afa-france.com.

Tabelle 3-1: AFA Verhaltenskodex

Betreibertypus	gespeicherte Verkehrsdaten	Speicherungsperiode bei AFA-Mitgliedern
Internet Zugangs-provider	PSTN Internet Zugangsdaten ("access logs"): • Nutzerkennung • zugewiesene IP-Adresse • genaues Datum und Zeit des Zugangs • genaues Datum und Zeit des Verbindungsende	durchschnittlich 3 Monate maximal 6 Monate
Betreiber von Cache Servern	Verbindungsdaten zu den Caches ("web proxy logs"): • IP-Adresse des Internetnutzers • Name des vom Nutzer angesteuerten Servers • angefordertes Dokument • genaues Datum und Zeit	durchschnittlich 3 bis 5 Tage
Web Hosting Provider	Verbindungsdaten von angebotenen Inhalten ("FTP logs"): • Nutzer-Login • die vom Zugangsprovider zugewiesene IP-Adresse des Nutzers • genaues Datum und Zeit der Verbindung • genaues Datum und Zeit des Verbindungsende	3 Monate

Quelle: http://usages.afa-france.com/#conservation

Nach Auskunft von AFA werden in der überwiegenden Mehrzahl der Abfragen durch die Strafverfolgungsbehörden Informationen zu den Teilnehmern und deren Zugangsdaten benötigt (vgl. Tabelle 3-2).

Tabelle 3-2: Häufigste Abfragen durch Strafverfolgungsbehörden bei AFA-Mitgliedsunternehmen

1.	Tracing eines Nutzers mit bestimmter Kreditkarten- oder Bankkontonummer
2.	Identifizierung einer E-Mail-Adresse
3.	Tracing eines Nutzers auf Basis des Namens und/oder der Adresse und/oder der Telefonnummer und/oder der E-Mail-Adresse
4.	Identifizierung eines Nutzers durch eine IP-Adresse in Verbindung mit Datum und Zeit
5.	Identifizierung eines Nutzers, der Zugang über einen Proxy-Server hatte
6.	Tracing von betrügerischen Aktivitäten ausgehend von einem bestimmten Nutzerkonto
7.	Identifizierung einer persönlichen Website oder Gruppe
8.	Abfangen von E-Mails
9.	Protokollierung des Zugangsverhaltens (ohne Auflistung der besuchten Websites)
10.	Zusammenstellung aller Bestandsdaten zu einem bestimmten Nutzer

Quelle: AFA

Was die Zwischenspeicherung, die Reaktionszeit auf behördliche Anfragen sowie die Übermittlungswege betrifft, gibt es in Frankreich derzeit noch keine gesetzlichen oder freiwilligen Regelungen.

Die Anzahl und Häufigkeit der strafbehördlichen Anfragen variiert zwischen den Betreibern. Die Mitglieder des Multiservice-Verbandes AFORM[11] bearbeiten im Durchschnitt eine Anordnung pro Monat. AFA-Mitgliedsunternehmen bearbeiten je nach Größe des ISP und seiner Kundenstruktur (z.B. Privat- oder Geschäftskunden) zwischen 0 und 2.000 Anfragen pro Jahr im Zusammenhang mit ihren Internetdiensten. Alle AFA-Mitgliedsunternehmen zusammen erhielten während der letzten 12 Monate insgesamt rund 10.000 Anordnungen.

11 AFORM (Association Française des Opérateurs Multiservices) ist der Verband der französischen Multiservice-Anbieter und insbesondere der wichtigsten Breitbandkabelunternehmen: France Télécom Câble, Groupe Reflex, NC Numéricâble, Noos, UPC France, Valvision, Vialis.

3.2.2 Kreis der Verpflichteten

Alle Anbieter von elektronischen Kommunikationsdiensten unterliegen in Frankreich der Verpflichtung zur Vorratsdatenspeicherung nach Artikel L34.1 P&EC. Ausnahmen hiervon sind nicht vorgesehen.

Verstöße gegen die Vorschriften des Artikels L34.1 of P&EC können nach Artikel L39-3 P&EC mit einjähriger Haftstrafe und Geldstrafe in Höhe von 75.000 Euro belegt werden.

Für den Fall, dass der Betreiber die mit der Vorratsdatenspeicherung und den Anordnungen verbundenen Dienstleistungen an Dritte vergibt, bestehen keine speziellen gesetzlichen Einschränkungen oder Auflagen.

3.2.3 Relevanz für Strafverfolgung und nationale Sicherheit

Nach den Erkenntnissen der AFA, welche der Verband in Diskussionen mit den Strafverfolgungsbehörden gewonnen hat, führt die gegenwärtige Vorratsdatenspeicherung der ISP dazu, dass Täter in der überwiegenden Mehrzahl der Fälle durch die Behörden ermittelt und verfolgt werden können.

3.3 Praxis der anlassbezogenen Datenspeicherung

In Artikel 60.2 des französischen Strafgesetzbuches ist geregelt, dass ein Mitarbeiter der Kriminalpolizei, der im Auftrag der Staatsanwaltschaft und mit gerichtlichem Beschluss ermittelt, die Betreiber elektronischer Kommunikationsdienste anweisen kann, unverzüglich alle Maßnahmen zu treffen, um die Inhalte der Kommunikationsdienste, die durch den Betreiber an verdächtige Nutzer übermittelt werden, für bis zu ein Jahr zu speichern.

Eine grundlose Weigerung des Betreibers, diese Anordnung zu befolgen, wird mit einer Geldstrafe in Höhe von 3.750 Euro belegt.

3.4 Praxis der Datenspeicherung für unternehmenseigene Zwecke

Die Betreiber elektronischer Kommunikationsdienste dürfen Datenspeicherungen aus folgenden Gründen betreiben:

- für das Billing, bis zum Ende der Rechnungsperiode und Einspruchsfrist (1 Jahr),
- für eigene Marketingzwecke, soweit die Teilnehmer ausdrücklich ihre Zustimmung gegeben haben. Der Zeitraum darf das Ende der Vertragsbeziehung nicht überdauern,
- sowie zur Gewährleistung der Netzsicherheit.

Solange das Implementierungsdekret für Artikel L34.1 P&EC des Staatsrates nicht verabschiedet ist, variieren in der Praxis die Kategorien und Zeiträume der gespeicherten Daten zwischen den Betreibern; abhängig von Größe, Diensteportfolio und Netzarchitektur.

Nach Auskunft der kontaktierten Verbände werden heute grundsätzlich folgende Daten durch die Betreiber für deren Zwecke gespeichert:

- Maximal 365 Tage: Teilnehmername und Adresse, E-Mail-Adresse und Passwörter, Daten zum Beginn einer Vertragsbeziehung und vereinbarter Zahlungsweg, Nummernportierung, Tarif, gebuchte Dienste und Art der Kommunikation.
- Maximal 90 Tage: angerufene Nummern, Nummern der Anrufer (nur aus Gründen der Netzsicherheit), IP-Adresse der Session, IP-Adresse des Senders und Empfängers, Datum und Zeit des Zugangs des Nutzers zum E-Mail-Konto.

Darüber hinaus werten die AFA-Mitglieder die entsprechend ihrem Verhaltenskodex derzeit freiwillig gespeicherten Daten (vgl. Tabelle 3-1) aus, um die Dimensionierung ihrer technischen Infrastruktur entsprechend der Nutzerbedürfnisse zu optimieren und um das Billing auf die Nutzungsdauer hin auszurichten.

3.5 Ausgestaltung des Zugriffs der berechtigten Stellen

Folgende staatliche Stellen dürfen Verkehrsdaten bei den Betreibern elektronischer Kommunikationsdienste abfragen:

- Justizbehörden (Artikel 29.II LSQ und Artikel L34.1 P&EC): Polizei und Gendarmerie, während ihrer Ermittlungen,
- Zollbehörden (Artikel 62.I des 2001 ergänzten Finanzgesetzes, das Artikel 65 des Zollgesetzbuches modifiziert): Die Zollbeamten müssen mindestens den Status eines Inspektors oder Offiziers besitzen oder mit Zollerhebungsaufgaben betraut sein,
- Verwaltungsbehörden (Artikel 62.II des 2001 ergänzten Finanzgesetzes, das Artikel L83 des Steuererhebungsgesetzbuches modifiziert),
- Ermittler der französischen Börsenaufsicht (Artikel 62.III des 2001 ergänzten Finanzgesetzes, das Artikel L621.10 des Geld- und Finanzgesetzbuches modifiziert).

Darüber hinaus ist der Zugang zu den kompletten, nichtbereinigten und aktuellen Teilnehmer- und Nutzerverzeichnissen nach Artikel L35.5 P&EC gestatten für

- Justizbehörden: Polizei und Gendarmerie, während ihrer Ermittlungen,
- Notrufdienste: Feuerwehr und medizinische Rettungsdienste, soweit sie Rettungsaktionen durchführen.

Im Zusammenhang mit Strafermittlungen wird zum Informationszugriff eine Anordnung benötigt. Diese wird, je nach Art der Anfrage und Untersuchung, von Staatsanwälten oder Richtern unterzeichnet.

Im Zusammenhang mit Verwaltungsvorgängen besteht das Recht zur Datenabfrage (das so genannte „droit de communication“) kraft der einschlägigen Verwaltungsgesetze.

3.6 Kostenentschädigung

3.6.1 Rechtliche Grundlagen

Es wird erwartet, dass das Umsetzungsdekret des Staatsrats für Artikel L34.1-I P&EC die Bestimmungen zur Entschädigung jener Kosten festlegt, die nachweis- und zurechenbar durch staatlich angeordnete Maßnahmen entstanden sind. In der Zwischenzeit gelten weiterhin die Bestimmungen des Artikels R.92.9 des Strafgesetzbuchs.

3.6.2 Abwicklungsprozess

Artikel R.92.9 des Strafgesetzbuchs legt fest, dass die Staatskasse für Ausgaben aufkommt, die auf Grund von gerichtlichen Anordnungen entstehen. Dies gilt auch für Kosten von technischen Arbeiten im Rahmen von Strafermittlungsverfahren. In der Praxis werden die Kosten der behördlichen Datenabfragen vierteljährlich auf Einzelfallbasis gegen Vorlage von Rechnungen und sonstiger schriftlicher Kostennachweise erstattet.

Dieses Kostenentschädigungssystem ist so komplex ausgestaltet, dass die Mehrheit der ISP auf die Rechnungstellung verzichtet.

Die Verbände erwarten, dass das kommende Umsetzungsdekret von Artikel L34.1-I P&EC dem französischen Staat vorschreibt, die Kosten der Netzaufrüstungen für die gesetzlich vorgeschriebene Vorratsdatenspeicherung zu übernehmen.

Einen wichtigen Einfluss dürfte in diesem Zusammenhang eine Entscheidung des französischen Verfassungsgerichts (N° 2000-441 DC) vom Dezember 2000 zu Echtzeit-Überwachungsmaßnahmen haben. In dieser Entscheidung wird darauf verwiesen, dass der Staat die Kosten tragen muss, die bei den Betreibern durch Anordnungen entstehen.

3.6.3 Höhe der Kostenentschädigung

Hierüber liegen keine öffentlichen Informationen vor.

3.7 Besonderheiten und aktuelle Entwicklungen

Der im Entwurf des Artikels L34.1 P&EC enthaltene Kostenentschädigungsmechanismus wird von den Betreiberverbänden stark kritisiert, da dieser nur eine fallweise Entschädigung für operative Kosten vorsieht. Die Kosten für Investitionen bei den Betreibern, um die Voraussetzungen für eine Datensammlung und längere Datenspeicherung sowie eine schnelle Datenabfrage und Lieferung an die Ermittlungsbehörden zu schaffen, werden danach nicht entschädigt.

AFA schätzt, dass sich dieses Entschädigungsregime besonders nachteilig auf die kleinen ISP und auf B2B-Provider auswirkt, da bei ihnen die Anzahl der behördlichen Datenabfragen sehr gering, wenn nicht sogar null ist. Hingegen hängen die durch die verpflichtende Vorratsdatenspeicherung verursachten Kosten von vielfältigen Faktoren ab, wie z.B. der Netzbeschaffenheit des ISP, der Anzahl der Teilnehmer, dem angebotenen Dienst, der Dauer und dem Umfang der Vorratsdatenspeicherung und ob die Daten bestimmten Qualitätskriterien entsprechen bzw. in bestimmter Weise aufbereitet weitergeleitet werden müssen.

Ähnlich wie in UK sind auch in Frankreich die Behörden und Provider bestrebt, Single Point of Contacts zu etablieren und die Abwicklung der Anordnungen zu standardisieren. Beide Seiten erwarten dadurch erhebliche Kosteneinsparungen. Die Unternehmen sind außerdem an der Schulung der Behördenmitarbeiter maßgeblich beteiligt.

4 Italien

4.1 Gesetzliche Grundlagen

4.1.1 Gesetzliche Grundlagen für Vorratsdatenspeicherung zum Zweck der Strafverfolgung

Die grundsätzliche Verpflichtung der TK-Anbieter und Betreiber von TK-Anlagen, die Strafverfolgungsbehörden bei der Überwachung zu unterstützen, ist in einem Dekret des Präsidenten aus dem Jahr 1997, mit dem die von der EU geforderten einheitlichen Rahmenbedingungen im Telekommunikationssektor in die italienische Gesetzgebung implementiert werden, festgelegt:

- Decreto del presidente della repubblica del 19 settembre 1997, n. 318: Regolamento per l'attuazione di direttive comunitarie nel settore delle telecomunicazioni.

In Art. 7, Abs. 13 befindet sich die Regelung, dass die Kooperation mit den Strafverfolgungsbehörden für Telekommunikationsnetzbetreiber und Service Provider verpflichtend ist. Diese Regelung bezieht sich nicht nur auf die Überwachung von Echtzeit-Kommunikation, sondern auch auf die Weitergabe von Bestandsdaten und Verkehrsdaten (Verbindungs- und Standortdaten).

Zum 1. Januar 2004 ist ein neues Datenschutz-Gesetz (Decreto legislativo n. 196 del 30 giugno 2003, genannt "Codice in materia di protezione dei dati personali")[12] in Kraft getreten, das mit dem Ziel der Harmonisierung und Vereinfachung alle im Bereich des Datenschutz geltenden gesetzlichen Vorschriften zusammenführt, die seit 1996 erlassen wurden. Das neue Datenschutzgesetz setzt die EU-Direktive 2002/58/EC um:

- Decreto legislativo n. 196 del 30 giugno 2003, genannt "Codice in materia di protezione dei dati personali" (Datenschutzgesetz).

Der Vorläufer des aktuellen Datenschutzgesetzes wurde im Jahr 1996 nach etwa 20jähriger Debatte über die Thematik erlassen (Legge 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali").[13] In diesem Gesetz wurde in Artikel 30 auch die Einrichtung der Datenschutzbehörde „Garante per la protezione dei dati personali" („Garante") beschlossen. Die Garante hat seit ihrem Bestehen zahlreiche weitere Richtlinien und Vorschriften zum Datenschutz erlassen.

---

12 In englischer Sprache Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003, abrufbar unter http://www.garanteprivacy.it/garante/document?ID=727068.

13 Veröffentlicht in Gazzetta Ufficiale n. 5 dell'8 gennaio 1997 - Supplemento Ordinario n. 3, abrufbar unter http://www.parlamento.it/parlam/leggi/96675l.htm.

Das neue Datenschutzgesetz bezieht sich im ersten Teil auf grundlegende Datenschutzprinzipien. Der zweite Teil des Gesetzes enthält sektorspezifische Vorschriften (darunter Telekommunikation) und der dritte Teil regelt Strafmaßnahmen und Rechtsmittel.

Der für Telekommunikation relevante Abschnitt des Gesetzes (Chapter I – Electronic Communication Services) setzt die Anforderungen der EU-Datenschutzrichtlinie um.

Der Umgang mit Telefonverkehrsdaten, die für die Strafverfolgung benötigt werden, ist in Abschnitt 132 des Datenschutzgesetzes geregelt. Für diesen Abschnitt wurden nach Inkrafttreten des Gesetzes Ende 2003 im sog. „Decreto sulla data retention" Veränderungen beschlossen (Decreto-legge 354/03, 24 dicembre 2003, Disposizioni urgenti per il funzionamento dei tribunali delle acque, nonche' interventi per l'amministrazione della giustizia), nachdem es massive Kritik seitens der Netzbetreiber gegeben hatte[14].

4.1.2 Gesetzliche Grundlagen für anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung

Über anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung bestehen keine gesetzlichen Regelungen in Italien. Data Preservation erscheint aus Sicht der Behörden vor allem deshalb nicht erforderlich, weil die Befugnisse zur Echtzeit-Überwachung sowie die neuen Regelungen zur Vorratsdatenspeicherung den Erfordernissen der Strafverfolgung und nationalen Sicherheit entsprechen.

4.1.3 Gesetzliche Grundlagen der Datenspeicherung für unternehmenseigene Zwecke

Der Umgang der TK- und Service Provider mit Verkehrsdaten für eigene Zwecke ist im Datenschutzgesetz in Abschnitt 123 geregelt. Die Regelungen beziehen sich insbesondere auf die Nutzung gespeicherter Daten für Abrechnung und Marketingmaßnahmen.

4.2 Praxis der Vorratsdatenspeicherung

4.2.1 Art, Umfang und Dauer

Grundsätzlich haben Netzbetreiber Verkehrsdaten, d.h. Verbindungs- und Standortdaten, im Hinblick auf deren Verwendung für die Strafverfolgung 24 Monate zu speichern

---

14 Vgl. z.B. Grande Fratello, consegnata la petizione, in: Punto Informatico, 22.01.2004, http://punto-informatico.it/p.asp?i=46628

(Datenschutzgesetz, Abschnitt 132, Abs. 1).[15] Zusätzlich zu den 2 Jahren ist eine Verlängerung um 2 Jahre bei Katalogstraftaten in besonders begründeten Fällen (z.B. organisiertes Verbrechen) vorgesehen, die in Abschnitt 407 (2) Buchst. a des Strafgesetzbuches „Criminal Procedure Code“ geregelt sind.

In Italien ist die Art der zu speichernden Daten nicht konkret festgelegt. Die genaue Ausgestaltung in der Praxis ist daher interpretationsbedürftig und wird kontrovers diskutiert.[16] Während zunächst die Speicherung von Daten sowohl im Zusammenhang mit Telefonie als auch mit dem Internet vorgesehen war, wird derzeit nur von einer Speicherung der Telefonverkehrsdaten (fix und mobil) ausgegangen. Üblicherweise werden alle Daten, die auch im Zusammenhang mit der Übertragung von Telefonverkehr und der Abrechnung der Dienste entstehen, gespeichert (darunter z.B. Datum, Zeit). Es ist jedoch nicht auszuschließen, dass die Vorratsdatenspeicherung künftig auch auf den Internetverkehr ausgeweitet wird.

Da keine verbindlichen Regelungen vorliegen, ist es in der Praxis der Entscheidung jedes Unternehmens überlassen, welche Festnetz- und Mobilfunkdaten gespeichert werden. Nach Experteneinschätzungen ist von einer umfassenden Speicherung aller relevanten Datensätze auszugehen, da die Bereitschaft zur Kooperation bei den Telefonieanbietern, im Gegensatz zu den ISP, sehr groß ist. Der Grund dafür ist darin zu suchen, dass die erforderlichen Daten im Telefoniebereich eher ohnehin vorhanden sind als im Internet-Bereich.

4.2.2 Kreis der Verpflichteten

Die Datenvorratsspeicherung gilt gemäß Artikel 121 des Datenschutzgesetzes generell für alle Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste, die über öffentliche Kommunikationsnetze übertragen werden. Im Gesetz sind keine Ausnahmen, z.B. für kleine Netzbetreiber, vorgesehen.

Eine allgemeine Verpflichtung für alle Netzbetreiber und Service Provider zur Überwachbarkeit der Telekommunikation wurde bereits im Decreto del presidente della repubblica del 19 settembre 1997, n. 318 festgelegt. Diese bestimmt, dass alle Netzbetreiber und Service Provider die technischen und organisatorischen Voraussetzungen zur Kooperation mit den Strafverfolgungsbehörden zu schaffen haben. Dabei differenzieren die Vorschriften zwischen Anbietern von drahtgebundenen, mobilen und satellitengestützten Diensten, Long-Distance-Calls und International Calls.

---

15 Zunächst war dieser Zeitraum auf 30 Monate festgelegt worden, wurde jedoch nach massiven Protesten der Unternehmen auf 24 Monate verkürzt.

16 Vgl. hierzu Andrea Monti: Dati del traffico: chi-conserva-cosa?, in: Interlex n. ro 276 del 05-01-04, abrufbar unter http://www.ictlaw.net.

4.2.3 Relevanz für Strafverfolgung und nationale Sicherheit

Es liegen keine Erkenntnisse in Italien zur Relevanz von Vorratsdatenspeicherung vor.

4.3 Praxis der anlassbezogenen Datenspeicherung

In Italien gibt es keine gesetzlichen Regelungen und daher auch keine Praxis des Data Preservation.

4.4 Praxis der Datenspeicherung für unternehmenseigene Zwecke

Die in Artikel 123 des Datenschutzgesetzes festgelegten Bestimmungen zur unternehmensinternen Nutzung von Verkehrsdaten sehen grundsätzlich vor, dass alle Daten gelöscht werden sobald sie nicht mehr für die Übertragung der Kommunikation benötigt werden.

Für bestimmte unternehmensinterne Zwecke gelten die folgenden Ausnahmen:

Das Gesetz sieht vor, dass Verkehrsdaten, die im Rahmen der Billing- und Interconnectionprozesse gebraucht werden, maximal 6 Monate lang aufbewahrt werden dürfen (Art. 123 Abs. 2). Die Teilnehmer müssen vom Netzbetreiber darüber informiert werden, dass ihre Daten gespeichert werden.

Des weiteren dürfen die in Art. 123 Abs. 2 genannten gespeicherten Daten auch für Marketingmaßnahmen und das Angebot von Mehrwertdiensten genutzt werden. Allerdings ist dafür die Zustimmung der betroffenen Teilnehmers erforderlich.

4.5 Ausgestaltung des Zugriffs der berechtigten Stellen

Der Zugriff auf gespeicherte Daten ist nur auf Antrag einer Strafverfolgungsbehörde beim Magistrat (Staatsanwalt) möglich, der eine Anordnung erlässt. Die genauen Umstände müssen aufgeführt werden, um zu beweisen, dass ein berechtigter Anlass zum Datenzugriff besteht (Katalogstraftaten). Im Zusammenhang mit der Bekämpfung von Terrorismus gilt die Ausnahmeregelung, dass Strafverfolgungsbehörden auch ohne Anordnung auf die gespeicherten Daten zugreifen dürfen.

Der Prozessablauf im Bereich der Datenvorratsspeicherung wird von den zuständigen Behörden als unproblematisch und effektiv wahrgenommen.

Es ist nicht bekannt, wie oft im Zuge der Strafverfolgung in der Vergangenheit auf gespeicherte Daten zugegriffen wurde.

4.6 Kostenentschädigung

4.6.1 Rechtliche Grundlagen

Basierend auf dem erwähnten Dekret Nr. 318 vom 19. September 1997 hat das Ministerium für Kommunikation gemeinsam mit dem Justizministerium Verordnungen erarbeitet, in denen die Verpflichtungen sowie die den Unternehmen zu gewährenden Entschädigungen beschrieben sind. Die Entschädigungssätze beziehen sich sowohl auf TKÜ-Maßnahmen als auch Recherchen nach gespeicherten Datensätzen. Ein entsprechendes Dekret, das die grundsätzlichen Rahmenbedingungen für die Kostenentschädigungen festlegt, wurde 2001 erlassen. In diesem Dekret wird auch die Liste der Verpflichtungen angekündigt, die detailliert die Anforderungen an die Unternehmen sowie die für diese Dienstleistung jeweils gewährten Kostenentschädigungen durch jeweiligen berechtigten Stellen beschreibt:

- Il Ministro delle Comunicazioni di concerto con Il Ministro delle Giustizia, Decreto 26 aprile 2001, Approvazione del listino relativo alle prestazioni obbligatorie per gli organismi di telecomunicazioni

Die Liste ist jedoch nur für die betreffenden Unternehmen zugänglich, nicht für die breite Öffentlichkeit. TK-Unternehmen können die Liste beim Ministerium für Kommunikation anfordern.[17]

4.6.2 Abwicklungsprozess

Die mit dem Decreto 26 aprile 2001 eingeführte „listino“ sieht ein Stufenkonzept vor, wonach die Unternehmen Investitions-, Wartungs- und Personalkosten geltend machen können. Die Kosten für die Übertragung werden zunächst von den Unternehmen getragen, die dann von dem jeweiligen Magistrat eine Rückerstattung erhalten können. Die Abrechnung erfolgt also lokal jeweils durch das Gericht, das die Überwachung angeordnet hat. Geltend gemacht werden können einzelne (Dienst-)Leistungen, die das Unternehmen für die berechtigte Stelle erbringt.

Von den Unternehmen wird kritisiert, dass die Abrechnung sehr aufwändig ist und die Rechnungen zu spät beglichen werden. Es müssen Einzelrechnungen pro Maßnahme gestellt werden. Diskutiert wird, künftig auch Sammelabrechnungen zum Jahresende zuzulassen, um den buchhalterischen Aufwand auf beiden Seiten zu verringern.

---

17 Vgl. Decreto 26 aprile 2001, Art. 6 (Adresse: Ministero delle comunicazioni, Direzione generale per la regolamentazione e la qualità dei servizi, viale America, 201, 00144 Roma, Italy).

4.6.3 Höhe der Kostenentschädigung

Die durch die Datenvorratsspeicherung bei den TK-Unternehmen entstehenden Kosten wurden im Rahmen heftiger Diskussionen um die Speicherungsdauer thematisiert. Es wurde insbesondere darauf hingewiesen, dass die in Italien außergewöhnlich lange Aufbewahrungsdauer die Kosten besonders stark in die Höhe treibt. Es liegen jedoch keine Kostenabschätzungen der TK-Wirtschaft über die genaue Höhe der anfallenden Kosten vor.

Die Höhe der gewährten Entschädigungen ist streng geheim. In der erwähnten „Listino“ sind die Tarifsätze im Detail festgelegt. Diese Liste ist für die Unternehmen zugänglich.

4.7 Besonderheiten und aktuelle Entwicklungen

Obwohl die gesetzlichen Grundlagen für Vorratsdatenspeicherung in Italien geschaffen wurden, sind einzelne Aspekte noch nicht gesetzlich geregelt und derzeit nur unvollständig geklärt. In der Praxis der Vorratsdatenspeicherung sind noch einige wichtige Fragen offen, darunter die genaue Art der zu speichernden Daten. Die gegenwärtig übliche Beschränkung der Vorratsdatenspeicherung auf Telefonverkehr wird in Zukunft wahrscheinlich aufgehoben. Die Ausweitung von Vorratsdatenspeicherung auf Internetverkehr wird bereits seit einiger Zeit intensiv diskutiert und entsprechende Gesetzesvorlagen sind in das italienische Parlament eingebracht worden.

5 Niederlande

5.1 Gesetzliche Grundlagen

5.1.1 Gesetzliche Grundlagen für Vorratsdatenspeicherung zum Zweck der Strafverfolgung

Eine eigene Gesetzgebung zu Vorratsdatenspeicherung existiert nicht. Die Grundlagen für eine Datenweitergabe an Strafverfolgungsbehörden für Strafverfolgungszwecke und an Nachrichtendienste sind im TKG festgelegt:

- Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet)[18]

genannt Tw. Relevant ist Kapitel 13, Artikel 1-8.

Einen Sonderfall, in dem Verbindungs- und Standortdaten (Verkehrsdaten) gespeichert werden müssen, regelt das Tw ebenfalls. Art. 13.4 (2) Tw bestimmt, dass für Dienste, für die keine Bestandsdaten vorliegen, die Verkehrsdaten drei Monate gespeichert werden müssen. Dies zielt insbesondere auf Prepaid-Karten im Mobilfunk.

Beschlüsse zu Vorratsdatenspeicherung

Weitere Regelungen sind im Beschuss v. 26.01.2000 zur Datenspeicherung von Bestandsdaten festgehalten:

- Besluit van 26 januari 2000, houdende regels voor de verstrekking van gegevens door aanbieders openbare telecommunicatienetwerken en -diensten met het oog op het onderzoek van telecommunicatie (Besluit verstrekking gegevens telecommunicatie, „Beschluss über das Bereitstellen von TK-Daten“).[19]

Diese Regelung spezifiziert die relevanten Artikel des Tw in Bezug auf die verpflichtende Speicherung und Weitergabe von Bestandsdaten .

Detaillierte Regelungen zur Verkehrsdatenspeicherung im Zusammenhang mit Prepaid-Karten enthält der Beschluss vom 18.12.2001:

---

18 Novelliert durch Wet van 22 april 2004 tot wijziging van de Telecommunicatiewet en enkele andere wetten in verband met de implementatie van een nieuw Europees geharmoniseerd regelgevingskader voor elektronische communicatienetwerken en -diensten en de nieuwe dienstenrichtlijn van de Commissie van de Europese Gemeenschappen. Es erfolgten keine relevanten Änderungen in Bezug auf das hier behandelte Thema.

19 Die Bestimmungen dieser Regelung wurden bisher freiwillig befolgt, seit 1. September 2004 ist der Beschluss vollständig in Kraft.

- Besluit van 18 december 2001, houdende regels voor de vergaring van nummergegevens door middel van afwijkend frequentiegebruik en bestandsanalyse met het oog op het onderzoek van telecommunicatie (Besluit bijzondere vergaring nummergegevens telecommunicatie, „Beschluss über das spezifische Sammeln von TK-Verkehrsdaten“)

Nach diesen Bestimmungen sind spezifische Daten für drei Monate aufzubewahren, die eine Identifikation von Teilnehmern erlauben, deren Bestandsdaten den TK-Anbietern aber nicht ohnehin zur Verfügung stehen. In der Praxis betrifft diese Regelung Mobilfunkanbieter, die Prepaid-Karten verkaufen.

5.1.2 Gesetzliche Grundlagen für anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung

Bestandsdaten müssen gespeichert werden, damit es den Strafverfolgungsbehörden möglich ist, Telekommunikation mitzuhören oder (ab einem bestimmten Zeitpunkt) aufzuzeichnen.

Der Gesetzentwurf „Aanpassing aan het Cybercrime Verdrag“, veröffentlicht Anfang 2004, hat die Umsetzung der Bestimmungen des Cybercrime-Abkommens in niederländisches Recht zum Ziel. Art 126ni und 126ui modifizieren die Strafprozessordnung dahingehend, dass ein stellvertretender Staatsanwalt per Anordnung Data Preservation veranlassen kann. Die Dauer soll 90 Tage betragen, eine einmalige Verlängerung um 90 Tage ist möglich. Die Anordnung darf erfolgen, wenn im Vorfeld der Anklageerhebung der Verdacht auf bestimmte Katalogstraftaten besteht.

In der Anordnung müssen schriftlich oder ausnahmsweise mündlich, bei Nachreichung der schriftlichen Anordnung innerhalb von drei Tagen, erfolgen. Die Anordnung muss enthalten: Beschreibung der zu speichernden Daten, Dauer und rechtliche Grundlage sowie Datum der Anordnung.

Es ist noch nicht absehbar, wann der Gesetzentwurf im Parlament verabschiedet wird und in Kraft tritt.

5.1.3 Gesetzliche Grundlagen der Datenspeicherung für unternehmenseigene Zwecke

Grundsätzlich müssen alle Daten nach einem Telekommunikationsvorgang anonymisiert oder gelöscht werden (Art. 11.5 Satz 2 Tw).

Ausnahmen sind gestattet für in Art. 11.5 Satz 3 Tw festgelegte Zwecke:

- Billing,
- Marktforschung,
- Marketing/Vertrieb,
- Klärung bei Einspruch gegen die Rechnung,
- Traffic Management,
- Speicherung für Zwecke des Teilnehmers (z.B. Einzelverbindungsnachweise etc.),
- Missbrauchsbekämpfung (z.B. Stalking Calls),
- andere gesetzlich geforderte Zwecke.[20]

Bei der Verwendung der Daten für Marktforschung, Marketing/Vertrieb muss der Teilnehmer sein Einverständnis geben (opt-in).

5.2 Praxis der Vorratsdatenspeicherung

5.2.1 Art, Umfang und Dauer

Laut niederländischem TKG sind diejenigen Daten zu speichern, die Informationen enthalten, die für die Pflichterfüllung der Strafverfolgungsbehörden bzw. berechtigten Stellen notwendig sind (Art. 13.4 Tw). Diese müssen gespeichert werden. Dazu zählen Bestandsdaten und Verkehrsdaten von Diensten, deren Bestandsdaten nicht zur Verfügung stehen (faktisch also Prepaid-Dienste im Mobilfunk).

a) Verpflichtung zur Speicherung und automatisierten Weitergabe von Bestandsdaten

Die TK-Anbieter müssen alle Daten weitergeben, die es den berechtigten Stellen erlauben, Telekommunikation aufzuzeichnen oder mitzuhören, also TKÜ-Maßnahmen durchzuführen. Dazu gehören ausdrücklich die folgenden Bestandsdaten (Art. 13.4 Tw):[21]

- Name,
- Adresse (Stadt, Postleitzahl),
- Rufnummer (einschließlich verdeckte oder geheime Nummern),
- Art der TK-Dienste, die in Anspruch genommen werden,

---

20 Gemeint ist z.B. die Strafverfolgung.
21 Auf niederländisch mit dem Kürzel NAW (für Name, Adresse, Kennung) bezeichnet.

- Identifizierung des TK-Anbieters.

Faktisch bedeutet dies, dass TK-Anbieter zum Monitoring und zur Speicherung aller Bestandsdaten verpflichtet sind. Die Einzelheiten sind in Art. 13.4 Tw, Art. 4 Besluit verstrekking gegevens telecommunicatie festgelegt.

Die og. Daten sind vom verpflichteten Unternehmen so zu speichern, dass sie jederzeit (24/7) von der dazu berechtigten „Zentralstelle" der Behörden, der sog. CIOT – Central Information System for Telecommunication Investigation, abgerufen werden können (Art. 2 und 3 Besluit verstrekking gegevens telecommunicatie). Für das automatisierte System des Bestandsdatenabrufs gibt es technische Spezifikationen.

Diese Zentralstelle kann auf die Bestandsdaten täglich aktualisiert zugreifen. Seit 1. September 2004 ist dieses Verfahren für alle – auch ISP – verpflichtend, bisher beruhte es auf einer freiwilligen Vereinbarung.

b) Speicherung und Weitergabe von Informationen für Prepaid-Mobilfunk

Sollten die Bestandsdaten den TK-Anbietern nicht ohnehin für eigene Zwecke vorliegen, sind sie verpflichtet, für diesen Dienst Verkehrsdaten zu speichern (Art. 13.4 (2) Tw). Diese allgemein formulierte Bestimmung betrifft in der Praxis die Mobilfunkanbieter.

Sie bedeutet im Einzelnen, dass bei Prepaid-Karten im Mobilfunk die Verkehrsdaten für drei Monate zu speichern sind. Im Besluit bijzondere vergaring nummergegevens telecommunicatie, Art. 7 ist in Bezug auf Art. 13.4 (2) Tw festgelegt, für welche Datenarten generell Vorratsdatenspeicherung für die Dauer von 90 Tagen verlangt wird. Dies sind

- Beginn und Ende der Telekommunikation (Zeit, Datum),
- Nummer des Anrufers und Angerufenen (z.B. bei SMS auch Sender IP-Adresse),
- Standortdaten (Cell Location im Mobilfunk), IMEI.[22]

Diese Daten, die für die Zentralstelle CIOT nicht unmittelbar zugänglich gehalten werden, sind „unverzüglich" an diese schriftlich auf Anforderung weiterzugeben; wenn es nicht anders möglich ist, auch mündlich (Art. 6 Satz 2 Besluit bijzondere vergaring nummergegevens telecommunicatie).

c) Weitergabe von Daten, die für unternehmenseigene Zwecke gespeichert werden

Allgemein gilt, dass weitere Daten, also Daten, die der Anbieter für eigene Zwecke speichert und die von den Strafverfolgungsbehörden benötigt werden, vom TK-Anbieter an die berechtigten Stellen auf Anforderung weiterzugeben sind.

---

22 Keine Verpflichtung zur Datenspeicherung besteht demnach also bei Prepaid-Karten für Name, Adresse und IMSI.

Die Datenweitergabe erfolgt in dem Format, in dem die Daten dem TK-Anbieter vorliegen.

Es handelt sich im wesentlichen um folgende Datentypen, die für unternehmenseigene Zwecke mit den angegebenen Fristen gespeichert werden:

- Bestandsdaten: Löschung 1 Jahr nach Vertragsende,
- Verkehrsdaten Mobilfunk, SMS, MMS: etwa 5 Monate,
- Verkehrsdaten Festnetz-Telefonie: etwa 6 Monate,
- Verkehrsdaten E-Mail: unterschiedlich, ca. eine Woche,
- Internet-Access: unterschiedlich, wenige Monate,
- WWW, Chat, IRC, News groups: keine Datenspeicherung.

5.2.2 Kreis der Verpflichteten

Alle Bestimmungen sind technikoffen formuliert. Daher sind alle Netzbetreiber und Anbieter von öffentlichen Telekommunikationsdienstleistungen zur Kooperation mit den Strafverfolgungsbehörden verpflichtet.

Von den spezifischen Vorratsdatenspeicherungs-Verpflichtungen durch den Beschluss „Besluit bijzondere vergaring nummergegevens telecommunicatie“ sind in der Praxis nur Mobilfunknetzbetreiber betroffen.

Ausnahmen von den Verpflichtungen des Tw sind möglich, wenn das zuständige Wirtschaftsministerium sie im Einvernehmen mit dem Innenministerium und dem Justizministerium gewährt. Es sind bisher keine Ausnahmen getroffen worden.

5.2.3 Relevanz für Strafverfolgung und nationale Sicherheit

Im Gegensatz zu Ländern wie z.B. Deutschland, USA oder UK existieren in den Niederlanden keinerlei offizielle Statistiken zu jährlich durchgeführten TKÜ-Maßnahmen und Datenabfragen der Strafverfolgungsbehörden.

Es gibt vereinzelte Hinweise auf die Häufigkeit von Bestandsdatenabfragen zu Strafverfolgungszwecken. Im Jahr 2001 bezifferte das zuständige Justizministerium die Abfrage

von Bestandsdaten auf etwa 300.000 bis 350.000 pro Jahr. Das Ministerium schätzt den Anstieg in den nächsten Jahren auf bis zu 900.000 Anfragen pro Jahr.[23]

Das niederländische Justizministerium hat außerdem im Jahr 2003 eine Studie in Auftrag gegeben, um den Beitrag von Bestandsdatenrecherche via CIOT und gespeicherten Verkehrsdaten bei der Aufklärung von Straftaten untersuchen zu lassen. Die Studie ist nicht öffentlich, wurde aber durch die niederländische Bürgerrechtsorganisation Bits of Freedom durch einen sog. „Public Access Request" nach dem Informationsfreiheitsgesetz öffentlich gemacht.[24]

Dem Bericht zufolge, so Bits for Freedom, würde eine über das bisherige Maß ausgedehnte Vorratsdatenspeicherung von Verkehrsdaten für die Strafverfolgung kaum eine Verbesserung der Situation für die Behörden leisten. Schon heute nutzt die Polizei standardmäßig in 90% aller Untersuchungen Telekommunikationsdaten (Bestandsdaten und teilweise Verkehrsdaten). Dabei scheint die Art der Daten, die heute von den TK-Anbietern für eigene Zwecke gespeichert wird, ausreichend zu sein. Zwei Drittel aller Fälle hätten auch ohne Kenntnisse über Verkehrsdaten gelöst werden können.

Vorhandene Daten werden hauptsächlich dazu genutzt, die Kommunikationswege (Kontaktpersonen) von Verdächtigen zu eruieren, Personenüberwachungen zu unterstützen oder Alibis zu überprüfen (z.B. durch GSM Standortdaten). In dem Bericht wird ausgeführt, dass nur selten Verkehrsdaten, die älter als sechs Monate sind, benötigt werden.

5.3 Praxis der anlassbezogenen Datenspeicherung

Zurzeit besteht keine Regelung zu Data Preservation, diese ist jedoch im Rahmen der Umsetzung des Cybercrime-Abkommens des Europarats geplant. Ein Gesetzentwurf dazu liegt vor (s. Kap. 4.7).

5.4 Praxis der Datenspeicherung für unternehmenseigene Zwecke

Nach Art. 11.5 Tw dürfen Unternehmen Daten für Rechnungstellung, Marketing und Mehrwertdienste für 6 Monate speichern, wenn der Teilnehmer zugestimmt hat. Bestandsdaten müssen ein Jahr nach Vertragsende gelöscht werden.

Standortdaten dürfen gespeichert werden, soweit diese anonymisiert werden oder wenn der Teilnehmer zugestimmt hat, dass diese Daten für die Dienstleistungserbringung verwandt werden.

---

23 Kamerstukken II 2001/02, 28 059, nr. 3, p.17.

24 http://www.bof.nl/docs/rapport_verkeersgegevens.pdf. Der Report ist nur auf niederländisch verfügbar. Die hier dargestellte Bewertung wurde übernommen von dem englischsprachigen Newsletter EDRI-gram biweekly newsletter about digital civil rights in Europe Number 2.18, 22 September 2004.

Diese Bestimmungen sind im novellierten Tw v. 22.04.2004 festgehalten (Staatsblad 2004, 189). Das Gesetz ist noch nicht in Kraft getreten, die Bestimmungen stellen jedoch keine wesentlichen Änderungen gegenüber der vorhergehenden Regelung dar.

5.5 Ausgestaltung des Zugriffs der berechtigten Stellen

Die rechtlichen Grundlagen für den Zugriff der berechtigten Stellen auf TK-Daten sind in den Niederlanden nicht im Strafgesetzbuch (Wetboek van strafvordering) festgelegt, sondern im Telekommunikationsgesetz (Art. 13.4 Tw).

Die Strafprozessordnung bestimmt nach Art. 126n und 126u, dass Staatsanwälte (officier van justitie) unter bestimmten Voraussetzungen Zugriff auf Kommunikationsinhalte und Verkehrsdaten erhalten dürfen.

Relevant ist außerdem das Gesetz Wet BOB (Wet Bijzondere opsporingsbevoegdheden) („Gesetz über besondere Befugnisse bei Ermittlungsverfahren“), welches am 1. Februar 2000 in Kraft trat und eine Novellierung der Strafprozessordnung beinhaltet. Neben zahlreichen anderen Veränderungen ist es nunmehr gestattet, Telekommunikation in einem geschlossenen Netz, z.B. einem Unternehmensnetzwerk, zu überwachen. Außerdem kann ein PC „verwanzt“ werden, d.h. beispielsweise, es darf technisches Equipment implementiert werden, um E-Mail-Kommunikation abzufangen, bevor sie ggf. verschlüsselt und über das Internet gesendet wird. Auch der Einsatz von Scannern (IMSI-Catchern) zum Abhören von Mobilkommunikation wurde mit der Gesetzesänderung legitimiert. Somit stehen den niederländischen Strafverfolgungsbehörden neben der TKÜ und der Auswertung historischer Verkehrsdaten weitere Ermittlungsmethoden zur Verfügung.

Eine weitere entscheidende Änderung durch das Wet BOB besteht darin, dass für die Überwachung keine richterliche Anordnung mehr erforderlich ist. Ein von einem Richter dazu autorisierter Staatsanwalt darf einen Durchsuchungsbefehl ausstellen, um die Telekommunikation eines Verdächtigen zu erhalten (Artikel 126n der niederländischen Strafprozessordnung).

5.6 Kostenentschädigung

5.6.1 Rechtliche Grundlagen

In den Niederlanden erfolgt eine Entschädigung der Anbieter nach Artikel 13.6 Tw.

Es ist dem für Telekommunikation zuständigen Wirtschaftsministerium (Ministerie van Economische Zaken) vorbehalten, in einer Verordnung die näheren Bestimmungen festzulegen. Dies ist bisher noch nicht geschehen. Die Rahmenbedingungen für eine Verordnung werden seit längerem kontrovers mit den Anbietern diskutiert.

Die Kostenentschädigungssätze werden vom zuständigen Justizministerium jeweils gesondert mit jedem Festnetz- und Mobilfunkanbieter vereinbart.[25] Diese Sätze unterscheiden sich zum Teil erheblich in Höhe und Struktur. Die tatsächliche Entschädigungssumme ist fallabhängig, d.h. jedes Unternehmen stellt eine Rechnung mit den aus seiner Sicht relevanten Kosten. Eine allgemein gültige Gebührenordnung existiert nicht.

5.6.2 Abwicklungsprozess

Das Abrechnungsverfahren in den Niederlanden ist dezentral organisiert. Die Zahlungen erfolgen über die „Reichskasse“, d.h. Anträge auf Kostenentschädigung können im jeweiligen der 19 niederländischen Distrikte beim zuständigen Staatsanwalt, der die Überwachung veranlasst hat, gestellt werden und dieser erhält die Mittel über das Finanzministerium.

5.6.3 Höhe der Kostenentschädigung

Grundsätzlich ist in Artikel 13.6 (1) TKG festgelegt, dass die Investitions-, die Betriebs- und Wartungskosten von den zur Überwachung bzw. Weitergabe von Bestands- und Verkehrsdaten verpflichteten Anbietern allein zu tragen sind.

Allerdings wird im nachfolgenden Absatz Artikel 13.6 (2) TKG eingeräumt, dass die Anbieter eine Entschädigung für ihre

- Administrations- und Personalkosten,

d.h. ihrer variablen Kosten, die im direkten Zusammenhang mit der Bearbeitung einer Anordnung stehen, beantragen können. Auf diese Weise erhalten die Anbieter einen Teil ihrer Betriebskosten zurück. Unternehmensweite Gemeinkosten können pro Anordnung anteilig geltend gemacht werden.

Kapitalkosten in Aufwendungen für Überwachungseinrichtungen oder Übertragungstechnik sind somit nicht entschädigungsfähig.

Die Kosten für die Übertragung der Echtzeit-Telekommunikation bzw. der Daten an die Untersuchungsbehörden werden vollständig auf Grundlage der marktüblichen Tarife erstattet.

Die Höhe der derzeitigen Kostenentschädigung ist ersichtlich aus einem Bericht des Justizministeriums über die Justizkosten (Aanvulling op de circulaire afbakening tussen

---

25 Die veröffentlichten Entschädigungssätze stammen aus dem Jahr 2000: Aanvulling op de circulaire afbakening tussen politie en justitiekosten (circulaire van 1 januari 2000, kenmerk 806730/889).

politie en justitiekosten (circulaire van 1 januari 2000, kenmerk 806730/889). Das Ministerium hat mit jedem Festnetz- und Mobilfunkanbieter[26] gesondert eine Vereinbarung über die Entschädigungssätze getroffen, die ab dem 1. März 2000 gelten.

Die Tarife unterscheiden sich nicht nur in der Höhe, sondern auch in ihrer Struktur (vgl. Tabelle 5-1). Hinzu kommen unterschiedliche Zuschläge je nach Anbieter pro Tag, die zusätzlich noch nach Uhrzeiten differenziert werden (Bürozeiten / außerhalb der Bürozeiten / Samstage / Sonn- und Feiertage).

Für die Ablieferung von Verkehrsdaten erhält KPN z.B. 25,41 Euro (Verkehrsdaten einer Woche) oder 3,63 Euro (Verkehrsdaten eines Tages). Seine Mobilfunktochter erhält dagegen 50,82 bzw. 7,26 Euro. Auch hier werden Zuschläge für Tätigkeiten außerhalb der üblichen Bürozeiten gezahlt.

Auskünfte werden pro Auskunft entschädigt. Auch hier existieren unterschiedliche Tarife. Es wird außerdem zwischen einfachen Auskünften über Name, Adresse und TK-Kennung (z.B. Telefonnummer) und weiteren Auskünften unterschieden. Diese beziehen sich z.B. darauf, welche Dienste der Teilnehmer sonst noch nutzt oder auch die Logfiles. Die Auskunft über Logfiles rechtfertigt zumeist den höchstmöglichen Entschädigungssatz von 180,60 Euro.

Den ISP ist es möglich, nach den Vorgaben des Tw ihre tatsächlich entstandenen Administrations- und Personalkosten einzufordern. Dabei hat die Erfahrung gezeigt, so der Verband der Internet-Provider NLIP, dass Stundensätze von rd. 50 bis 100 Euro akzeptiert werden. Es können also die tatsächlichen Stundensätze für Fachkräfte wie Netzwerkadministratoren, Sicherheitsmanager oder auch Juristen, die die Anordnungen prüfen müssen, geltend gemacht werden.

Die Ausführungen verdeutlichen, dass es kaum möglich erscheint, aus diesem komplexen Tarifmodell und der vorgefundenen Praxis auf die im Durchschnitt an die Anbieter geleisteten Zahlungen zu schließen. Veröffentlichte Statistiken liegen dazu nicht vor.

---

26 Damals waren dies die Unternehmen KPN vast net, KPN mobiel, Libertel mobiel, BEN mobiel und Dutchtone.

Tabelle 5-1: Kostenentschädigung an TK-Anbieter für Legal Interception in den Niederlanden (Stand Januar 2000)

Art der Daten	Zeitraum	KPN vast net	KPN mobiel	Libertel mobiel	BEN mobiel	Dutchtone (per Tap)
Leveren van verkeersgegevens (historische) gegevens (eenmalig) ***(Ablieferung von historischen Verkehrsdaten, einmalig)***	08.00-17.00h			7,94 €		
per week *(Verkehrsdaten pro Woche)*	08.00-17.00h	25,41 €	50,82 €			
per dag *(Verkehrsdaten pro Tag)*	08.00-17.00h	3,63 €	7,26 €			
verkehrsgeg. basisstations *(Verkehrsdaten Basisstation)*	08.00-17.00h		63,98 €			
NAW gegevens ***(Bestandsdaten (Name, Adresse, Telnr./Kennung))***				6,47 €	11,34 €	11,34 €
NAW Daten anderer Provider				3,97 €		
NAW Daten o.b.v. nacalculatie uurtarief *(Bestandsdaten nach Stundentarif)*					37,44 €	41,53 €
Abfrage PUK-Code				10,60 €		
data analyse/locatiebepaling (diepgaand) *(Datenanalyse/Standortdaten (ausführlich))*				20,42 €		
Invormationsverstrekking *(Auskünfte)*						
enkelvoudige info verstrekking *(einfache Auskunft)*	08.00-17.00h	2,18 €				
Meervoudige infoverstrekking *(mehrteilige Auskunft)*	08.00-17.00h	34,03 €				
Diepgaande infoverstrekking *(detaillierte Auskunft [z.B. logfiles])*	08.00-17.00h	180,60 €				

Quelle: Aanvulling op de circulaire afbakening tussen politie en justitiekosten (circulaire van 1 januari 2000, kenmerk 806730/889)

5.7 Besonderheiten und aktuelle Entwicklungen

Innerhalb der für die Regelung der TK-Überwachungsverpflichtungen zuständigen niederländischen Regulierungsbehörde OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) existiert ein Konsultationsgremium, unter dem auch ein Beratungsgremium zu Fragen der Telekommunikation und Strafverfolgung angesiedelt ist. Dieses Gremium besteht aus Vertretern verschiedener Telekommunikationsanbieter und Repräsentanten der zuständigen Regierungsbehörden, wie etwa des Generalbundesanwalts, der Polizei, des Innenministeriums, des Wirtschaftsministeriums und des Justizministeriums. Innerhalb dieses ständigen Gremiums werden regelmäßig Fragen im Zusammenhang mit der TK-Überwachung und Datenspeicherung erörtert. Die Institution hat sich nach Auffassung der Beteiligten bewährt, um frühzeitig Kontroversen zu diskutieren.

6 Schweden

6.1 Gesetzliche Grundlagen

In Schweden gibt es keine gesetzlichen Regelungen, die sich auf die Vorratsdatenspeicherung zum Zweck der Strafverfolgung beziehen. Bisher gilt, dass Netzbetreiber zu diesem Zwecke all diejenigen Daten bereitstellen, über die sie verfügen. Eine gesetzliche Regelung zur Vorratsdatenspeicherung ist zwar geplant, es liegt aber noch kein Gesetzesentwurf vor.

Die Aktivitäten zur gesetzlichen Reglung der Vorratsdatenspeicherung beschränken sich allein auf den Vorschlag zu einem Rahmenbeschluss, den Schweden zusammen mit Großbritannien, Frankreich und Irland bei der EU eingebracht hat.

Andere Gesetze, die im Zusammenhang mit der Speicherung von Daten durch TK-Netzbetreiber relevant sind, existieren jedoch:

- Datenschutzgesetz „Personuppgiftslag“ (1998:204)

  Im Datenschutzgesetz (Personuppgiftslag), das am 24. Oktober 1998 in Kraft trat, wurde die EU-Direktive 95/46/EC zum Datenschutz umgesetzt. Es ersetzt den Swedish Data Act von 1973.[27] In einer Übergangszeit bis zum 30. September 2001 galten für persönliche Daten, die vor dem 24. Oktober 1998 erhoben wurden, noch die Regelungen des alten Gesetzes.

  Das Datenschutzgesetz bezieht sich grundsätzlich auf alle personenbezogenen Daten, die ganz oder teilweise automatisch verarbeitet werden. Es enthält keine Regelungen für den Umgang mit Daten, die im Zusammenhang mit der Übertragung von TK-Diensten entstehen.

  Als unabhängige zentrale Datenschutzbehörde wurde die Behörde „Datainspektionen“ eingerichtet, die sich um den Erlass von Gesetzen und anderen Rechtsvorschriften kümmert, die Entwicklungen im Bereich des Datenschutzes beobachtet und als fachlich kompetenter Ansprechpartner bereitsteht.[28]

- Telekommunikationsgesetz „Lag om elektronisk kommunikation” (2003:389)

  Im neuen Telekommunikationsgesetzes, das am 25. Juli 2003 in Kraft getreten ist (Lag om elektronisk kommunikation) wird in Kapitel 6 die Verarbeitung von Ver-

---

27 Die schwedische Version des Personal Data Act kann heruntergeladen werden unter der Adresse http://www.notisum.se/rnp/sls/lag/19980204.HTM.

28 Vgl. www.datainspektionen.se.

kehrsdaten geregelt.[29] Als Verkehrsdaten werden in dem Gesetz alle Daten definiert, die zum Zwecke der Übertragung elektronischer Nachrichten über elektronische Kommunikationsnetze oder zur Abrechnung der erbrachten Dienste verarbeitet werden, also Verbindungs- und Standortdaten.

Grundsätzlich müssen Verkehrsdaten sofort gelöscht werden, sobald sie nicht mehr aus technischen Gründen zur Übermittlung des Dienstes gebraucht werden (Kapitel 6, Artikel 5). Es bestehen jedoch drei Ausnahmen (Artikel 6 und 8):

a) Verkehrsdaten, die für das Billing der Dienste benötigt werden, dürfen von den Diensteanbietern gespeichert werden, bis die Rechung gezahlt und die Anfechtungsfrist abgelaufen ist.

b) Soweit die Teilnehmer ihre Zustimmung geben, dürfen die Verkehrsdaten auch für Marketingzwecke gespeichert werden. Die Zustimmung kann jederzeit wider rufen werden.

In beiden Ausnahmefällen a) und b) müssen die Diensteanbieter die Teilnehmer darüber informieren, welche Art von Daten für diese Zwecke gespeichert werden und wie lange dies geschieht.

c) Die dritte Ausnahme von der grundsätzlichen Löschpflicht betrifft Daten, die durch gesetzliche Überwachungsmaßnahmen gewonnen werden.

Der Zugriff der Strafverfolgungsbehörden auf bei den Netzbetreibern und Diensteanbietern gespeicherten Verkehrsdaten erfolgt auf Grundlage der Regelungen in Kapitel 6 Artikel 22 in Verbindung mit Artikel 20.

Bestandsdaten dürfen die Strafverfolgungsbehörden dann abfragen, wenn sie im Zusammenhang mit einem Verbrechen ermitteln, für das eine Freiheitsstrafe verhängt werden kann und die Behörden auch davon ausgehen, dass mehr als eine Geldstrafe verhängt wird.

Verkehrsdaten dürfen die Strafverfolgungsbehörden nur dann abfragen, wenn sie im Zusammenhang mit einem Verbrechen ermitteln, auf das eine Freiheitsstrafe von mindestens zwei Jahren steht.[30]

---

29 Die englische Version des Telekommunikationsgesetzes ist verfügbar unter http://www.pts.se/Archive/Documents/EN/Engelsk_ekomlag.pdf

30 Diese Bestimmung soll künftig entschärft werden und der Datenzugriff bereits bei Verbrechen mit 6-monatiger Mindeststrafe erlaubt werden (vgl. Abschnitt 6.7).

6.1.1 Gesetzliche Grundlagen für Vorratsdatenspeicherung zum Zweck der Strafverfolgung

Gesetzliche Grundlagen für Vorratsdatenspeicherung zum Zweck der Strafverfolgung sind in Schweden bisher noch nicht geschaffen worden.

6.1.2 Gesetzliche Grundlagen für anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung

Für anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung existieren in Schweden keine gesetzlichen Regelungen und somit wird dieses Instrument der Strafverfolgung auch nicht eingesetzt.

6.1.3 Gesetzliche Grundlagen der Datenspeicherung für unternehmenseigene Zwecke

Die Speicherung von Verkehrsdaten für Marketingzwecke ist nach dem schwedischen Telekommunikationsgesetz Kapitel 6, Artikel 6 dann erlaubt, wenn die Zustimmung der Teilnehmer vorliegt und diese über Art der Daten und Dauer der Speicherung informiert sind.

6.2 Praxis der Vorratsdatenspeicherung

Nicht zutreffend, da Vorratsdatenspeicherung nicht gesetzlich geregelt ist.

6.3 Praxis der anlassbezogenen Datenspeicherung

nicht zutreffend

6.4 Praxis der Datenspeicherung für unternehmenseigene Zwecke

Im Prinzip dürfen TK-Unternehmen in Schweden entscheiden, welche Daten sie mit Einverständnis der Teilnehmer oder Nutzer speichern.

6.5 Ausgestaltung des Zugriffs der berechtigten Stellen

Zu den Behörden, die auf gespeicherte Daten im Rahmen der Strafverfolgung zugreifen dürfen, gehören u.a. Polizei, Finanzpolizei, Küstenwacht und Zollbehörden.

Anlässlich des EU-Meetings zum Thema Vorratsdatenspeicherung am 14. Juni 2004 in Brüssel führte TeliaSonera aus, dass etwa 3.000 - 4.000 Anfragen pro Jahr stattfinden. Davon bezieht sich etwa die Hälfte auf leichte Verbrechen, für die nur Bestandsdaten, aber keine Verkehrsdaten abgefragt werden dürfen.

Die Anfragen beziehen sich zu 68% auf Mobilfunk-, zu 30% auf Festnetz- und zu 2% auf Internetdienste. 85% der angefragten Daten stammen aus einem Zeitraum, der nicht länger als 3 Monate zurückliegt. Weitere 10% der Daten sind maximal ein halbes Jahr alt. Über 1 Jahr alt sind nur 0,5% aller von den berechtigten Behörden angefragten Informationen.[31]

6.6 Kostenentschädigung

Es existieren keine gesetzlichen Regelungen zur Kostenentschädigung. In der Praxis werden Kosten der strafbehördlichen Datenabfragen jedoch in der Regel erstattet.

6.6.1 Rechtliche Grundlagen

Es existieren keine gesetzlichen Regelungen zur Kostenentschädigung der Datenabfragen. Da bislang auch noch kein Gesetzesentwurf zur Vorratsdatenspeicherung vorliegt, sind künftige Kostenentschädigungen für Vorratsdatenspeicherungen noch völlig offen.

6.6.2 Abwicklungsprozess

In Schweden existiert kein einheitlicher Abwicklungsprozess für die Kostenrückerstattung, da jede Behörde fallweise die Kosten zurückerstattet.

Anbietern zufolge können die Kosten der Vorratsdatenspeicherung den anfragenden Behörden in Rechnung gestellt werden. Allerdings dürfen dabei lediglich die Kosten für den Personalaufwand angesetzt werden.

Nach Auskunft des Justizministeriums stellen die Netzbetreiber Datenauskünfte unterschiedlich hoch in Rechnung. Einige Netzbetreiber verzichten auf eine Berechnung der Datenauskunft, da die Rechnungstellung zu aufwändig erscheint.

---

31 Vgl. Thomas Holst, TeliaSonera: Retention of Communications Data to Fight Crime & Terrorism, Folie 3 und 4.

6.6.3 Höhe der Kostenentschädigung

Über die konkrete Höhe der Kostenentschädigungen liegen keine Informationen vor.

6.7 Besonderheiten und aktuelle Entwicklungen

Am 1. Oktober 2004 tritt eine Gesetzesänderung in Kraft, die es erlaubt, dass Verkehrsdaten bereits für Ermittlungen im Zusammenhang mit Verbrechen mit sechsmonatiger Mindesthaftstrafe angefordert werden dürfen, anstatt nur bei Verbrechen mit mindestens zweijähriger Haftstrafe. Diese Änderung ist Bestandteil eines neuen Überwachungsgesetzes, das nach Einschätzung der Einschätzung von Rechtsexperten angefochten und gerichtlich überprüft werden wird.

7 Spanien

7.1 Gesetzliche Grundlagen

7.1.1 Gesetzliche Grundlagen für Vorratsdatenspeicherung zum Zweck der Strafverfolgung

Das Fernmeldegeheimnis ist in der spanischen Verfassung Art. 18 Abs. 3 garantiert. Fernmeldekommunikation darf nur offen gelegt werden, wenn eine richterliche Anordnung vorliegt. Diese Bestimmung findet sich sowohl in der Verfassung als auch im Strafgesetzbuch. Es ist im spanischen Recht nicht explizit kodifiziert und daher umstritten, ob außer den Inhalten einer Kommunikation auch die „Randdaten", also die Verkehrsdaten, durch das Fernmeldegeheimnis geschützt sind.

Das Gesetz zum allgemeinen Datenschutz in Bezug auf „Dienste der Informationsgesellschaft und Electronic Commerce", das auch die Regelungen zu Vorratsdatenspeicherung enthält, trat in Spanien im Sommer 2002 in Kraft:

- Ley 34/2002 de 11 de julio, se servicios del sociedad de la información y de comercio electrónico, BOE núm 166 (Gesetz 34/2002 vom 11. Juli über Dienste der Informationsgesellschaft und Electronic Commerce).[32]

Art. 12 regelt die Vorratsdatenspeicherung. Das Gesetz wird im allgemeinen Sprachgebrauch mit „LSSI" abgekürzt.

Die näheren Bestimmungen sollen durch eine den gesetzlichen Rahmen ausfüllende Verordnung geregelt werden (Art. 12 Abs. 4). Diese wird folgende Regelungstatbestände enthalten:

- Art der Daten, die gespeichert werden müssen,
- Dauer der Speicherung für jeden Datentyp (bei Beachtung der Höchstgrenze von 12 Monaten),[33]
- Vorschriften für die Art der Datenspeicherung, der Verarbeitung und Sicherung sowie die Form der Weitergabe an die berechtigten Stellen,
- Vorschriften für die Löschung von Daten.

---

32 Gesetz wurde geändert durch: BOE No. 264 v. 4.11.2003, BOE No. 304 v. 20.12.2003.

33 In der Verordnung wird demnach die Mindestspeicherfrist festgelegt werden. Das LSSI enthält nur die maximale Speicherfrist.

Nach mittlerweile zwei Jahren seit Verabschiedung des Gesetzes liegt immer noch kein Verordnungsentwurf vor.

7.1.2 Gesetzliche Grundlagen für anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung

Anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung kann auf Basis der spanischen Strafprozessordnung auf richterliche Anordnung bzw. Anordnung eines Staatsanwalts erfolgen.

7.1.3 Gesetzliche Grundlagen der Datenspeicherung für unternehmenseigene Zwecke

Die Speicherung persönlicher Daten ist in Spanien durch das allgemeine Datenschutzgesetz geregelt:

- Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal. BOE núm. 298
  (Gesetz 15/1999 vom 13. Dezember über den Schutz persönlicher Daten)

Das Gesetz ist unter dem Kürzel „LOPD“ bekannt.

Es enthält allgemeine Vorschriften zum Schutz persönlicher Daten, die im öffentlichen oder privaten Sektor gespeichert werden. Persönliche Daten dürfen nur zweckbezogen verwendet werden, d.h. für die Zwecke, für die sie erhoben wurden. Sie dürfen nur dann weitergegeben werden, wenn die jeweilige Person zugestimmt hat (opt-in). Es existieren aber auch Ausnahmen, bei denen die Verwendung gestattet ist, ohne dass die ausdrückliche Zustimmung der Person vorliegt.

Die Durchsetzung der Bestimmungen obliegt der spanischen Datenschutzbehörde (Agencia de Protección de Datos - APD). Behörden und Unternehmen, die Datenbanken verwalten, müssen diese bei der Datenschutzbehörde registrieren. Die Behörde ist befugt, bei Verstößen gegen das LOPD Sanktionen (z.B. Geldstrafen) zu verhängen.

Die spezifischen Regelungen zum Datenschutz im Zusammenhang mit Telekommunikation finden sich im spanischen TKG, novelliert im Jahr 2003. Teil III (Título III Obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas) des spanischen TKG enthält die Datenschutzbestimmungen in Bezug auf Telekommunikation:

- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, BOE núm. 264 (Gesetz 32/2003 vom 3. November)

Die spezifizierten Regelungen enthält das Königliche Dekret aus dem Jahr 1998, das den Teil III des spanischen TKG[34] in Kraft setzt:[35]

- Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el Título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones, BOE núm. 213.

Das LSSI (Ley 34/2002) bildet eine weitere gesetzliche Grundlage für die Speicherung von Daten für Werbezwecke, die im Zusammenhang mit TK-Dienstleistungen entstehen. Die Bestimmungen des LSSI modifizieren insofern die strengeren Regelungen des TKG geringfügig.

Auch in Bezug auf die sektorspezifische Datenschutzgesetzgebung ist die spanische Datenschutzbehörde sanktionsbefugt.

7.2 Praxis der Vorratsdatenspeicherung

7.2.1 Art, Umfang und Dauer

Die Maximalspeicherfrist für Zwecke der Strafverfolgung und nationalen Sicherheit beträgt nach LSSI 12 Monate.

Eine Mindestspeicherfrist ist nicht gesetzlich festgelegt. Dies ist insofern bemerkenswert, als ein TK-Anbieter die gesetzlichen Vorgaben dadurch auch dann erfüllt, wenn er die geforderten Daten nur beispielsweise für 12 Stunden speichert und danach mit neu gewonnenen Datensätzen überschreibt. Nach Expertenaussagen kommt diese „kostensparende Auslegung“ des Gesetzes in der Praxis durchaus häufig vor. Eine Mindestspeicherfrist soll in der noch ausstehenden Verordnung festgelegt werden.

Daten, die das Fernmeldegeheimnis betreffen, dürfen laut LSSI nicht für Zwecke der Strafverfolgung gespeichert werden.

Darüber hinaus dürfen die verpflichteten Unternehmen die im Rahmen von Vorratsdatenspeicherung gespeicherten Daten auch für eigene Zwecke verwenden, wenn dies mit dem LSSI und der allgemeinen Datenschutzgesetzgebung in Einklang steht.

---

34 Damals die erste Fassung des TKG (Ley 11/1998, de 24 de abril, General de Telecomunicaciones).

35 Das Dekret ist trotz der Novellierung des TKG im Jahr 2003 immer noch gültig, muss aber noch an die jetzt geltende Rechtslage angepaßt werden. Ein Dekretentwurf befindet sich in der behördeninternen Diskussion.

Sie sind verpflichtet, Sicherheitsmaßnahmen zu ergreifen, die Verlust, unbeabsichtigte Änderungen und den Zugang von nicht-autorisierten Dritten zu diesen Daten verhindern (Art. 12 Abs. 2 Satz 4).[36]

Das Königliche Dekret 994/1999 vom 11. Juni

- Real Decreto 994/1999 , de 11 de junio por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal

umfasst weitgehende, detaillierte Vorschriften über den Umgang mit persönlichen Daten. Darin werden verpflichtende Sicherheitsmaßnahmen festgelegt. Die Vorschriften, die nicht nur TK-Anbieter betreffen, führen nach Ansicht der Unternehmen zu hohen Kosten bei der Speicherung und Verarbeitung von Daten. Die weitgehenden, verbindlich vorgeschriebenen Sicherheitsverpflichtungen werden als entscheidende Kostentreiber im Zusammenhang mit Regelungen zur Vorratsdatenspeicherung gesehen.

7.2.2 Kreis der Verpflichteten

Folgende Unternehmenstypen sind zu Vorratsdatenspeicherung für Zwecke der Strafverfolgung von bestimmten Datentypen verpflichtet (LSSI Art. 12 Abs. 1):

• Netzbetreiber und Service Provider (operadores de redes y servicios de comunicaciones electróicas)	ausschließlich Daten, die geeignet sind, Endgeräte zu lokalisieren (Standortdaten)
• Access Provider (proveedores de acceso a redes de telecomunicaciones):	ebenfalls ausschließlich Daten, die geeignet sind, Endgeräte zu lokalisieren (Standortdaten)
• Housing Provider (prestadores de servicios de alojamiento de datos):	ausschließlich Daten, die geeignet sind, die Herkunft der gespeicherten Daten zu bestimmen sowie Daten, die den Beginn der Nutzung einer Dienstleistung bezeichnen.

Innerhalb dieses Rahmens gibt es keinerlei Ausnahmen von den Speicherungs-Vorschriften.

---

36 Weitgehende Vorschriften zur Gewährleistung von IT-Sicherheit im Zusammenhang mit gespeicherten Daten finden sich im Königlichen Dekret 994/1999 v. 11. Juni 1999, BOE núm.151.

In der geplanten Verordnung werden die Datentypen und die Speicherungsdauer im Einzelnen festgelegt werden.

7.2.3 Relevanz für Strafverfolgung und nationale Sicherheit

In Spanien liegen keine Untersuchungen zur Relevanz von Vorratsdatenspeicherung für die Strafverfolgung und belange der nationalen Sicherheit vor. Die erwähnte Praxis der Vorratsdatenspeicherung nach dem Prinzip der Ausnutzung einer kürzestmöglichen Speicherfrist legt jedoch nahe, dass die Wirksamkeit des Gesetzes stark begrenzt ist.

7.3 Praxis der anlassbezogenen Datenspeicherung

In Spanien wurde die Cybercrime Convention des Europarats noch nicht ratifiziert. Data Preservation ist jedoch prinzipiell möglich, wenn im Rahmen einer strafrechtlichen Untersuchung eine richterliche Anordnung oder die Anordnung eines Staatsanwalts nach der span. Strafprozessordnung vorliegt. Dieses Instrument wird nach Expertenaussagen kaum eingesetzt, vielmehr werden bei Bedarf Echtzeit-Überwachungsmaßnahmen durchgeführt.

7.4 Praxis der Datenspeicherung für unternehmenseigene Zwecke

Die Praxis der Datenspeicherung für unternehmenseigene Zwecke erfolgt auf den gesetzlichen Grundlagen. Um welche Datentypen es sich im Einzelnen handelt, bleibt den jeweiligen Unternehmen überlassen.

Ley 32/2003 (Span. TKG)

Die im Zusammenhang mit der Speicherung für Werbezwecke relevanten Bestimmungen des Ley 32/2003 lauten zusammengefasst wie folgt:

- Teilnehmer haben das Recht, dass ihre Verbindungsdaten unverzüglich anonymisiert oder gelöscht werden, wenn sie nicht mehr für die Übertragung der Kommunikation benötigt werden (Art. 38, Abs. 3a, Satz 1).

- Bestandsdaten, die für Billing oder Interconnection benötigt werden, dürfen gespeichert werden, so lange gegen Rechnungen in diesem Zusammenhang Einspruch eingelegt werden darf (Art. 38, Abs. 3a, Satz 2).

- Verbindungsdaten der Teilnehmer dürfen nur dann für Werbezwecke genutzt werden, wenn der Teilnehmer darüber informiert wurde und dazu sein Einverständnis gegeben hat (opt-in) (Art. 38, Abs. 3b).

- Standortdaten dürfen nur dann verarbeitet werden, wenn sie anonymisiert sind oder wenn der Teilnehmer eingewilligt hat (opt-in) und die Daten nur für den Zweck und die Dauer des jeweiligen Services übertragen werden (Art. 38, Abs. 3d).

- Alle oben genannten Regelungen gelten sinngemäß auch für die Nutzer eines Anschlusses (Art. 38, Abs. 4).

- Die Datenschutzregelungen bezüglich Standortdaten gelten nicht, soweit sie Notrufe betreffen (Art. 38, Abs. 5).

- Die Bestimmungen des LSSI bleiben durch Art. 38, Abs. 3a unberührt (Art. 38, Abs. 5 Satz 3).[37]

Real Decreto 1736/1998

Verkehrs- und Rechnungsdaten dürfen so lange gespeichert werden, wie es für Zwecke der Rechnungstellung notwendig ist (z.B. dürfen die Daten, wenn die Rechnung strittig ist, so lange aufbewahrt werden, wie es zur Klärung notwendig ist).

Die maximal gestattete Speicherdauer beträgt somit 5 Jahre (Einspruchsfrist).

Folgende Daten dürfen gespeichert werden (Art. 65):

- Die Nummer oder die Kennung des Subscribers.

- Die Adresse des Subscribers sowie die Art des Endgeräts.

- Die Gesamtzahl der Tarifeinheiten, die berechnet werden.

- Die Nummer des Angerufenen.

- Die Art, der Zeitpunkt des Beginns und die Dauer des Anrufs bzw. das übertragene Datenvolumen.

- Das Datum des Anrufs oder Services.

- Andere rechnungsrelevante Daten, wie etwa Art der Zahlung (Einzugsermächtigung u.ä.).

LSSI

Es ist nach Art. 21 Abs. 1 LSSI grundsätzlich verboten, ohne Einverständnis des Teilnehmers E-Mail oder andere elektronische Nachrichten für Werbezwecke zu versenden (opt-in Prinzip).

---

37 Das LSSI enthält nähere Bestimmungen für die Verwendung von Daten für Werbezwecke (s.u.).

Allerdings gibt es eine Ausnahmeregelung für den Fall, dass der Teilnehmer eine Vertragsbeziehung mit dem Unternehmen eingegangen ist (Art. 21 Abs. 2). Unter dieser Voraussetzung darf das Unternehmen die Kontaktdaten, die im Rahmen des Vertragsverhältnisses erhoben werden, für Werbezwecke nutzen, die ähnliche Services zum Gegenstand haben.

Dieser Nutzung seiner Daten muss der Kunde aber jederzeit widersprechen können.

Massenaussendungen von „unsolicited E-Mail“ („Spam“) oder von anderen Kommunikationsdiensten sind somit verboten, werden als „schwerwiegende“ Verstöße eingestuft und entsprechend geahndet (Art. 38). Die spanische Datenschutzbehörde besitzt die Kompetenz, Sanktionen bei Verstößen zu erlassen.

7.5 Ausgestaltung des Zugriffs der berechtigten Stellen

Zu den berechtigten Stellen, die Vorratsdaten anfordern dürfen, zählen laut LSSI Art. 12 Behörden, die im Rahmen eines Strafprozesses, der Aufrechterhaltung der öffentlichen Sicherheit sowie der Gewährleistung der nationalen Sicherheit auf die Vorratsdaten zugreifen müssen. Dieses sind

- Gerichte,
- Staatsanwälte,
- das Finanzministerium.

Die Polizeien sind berechtigt, unter Berücksichtigung der allgemeinen Datenschutzgesetzgebung LOPD auf die Vorratsdaten nach Bedarf der og. Behörden zuzugreifen. Eine richterliche Anordnung wie sie bei Echtzeit-Überwachung notwendig ist, ist zum Erhalt der Daten nicht zwingend erforderlich. In der Praxis wird dies unterschiedlich gehandhabt.

Ein festgelegtes formales Vorgehen für die Anforderung der Daten existiert nicht. Eine schriftliche Anfrage gegenüber dem TK-Anbieter ist nicht unbedingt erforderlich. Üblicherweise werden Anfragen per Fax und Telefon abgewickelt.

7.6 Kostenentschädigung

7.6.1 Rechtliche Grundlagen

Es existieren keine rechtlichen Grundlagen, nach denen den TK-Unternehmen die Kosten der Vorratsdatenspeicherung erstattet werden.

Diese Regelung entspricht der Kostenentschädigungsregelung bei Echtzeit-Überwachung. Nach Art. 33 des spanischen TKG müssen die TK-Anbieter Maßnahmen, die durch die Strafprozessordnung zum Abhören der Telekommunikation gefordert werden sowie Maßnahmen, die die Überwachungsbefugnisse der Nachrichtendienste betreffen, auf eigene Kosten realisieren (Ley 32/2003 Art. 33).

Auch im Rahmen der Bestimmungen des LSSI wird zwar eine Kostenentschädigung von den Unternehmen gefordert, es ist jedoch bisher nichts in dieser Richtung vorgesehen.

7.6.2 Abwicklungsprozess

nicht zutreffend

7.6.3 Höhe der Kostenentschädigung

nicht zutreffend

7.7 Besonderheiten und aktuelle Entwicklungen

In Spanien steht der zuständige Verordnungsgeber, das Industrieministerium (Ministerio de Industria, Turismo y Comercio), vor der Herausforderung, die im LSSI angekündigte Verordnung zu Vorratsdatenspeicherung zu entwerfen, die die Anforderungen an die TK-Anbieter im Detail festlegt. Bisher liegt noch nichts diesbezüglich vor.

Der Protest der Internet-Community gegen das Vorratsdatenspeicherungs-Gesetz LSSI kumulierte Ende 2002 in der Verleihung des „Big-Brother-Awards“ an die damalige spanische Regierung. Diskussionen um Datenschutz und Vorratsdatenspeicherung werden in der spanischen Öffentlichkeit sehr intensiv und kontrovers diskutiert.

Die spanische Datenschutzbehörde AGD verfügt über Kontroll- und Sanktionsbefugnisse. Bei schweren Verstößen gegen den Datenschutz können gegen Unternehmen Geldstrafen von bis zu 600.000 Euro verhängt werden.[38] Die Namen der Empfänger von Strafbescheiden sowie die Höhe der Strafe werden veröffentlicht. Die Behörde kann selbst aktiv die Datenschutzpraxis von Unternehmen und Behörden untersuchen oder Beschwerden nachgehen. Datenschutzbeauftragte in Organisationen sind nicht vorgeschrieben.

---

38 Die Refinanzierung der Behörde erfolgt u.a. aus den Einnahmen aus Strafgebühren.

8 United Kingdom

8.1 Gesetzliche Grundlagen

8.1.1 Gesetzliche Grundlagen für Vorratsdatenspeicherung zum Zweck der Strafverfolgung

Zurzeit existiert zwar eine gesetzliche Verpflichtung für TK-Anbieter, Bestandsdaten und Verkehrsdaten für Zwecke der nationalen Sicherheit zu speichern, die Speicherung erfolgt aber in der Praxis auf Basis einer freiwilligen Vereinbarung zwischen TK-Industrie und Home Office.[39]

Ein erster Schritt zur Regelung von Vorratsdatenspeicherung im Vereinigten Königreich war das im Jahr 2000 verabschiedete Gesetz über Ermittlungsbefugnisse der Strafverfolgungsbehörden und Nachrichtendienste

- Regulation of Investigatory Powers Act 2000

kurz RIPA genannt. Part I Chapter II „Acquisition and Disclosure of Communications Data“ legt die Gewinnung und Weitergabe von „communications data“, d.h. Verbindungsdaten und Standortdaten über die ein TK-Anbieter (ohnehin) verfügt, für die berechtigten Stellen fest. Dieser Teil des Gesetzes stellte den umstrittensten dar. Er ist daher mit einer erheblichen Zeitverzögerung in Kraft getreten.

Besonders kontrovers wurde die Ausweitung der Befugnisse im Bereich der Datengewinnung diskutiert, insbesondere was die Anzahl der berechtigten Stellen angeht. Neben den Strafverfolgungsbehörden können auch zahlreiche kommunale Behörden sowie andere Behörden mit Sicherheitsaufgaben (Feuerwehren etc.) Zugriff auf verschiedene Datentypen, je nach Befugnissen der spezifischen Behörden, erhalten.

Die eigentlichen Bestimmungen zu Vorratsdatenspeicherung für Strafverfolgungszwecke finden sich im ein Jahr später verabschiedeten

- Anti-Terrorism, Crime And Security Act 2001

bekannt unter dem Kürzel ATCSA. Beide Gesetze liegen im Zuständigkeitsbereich des Innenministers (Secretary of State for the Home Department).

---

39 Für das Verständnis dieser Regelungsweise ist zu berücksichtigen, dass das „Common Law“ in UK sich von den Rechtssystemen im übrigen Europa prinzipiell unterscheidet. Im Gegensatz zu z.B. Frankreich, Deutschland oder Spanien gibt es in UK keine kodifizierte Verfassung oder ein Grundgesetz. Das sog. Fallrecht in UK weist nicht die in diesen Ländern übliche hierarchische Struktur auf.

Das ATCSA beinhaltet - neben zahlreichen anderen Artikeln zu verschiedenen Aspekten der Terrorismusbekämpfung - Bestimmungen zu Auskunftsersuchen und zu Vorratsdatenspeicherung:

- Part 3 Disclosure of Information,[40]

- Part 11 Retention of Communications Data.

Die näheren Bestimmungen zu Part 11 werden in einer Verordnung (Code of Practice) des Home Office festgelegt (Part 11, Sec. 102 (1)):

- Retention of Communications Data (Code of Practice) Order 2003, Explanatory Memorandum and Code of Practice

Die Einhaltung der im „Code of Practice" festgehaltenen Vorratsdatenspeicherungs-Bestimmungen geschieht auf freiwilliger Basis.[41]

Ein Review des Anti-Terrorismus-Gesetzes wurde bereits im Frühjahr 2002 vom Home Secretary initiiert. Das Privy Counsellor Review Committee legte im Dezember 2003 dem Parlament den entsprechenden Bericht vor.[42]

Das Komitee schlägt in Bezug auf Part 11 (Data Retention[43]) vor,

- eine Mindestspeicherfrist für Verkehrsdaten in der allgemeinen Gesetzgebung festzulegen und nicht, wie geschehen, in einem spezifischen Anti-Terrorismus-Gesetz,[44]

- Part 11 ATCSA durch ein allgemeines Vorratsdatenspeicherungs-Gesetz zu ersetzen, in dem die Maximalspeicherfrist auf ein Jahr festgelegt wird,

- dem Information Commissioner[45] die Kompetenz für die Kontrolle der Vorratsdatenspeicherungs-Regelungen, inklusive der entsprechenden Regelungen des RIPA, zu übertragen,

- eine Regelung zu Data Preservation (im Sinne einer Verhinderung der Anonymisierung von „communications data") in Ergänzung zur Vorratsdatenspeicherung einzuführen.

---

40 Gemeint sind z.B. Auskünfte zu Adressen, Telefonnummern etc.
41 Retention of communications data under Part 11: Anti-Terrorism, Crime & Security Act 2001, Voluntary Code of Practice
42 Privy Counsellor Review Committee (2003): Anti-terrorism, Crime and Security Act 2001 Review: Report, Presented to Parliament pursuant to Section 122(5) of the Anti-terrorism, Crime and Security Act 2001, Ordered by The House of Commons to be printed 18th December 2003
43 Engl. Begriff für Vorratsdatenspeicherung.
44 Strenggenommen kann nach ATCSA Data Retention (Vorratsdatenspeicherung) nur für Zwecke der nationalen Sicherheit erfolgen, der Fall der Strafverfolgung wird nicht explizit erwähnt.
45 Der unabhängige Information Commissioner ist für den Datenschutz zuständig.

Das Komitee schlägt in Bezug auf Part 3 (Disclosure of Information) vor,

- Kontrollen einzuführen,
- die interne Autorisierung von Datenabfragen zu vereinfachen.

Fazit

Es existiert zwar eine gesetzliche Grundlage zu Vorratsdatenspeicherung in Form des ATCSA und einer entsprechenden Verordnung, die Praxis beruht aber auf Freiwilligkeit. Die Vorratsdatenspeicherungs-Regelungen sind erst seit Anfang 2004 in der Praxis wirksam.

Intention dieser freiwilligen Vereinbarung ist, dass die Unternehmen allein zur Speicherung derjenigen Datentypen veranlasst werden, die diese bereits zu unternehmenseigenen Zwecken vorhalten. Der Umfang an Datentypen soll durch den Voluntary Code of Practice nicht erweitert werden, allein die Speicherdauer soll ausgeweitet werden.

Inwieweit Vorratsdatenspeicherung auf „freiwilliger Basis“ funktioniert, ist aufgrund mangelnder Erfahrung noch unklar und unterliegt darüber hinaus der Geheimhaltung. Ob und wieviele CSP im März 2004 die freiwillige Vereinbarung unterzeichnet haben, bleibt unklar. Das Home Office erklärt, diese Informationen unterlägen der Geheimhaltung. Die Aussagen von Unternehmensvertretern deuten darauf hin, dass die Bereitschaft der TK-Anbieter zur Kooperation vorhanden ist, es bestehe aber Uneinigkeit darüber, ob eine freiwillige Vereinbarung oder eine formale Verordnung vorteilhafter sei.

8.1.2 Gesetzliche Grundlagen für anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung

Data Preservation bzw. Data Freeze erfolgt auf freiwilliger Basis durch die TK-Anbieter. Data Preservation kann, so eine häufige Interpretation von Rechtsexperten, auf Basis des RIPA Part 1 Chapter II von den Strafverfolgungsbehörden verlangt werden.

8.1.3 Gesetzliche Grundlagen der Datenspeicherung für unternehmenseigene Zwecke

Das Parlament hat die EU-Direktive 2002/58/EC nahezu unverändert im „The Privacy and Electronic Communications (EC Directive) Regulations 2003“ übernommen (S.I. 2003 number 2426, amended by S.I. 2004 number 1039 (The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004)). Dieses Datenschutzgesetz bildet die Grundlage für das Speichern von Daten für Marketing- und Abrechnungszwecke.

8.2 Praxis der Vorratsdatenspeicherung

8.2.1 Art, Umfang und Dauer

Es existieren keine spezifischen Anforderungen an die Analyse und Aufbereitung der Daten. Es sollen nur die ohnehin beim TK-Anbieter vorhandenen Datensätze, für einen längeren Zeitraum als für Unternehmenszwecke üblich, für die Abfrage der LEAs bereitgehalten werden.

Grundsätzlich muss eine Anfrage nach Bestands- und Verkehrsdaten verhältnismäßig und notwendig für den jeweiligen Zweck der Strafverfolgung sein. Die Formulierung der Anfrage ist detailliert zu gestalten (z.B. „Auflistung aller Anrufe an Telefonnummer x zwischen Datum – Uhrzeit y und z, mit Anrufernummer und Dauer“). Der TK-Anbieter darf *nur diese* angeforderte Information aus seinen Daten extrahieren und weitergeben.

Zugang zu Computerdateien und Programmen muss nur in der Weise gewährt werden, wie der Zugang zu den jeweiligen Endgeräten möglich war. Dies wird in der Praxis dahingehend interpretiert, dass bei URLs der Hostname oder die Host IP Adresse ausreichend ist, ohne Port Nummer oder Pfad-Angabe.

Der Voluntary Code of Practice gestattet es den TK-Anbietern grundsätzlich, „communications data“ (d.h. alle Daten, außer Inhalte) zu speichern. Es sollen nur die Datenarten gespeichert werden, die die Unternehmen ohnehin vorhalten. Für unterschiedliche Datenarten gelten dann unterschiedliche Fristen der Speicherung für Strafverfolgungszwecke und Zwecke der nationalen Sicherheit:

Tabelle 8-1: Zusammenfassung der wichtigste Datentypen für freiwillige Vorratsdatenspeicherung in UK (Art und Dauer)

Art der Daten	Dauer der Speicherung
Webaktivitäten (Logfiles):	max. 4 Tage
SMS, EMS, MMS, sonstige Internet-Daten:	max. 6 Monate
Telefon-Verbindungsdaten und Bestandsdaten:	max. 1 Jahr

Quelle: WIK-Consult Analyse

Tabelle 8-2 Vorratsdatenspeicherung (Art der Daten und Dauer) im Detail lt. Voluntary Code of Practice

SUBSCRIBER INFORMATION: 12 months
(From end of subscription/last change)
Subscriber details relating to the person
e.g. Name, date of birth, installation and billing address, payment methods, account/credit card details
Contact information (information held about the subscriber but not verified by the CSP)
e.g. Telephone number, email address
Identity of services subscribed to (information determined by the communication service provider)
Customer reference/account number, list of services subscribed to

Telephony:	telephone number(s), IMEI, IMSI(s)
Email:	email address(es), IP at registration
Instant messaging:	Internet Message Handle, IP at registration
ISP - dial-in:	Log-in, CLI at registration (if kept)
ISP - always-on:	Unique identifiers, MAC address (if kept), ADSL end points, IP tunnel address

TELEPHONY DATA: 12 months
All numbers (or other identifiers e.g. name@bt) associated with call (e.g. physical/presentational/network
assigned CLI, DNI, IMSI, IMEI, exchange/divert numbers)
Date and time of start of call
Duration of call/date and time of end of call
Type of call (if available)
Location data at start and/or end of call, in form of lat/long reference.
Cell site data from time cell ceases to be used.
IMSI/MSISDN/IMEI mappings.
For GPRS & 3G, date and time of connection, IMSI, IP address assigned.
Mobile data exchanged with foreign operators; IMSI & MSISDN, sets of GSM triples, sets of 3G quintuples, global titles of equipment communicating with or about the subscriber.
SMS, EMS and MMS DATA: 6 months
Calling number, IMEI
Called number, IMEI
Date and time of sending
Delivery receipt - if available
Location data when messages sent and received, in form of lat/long reference.
EMAIL DATA: 6 months
Log-on (authentication user name, date and time of log-in/log-off, IP address logged-in from)
Sent email (authentication user name, from/to/cc email addresses, date and time sent)
Received email (authentication user name, from/to email addresses, date and time received)
ISP DATA: 6 months
Log-on (authentication user name, date and time of log-in/log-off, IP address assigned)

Dial-up:	CLI and number dialled
Always-on:	ADSL end point/MAC address (If available)

WEB ACTIVITY LOGS: 4 days
Proxy server logs (date/time, IP address used, URL's visited, services)

The data types here will be restricted **solely to Communications Data and exclude content of communication.** This will mean that storage under this code can only take place to the level of www.homeoffice.gov.uk/…….
OTHER SERVICES: Retention relative to service provided
Instant Message Type Services (log-on/off time) If available.
COLLATERAL DATA: Retention relative to data to which it is related
Data needed to interpret other communications data.for example -the mapping between cellmast identifiers and their location –translation of dialling (as supported by IN networks)

Notes:
All times should include an indication of which time zone is being used (Universal Co-ordinated Time is preferred).
An indication should also be given of the accuracy of the timing.

Quelle: Home Office UK, Consultation on a Code of Practice for voluntary retention of communications data, March 2003

8.2.2 Kreis der Verpflichteten

Alle „public communications service provider“ (CSP) sind zur Unterstützung der berechtigten Stellen per Gesetz verpflichtet, also alle TK-Anbieter von TK-Dienstleistungen für die Öffentlichkeit.

Es ist zu unterscheiden erstens zwischen Interception (RIPA Part I Chapter I), also der Echtzeit-Überwachung, für die zahlreiche spezifische Anforderungen festgelegt wurden, zweitens Acquisition (Herausgabe) von „communications data“, die (ohnehin) beim TK-Anbieter vorhanden sind (RIPA Part I Chapter II) sowie drittens Vorratsdatenspeicherung nach ATCSA.

Für die beiden letzteren Bestimmungen gibt keine Ausnahmen und auch keine spezifischen, festgelegten Anforderungen hinsichtlich Hardware, Software oder Administration. Die Daten müssen in der Form weitergegeben werden, in der sie dem TK-Anbieter vorliegen.

8.2.3 Relevanz für Strafverfolgung und nationale Sicherheit

In UK stehen keine Studien, die Ergebnisse über die Relevanz von Vorratsdatenspeicherung enthalten, zur Verfügung. Zum Teil ist dies darauf zurückzuführen, dass entsprechende Maßnahmen erst seit Anfang 2004 durchgeführt werden.

8.3 Praxis der anlassbezogenen Datenspeicherung

Anlassbezogene Datenspeicherung erfolgt auf freiwilliger Basis, ebenso Data Freeze. Die Daten sind auf Anforderung nach RIPA in der Form weiterzugeben, in der sie beim TK-Anbieter vorliegen.

In der Praxis scheint Data Preservation kaum eine Rolle zu spielen. Grundsätzlich ist auch eine „Durchsuchung“ von z.B. Servern möglich, um Daten für Strafverfolgungszwecke zu erhalten.

Grundsätzlich ist es nach RIPA für einen dazu berechtigten Mitarbeiter einer LEA gestattet, Daten auf jede Art und Weise zu gewinnen bzw. Zugang zu diesen zu erlangen. Voraussetzung ist, dass die Schritte dazu verhältnismäßig und notwendig sind. Beispielsweise wäre ein Polizeibeamter dazu berechtigt, Daten von einem PBX (Private Branch Exchange) herunterzuladen, wenn der Betreiber dazu sein Einverständnis erklärt und selbst dazu nicht in der Lage ist (z.B. aufgrund mangelnder Qualifikation).

8.4 Praxis der Datenspeicherung für unternehmenseigene Zwecke

Anders als in einigen anderen Staaten enthalten die relevanten Vorschriften in UK keine Begrenzungen, für wie lange die Daten höchstens gespeichert werden dürfen, sondern nur allgemein die Vorgabe, dass Daten gelöscht werden müssen, sobald sie nicht mehr zu den beschriebenen Zwecken benötigt werden; d.h. grundsätzlich müssen auch in UK Daten, die nicht mehr für geschäftliche Zwecke erforderlich sind, unverzüglich anonymisiert oder gelöscht werden. In UK wird zwischen Traffic data (Verbindungsdaten), Location data (Standortdaten) und Subscriber data (Bestandsdaten) unterschieden.

Es sind Ausnahmebestimmungen in den Privacy and Electronic Communications (EC Directive) Regulations 2003 enthalten für TK-Netz –sowie Diensteanbieter sowie Teilnehmer in Bezug auf

- Verwendung von öffentlich verfügbaren communications services für Direktmarketing,
- unverlangte Direktwerbung (unsolicited direct marketing) via Telefon, Fax, E-Mail (Text/Video/Picture messaging und E-Mail) und via Automated Calling Systems.

Des Weiteren gibt es Bestimmungen, die nur TK-Netz –sowie Diensteanbieter betreffen zu den Bereichen:

- Verarbeitung von Verbindungsdaten,
- Standortdaten und Rechnungsdaten,

- Rufnummernidentifizierung,
- Teilnehmerverzeichnisse/Auskunft,
- Sicherheitsanforderungen und die Verwendung von “Cookies”.

Traffic data dürfen solange gespeichert werden, wie es für das technische Bereitstellen des Service sowie für die Rechnungstellung notwendig ist. Traffic data sind definiert als Daten, die das Routing, die Dauer oder den Zeitpunkt einer Kommunikation betreffen.

Das bedeutet, dass die Daten unverzüglich gelöscht werden müssen, wenn sie nicht für die Rechnungstellung benötigt werden. Traffic data für Rechnungszwecke dürfen so lange gespeichert werden, wie es nach allgemeinem Vertragsrecht möglich ist, Einspruch gegen die Rechnung einzulegen. Die Speicherfrist beträgt somit 6 Jahre (zzgl. Dauer der Streitschlichtung, falls notwendig).

Traffic data dürfen für Marketingzwecke des Providers verwendet werden, wenn der Teilnehmer zugestimmt hat. Dasselbe gilt für die Weitergabe der Daten an Dritte (opt-in-Prinzip).

Location data dürfen gespeichert werden, wenn entweder der Teilnehmer aus den Daten nicht erkennbar ist oder wenn er der Speicherung für Zwecke der spezifischen Dienstleistung zugestimmt hat.

Subscriber data dürfen gespeichert und für Marketing-Zwecke verwendet werden. Der Datenschutz im Vereinigten Königreich basiert dabei prinzipiell auf dem „opt-out“-Prinzip, d.h. z.B. eine E-Mail-Adresse darf für Direktwerbung genutzt werden, wenn sie dem Unternehmen im Zusammenhang mit einem Einkauf/Verkaufsverhandlungen bekannt wurde. Ein „opt-in“ ist dann nicht nötig. Personen, die keine Werbesendungen per Post/E-Mail, Telefon oder Fax wünschen, können sich auch bei der Datenschutzbehörde registrieren lassen (vergleichbar mit „Robinson-Listen“ in Deutschland). Direct Marketing, z.B. auch via Automated Calling Systems, wird in UK wesentlich intensiver von den Unternehmen genutzt als in Deutschland.

Unternehmen kritisieren, dass in der Praxis die unterschiedlichen Bestimmungen für Datenschutz und Vorratsdatenspeicherung dazu führen können, dass beispielsweise von über 80 anfallenden Datensätzen für einen Kommunikationsvorgang im Mobilfunk nur 6 Datensätze lt. Voluntary Code of Practice gespeichert werden müssen, alle übrigen sind zu löschen. Diese unterschiedlichen Anforderungen werden von den Unternehmen als äußerst aufwendig bewertet.

8.5 Ausgestaltung des Zugriffs der berechtigten Stellen

Es wird geschätzt, dass jährlich rund 500.000 Anfragen von den berechtigten Stellen gestellt werden. Da die derzeitige Regelung jedoch erst seit 2004 besteht, sind keine aktuellen Zahlen verfügbar.

Folgende Anfragen werden typischerweise gestellt:

- Identifikation eines Teilnehmers auf Basis von Telefonnummer, E-Mail-Adresse, Website, IP-Adresse (unter Datum/Zeitangabe wg. dynamischer IP-Adressen),
- Auflistung aller Anrufe an/von einem bestimmten Anschluss.

Die Verkehrsdatengewinnung gemäß RIPA Part I Chapter II ist zu folgenden Zwecken zu ermöglichen:

- im Interesse der nationalen Sicherheit,
- zum Schutz vor bzw. zur Aufdeckung von schweren Straftaten oder Aufruhr,
- im Interesse des wirtschaftlichen Wohlergehens des Vereinigten Königreichs,
- im Interesse der öffentlichen Sicherheit,
- im Interesse der öffentlichen Gesundheit,
- zum Zweck des Festsetzens oder Kassierens von Steuern, Zoll, Abgaben o.ä.,
- für jeden weiteren Fall, der den Zielen der o.g. Punkte entspricht, wenn dies vom zuständigen Minister angeordnet wird.

Nach dem ATCSA können vorhandene Daten aus zwei Gründen von berechtigten Stellen angefordert werden:

- zur Gewährleistung der nationalen Sicherheit im Allgemeinen,
- zum Zweck des Schutzes oder der Aufdeckung von Straftaten bzw. die Entdeckung von Straftätern die im Zusammenhang mit der Gefährdung der nationalen Sicherheit stehen.

Letzteres bedeutet streng interpretiert, dass eine Verwendung von Daten aus Vorratsdatenspeicherung für Strafverfolgungszwecke nicht gestattet ist. Dieser Punkt ist in UK umstritten und bedarf noch der juristischen Klarstellung.

Im Vereinigten Königreich sind zahlreiche Stellen befugt, Daten, die im Rahmen einer Vorratsdatenspeicherung gespeichert wurden, abzurufen. Die Kompetenz dazu wird nach zwei Kriterien festgelegt: Erstens nach dem Rang des jeweiligen Vertreters der

Behörde, der diese Daten abrufen darf und zweitens nach dem Anlass, für den die jeweiligen Daten abgerufen werden dürfen (Katalog nach 22 (2)). Die Stellen sind in der entsprechenden Verordnung tabellarisch aufgelistet.[46] Auf eine detaillierte Auflistung der unterschiedlichen Kompetenzen kann an dieser Stelle verzichtet werden. Die Genehmigung zur Datenabfrage erfolgt aufgrund einer Autorisierung durch ranghohe Vertreter der jeweiligen Behörde oder Institution. Die TK-Anbieter erhalten dann eine Mitteilung („Notice") über die herauszugebenden Daten.

Das Verfahren folgt einer SPoC-Policy (Single Point of Contact). Das heißt, jede abfrageberechtigte Organisation hat einen Kontakt zu benennen. Diese Personen müssen eine bestimmte Schulung durchlaufen haben, die sie befähigt, „Accredited Officers" (AO) der jeweiligen Behörde oder Institution zu sein.[47] Nur AO dürfen die CSP in Bezug auf Vorratsdatenspeicherung kontaktieren. Der CSP kann anhand von Verifizierungsverfahren feststellen, ob der jeweils Anfragende dazu berechtigt ist.

Folgende Institutionen dürfen auf die Vorratsdaten bei den TK-Anbietern zugreifen:[48]

1. Folgende Polizeien und andere Strafverfolgungsbehörden sowie Nachrichtendienste besitzen umfassende Kompetenzen für den Zugriff auf alle „communications data" (RIPA 21 (4)

Police Forces:

- police forces in England and Wales outside London
- police force of Scotland
- The metropolitan police force
- The City of London police force
- The Police Service of Northern Ireland
- The Ministry of Defence Police
- The Royal Navy Regulating Branch
- The Royal Military Police
- The Royal Air Force Police
- The British Transport Police
- The National Criminal Intelligence Service
- The National Crime Squad
- The Commissioners of Customs and Excise
- The Commissioners of Inland Revenue

---

46 The Regulation of Investigatory Powers (Communications Data) Order 2003, Statutory Instrument 2003 No. 3172.

47 Die Schulungen werden von Dozenten der Polizei und der CSP gemeinsam durchgeführt.

48 Es wurde darauf verzichtet, die jeweils angegebenen gesetzlichen Grundlagen für die Kompetenzen dieser Institutionen hier zu zitieren.

The Intelligence Services:
- Government Communications Headquarters (GCHQ)
- The Security Service (z.B. MI5)
- The Secret Intelligence Service (z.B. MI6, SIS)

2. Folgende weitere Institutionen besitzen dieselben Zugriffsrechte:

- The Financial Services Authority
- The Scottish Crime Squad within the meaning of the Regulation of Investigatory Powers (Scotland) Act 2000
- The United Kingdom Atomic Energy Authority Constabulary
- The Department of Trade and industry
- The Office of the Police Ombudsman for Northern Ireland
- A National Health Service trust whose functions include the provision of emergency ambulance services
- The Welsh Ambulance Services NHS Trust
- The Scottish Ambulance Service Board
- The Northern Ireland Ambulance Service Health and Social Services Trust
- The Department for Transport
- Any fire authority
- Scottish councils
- Any joint Board of the Fire Services
- The Fire Authority for Northern Ireland

3. Folgende Institutionen dürfen keine Verbindungsdaten (Traffic data) im engeren Sinne abrufen, sondern nur alle anderen Daten, die bei der elektronischen Kommunikation entstehen (RIPA 21 (4) (b) (c):

- The Department of Trade and Industry
- A National Health Service Trust / emergency ambulance services
- The Welsh Ambulance Services NHS Trust
- The Scottish Ambulance Service Board
- The Northern Ireland Ambulance Service Health and Social Services Trust
- The Department for Transport
- Any fire authority

- Scottish councils
- Any joint Board of the Fire Services Act of Scotland
- The Fire Authority for Northern Ireland

4. Folgende weitere Institutionen dürfen keine Verbindungsdaten (Traffic data) im engeren Sinne abrufen, sondern nur alle anderen Daten, die bei der elektronischen Kommunikation entstehen (RIPA 21 (4) (b) (c):

- The Department for Environment, Food and Rural Affairs
- The Food Standards Agency
- The Department of Health
- The Home Office
- The Department of Enterprise, Trade and Investment for Northern Ireland
- Any county council or district council in England, a London borough council, the Common Council of the City of London in its capacity as a local authority, the Council of the Isles of Scilly, and any county council or county borough council in Wales
- district councils Northern Ireland
- The Counter Fraud and Security Management Service
- The Common Services Agency for the Scottish Health Service
- The Northern Ireland Health and Social Services Central Services Agency
- The Charity Commission
- The Environment Agency
- The Gaming Board for Great Britain
- The Health and Safety Executive
- The Information Commissioner
- The Office of Fair Trading
- The Serious Fraud Office
- The Scottish Environment Protection Agency
- Universal Postal Service Providers

8.6 Kostenentschädigung

8.6.1 Rechtliche Grundlagen

Nach ATCSA und auch nach dem Code of Practice ist eine Kostenentschädigung vorgesehen. Ob teilweise oder voll entschädigt wird, liegt im Ermessen der Regierung. Es ist zurzeit sowohl für die Öffentlichkeit als auch für die TK-Anbieter intransparent, ob und in welcher Höhe Entschädigungen gezahlt werden. Details sind im Gesetz nicht festgelegt. Da erst seit Anfang 2004 Vorratsdatenspeicherung durchgeführt wird, ist noch unklar, welche Entschädigungen gezahlt werden.

Nach RIPA Sec. 14 muss die Regierung einen angemessenen Beitrag zu den entstehenden Kosten leisten („fair contribution towards the costs incurred“).

8.6.2 Abwicklungsprozess

Die Kostenentschädigung wird durch die berechtigte Stelle, die die Daten abruft, nach Rechnungstellung im Einzelfall gezahlt.

8.6.3 Höhe der Kostenentschädigung

Angeblich hat die Regierung Mittel von 20 Mio. GBP für den Zeitraum von 2001 bis 2004 in den Haushalt eingestellt, um diese an TK-Unternehmen zur Entlastung für die erforderlichen Investitionen im Zusammenhang mit TKÜ- und Vorratsdatenspeicherpflichten zu verteilen. Es ist zurzeit unklar, nach welchen Kriterien diese Gelder beantragt werden können.

Im Bereich der TKÜ ist die Zahlung von Aufwandsentschädigungen eine seit langem geübte Praxis und die Unternehmen haben dazu jeweils Tariflisten mit den Behörden abgestimmt. Die Höhe der Zahlungen unterliegt der Geheimhaltung.

Um zu vermeiden, dass die TK-Anbieter mit der Unterstützung der Strafverfolgungsbehörden Gewinne erwirtschaften, existieren keine festen Gebühren- bzw. Entgeltverordnungen, sondern es werden Einzelfallentscheidungen vorgenommen. Dies wird, so vermuten die Unternehmen, auch im Bereich der Vorratsdatenspeicherung künftig der Fall sein.

Scheinbar werden Entschädigungen für die Vorratsdatenspeicherung heute in Aussicht gestellt, um die „freiwillige“ Speicherung für nicht-unternehmensrelevante Zwecke zu kompensieren. Es wird von manchen vermutet, dass Unternehmen die freiwillige Vereinbarung unterzeichnen werden, weil sie befürchten, sonst keine Entschädigung mehr zu erhalten, wenn die Speicherung verpflichtend wird.

8.7 Besonderheiten und aktuelle Entwicklungen

Die zu speichernden Datenkategorien für Strafverfolgungszwecke und die Gewährleistung der nationalen Sicherheit sind in einem freiwilligen Code of Practice festgelegt. Eine gesetzliche Grundlage für Vorratsdatenspeicherung fehlt noch, das Anti-Terrorismusgesetz ATCSA bezieht sich nur auf nationale Sicherheit. Das Datenschutzgesetz erfordert, dass Daten gelöscht werden, die nicht freiwillig gespeichert werden dürfen.

Bisher existiert keine schriftliche Zusage über Kostenentschädigungen für Vorratsdatenspeicherung an die CSP. Im Gegensatz zum Bereich Legal Interception ist somit die Kostenentschädigung bei Vorratsdatenspeicherung noch nicht abschließend geregelt.

Eine Besonderheit des Systems in UK ist, dass alle berechtigten Stellen ein Qualifizierungsprogramm durchlaufen und SPoC einrichten müssen. Dies trägt zu Prozesskosteneinsparungen sowohl auf Seiten der Behörden als auch auf Seiten der TK-Anbieter bei.

9 Österreich

9.1 Gesetzliche Grundlagen

9.1.1 Gesetzliche Grundlagen für Vorratsdatenspeicherung zum Zweck der Strafverfolgung

In Österreich gibt es wie in Deutschland keine Vorratsdatenspeicherung zum Zweck der Strafverfolgung und für die Gewährleistung der nationalen Sicherheit. Es existieren aber Bestimmungen, die die TK-Überwachung (Echtzeit für Inhalt und/oder Verkehrsdaten) sowie - unabhängig von TKÜ-Maßnahmen - die Rufdatenrückerfassung, also die Auswertung der bei den Unternehmen vorhandenen Verkehrsdaten, betreffen.

Das aktuelle, am 20. August 2003 in Kraft getretene österreichische TKG

- Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - TKG 2003) BGBl. I Nr. 70/2003)

regelt in § 94 „Technische Einrichtungen“ die Verpflichtungen der Anbieter und Betreiber bezüglich der Telekommunikationsüberwachung.

Grundlage der Befugnisse der Strafverfolgungsbehörden ist auch in Österreich die Strafprozessordnung, welche bestimmt, in welchen Fällen Telekommunikation überwacht werden darf (§ 149a bis 149p). Wie auch in anderen Staaten handelt es sich dabei ausnahmslos um Fälle, in denen Verdacht auf schwere Straftaten besteht. So ist etwa die Überwachung von Telefonen nur gestattet, um im Zusammenhang mit einer Straftat, für die mindestens ein Jahr Gefängnisstrafe verhängt werden kann, zu ermitteln. Bei Überwachungen anderer elektronischer Kommunikation oder Durchsuchungen von Computerspeichern muss es sich um Straftaten handeln, die mit mindestens 5 Jahren Gefängnis geahndet werden können.

Korrespondierend zum TKG wurde vom zuständigen Ministerium eine Überwachungsverordnung (ÜVO)

- Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung - ÜVO) BGBl. II Nr. 418/2001)

erlassen. Diese regelt die Gestaltung der technischen Einrichtungen zur Gewährleistung der Überwachung nach den Bestimmungen der StPO. Ergänzend hat das zuständige BMVIT auf Basis des ETSI-Standards ETSI TS 101 331 V1.1.1 technische Anforderungen formuliert, die im Ministerium zur Einsicht ausliegen.

9.1.2 Gesetzliche Grundlagen für anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung

Data Preservation ist nicht geregelt und findet somit nicht statt. Nach den og. gesetzlichen Grundlagen ist es den Strafverfolgungsbehörden möglich, eine Echtzeit-Überwachung der Verkehrsdaten mit richterlichem Beschluss durchzuführen.

9.1.3 Gesetzliche Grundlagen der Datenspeicherung für unternehmenseigene Zwecke

Die gesetzlichen Grundlagen für die Datenspeicherung finden sich wie in Deutschland in das TKG integriert. In der novellierten Fassung von 2003 handelt der Abschnitt 12 von Kommunikationsgeheimnis und Datenschutz.

Grundsätzlich dürfen nach Art. 96 TKG Bestandsdaten, Verkehrsdaten und Inhalte nur für Zwecke der Erbringung einer TK-Dienstes gespeichert werden.

Zur Verarbeitung der Daten für Marketingzwecke und Mehrwertdienste bedarf es der Zustimmung des Nutzers (opt-in). Der TK-Anbieter hat den Nutzer auf diese Möglichkeit entsprechend hinzuweisen.

9.2 Praxis der Vorratsdatenspeicherung

9.2.1 Art, Umfang und Dauer

nicht zutreffend

9.2.2 Kreis der Verpflichteten

Grundsätzlich sind alle Anbieter nach § 94 TKG zur Vorhaltung von Überwachungstechnik verpflichtet und auch dazu, gespeicherte Daten den Strafverfolgungsbehörden zugänglich zu machen. Ebenso müssen alle Betreiber, d.h. Unternehmen, die ein öffentliches Kommunikationsnetz oder eine zugehörige Einrichtung bereitstellen, an der Überwachung mitwirken. Für alle Unternehmen gilt, dass die Vorschriften der ÜVO sowie die technischen Detailvorschriften zu befolgen sind. In der Praxis ist derjenige Betreiber, der den Teilnehmeranschluss der zu überwachenden Person bereitstellt, in die Überwachung involviert.

9.2.3 Relevanz für Strafverfolgung und nationale Sicherheit

Erkenntnisse zur Relevanz der Auswertung von bei den Unternehmen gespeicherten Daten zum Zweck der Strafverfolgung liegen nicht vor. In Österreich wird jedoch, im Gegensatz zu anderen Ländern, die Rufdatenrückerfassung (Auswertung von gespeicherten Daten) im Rahmen von Anordnungen regelmäßig statistisch erfasst.[49] Für die Anzahl von Bestandsdatenabfragen liegen keine Statistiken vor.

Tabelle 9-1: Anzahl der Verfahren, in denen Rufdatenrückerfassung stattfindet, in Österreich (1997 – 2002)

Jahr	Verfahren	betroffene Anschlüsse	davon nur Rufdatenrückerfassung	davon Inhaltsüberwachung
1997	444	751	509	141
1998	493	804	617	k.A.
1999	496	1228	932	275
2000	759	1479	1069	410
2001	787	1721	1257	464
2002	993	2064	1423	641

Quelle: Himberger 2003 (Basis: Gerichtliche Kriminalstatistik Österreich/Österreichisches Statistisches Zentralamt)

9.3 Praxis der anlassbezogenen Datenspeicherung

Es gibt keine Vorschriften für das Data Preservation. Vielmehr werden bei Bedarf Echtzeit-Überwachungen für die direkte Übermittlung der Inhalte und/oder der Verkehrsdaten an die Strafverfolgungsbehörden geschaltet.

Die Bestimmungen der ÜVO bezüglich der elektronischen Übermittlung von Verkehrsdaten an die Strafverfolgungsbehörden treten erst zum 1. Januar 2005 in Kraft, so dass den Unternehmen noch eine Übergangszeit bleibt, um ihre Systeme anzupassen.

---

49 Vgl. auch Himberger, S. (2003): Fernmeldegeheimnis und Überwachung Schutzbereiche & Eingriffe – Durchführung & Kosten, Dissertation, Wien

9.4 Praxis der Datenspeicherung für unternehmenseigene Zwecke

Bestandsdaten dürfen nur für die Dauer des Vertragsverhältnisses gespeichert werden. Sie dürfen nur zu folgenden Zwecken verwendet werden:

- Vertragsabschluss/-beendigung, Durchführung, Änderung,
- Verrechnung der Entgelte,
- Erstellung des Teilnehmerverzeichnisses (mit den entsprechenden Wahlmöglichkeiten der Teilnehmer),
- Auskünfte an Notrufdienste.

Die Bestandsdaten dürfen für Marketingzwecke verwendet werden unter der Voraussetzung, dass der Teilnehmer zugestimmt hat. Die Verwendung ist auch bei Zustimmung des Teilnehmers „auf das erforderliche Maß und den zur Vermarktung erforderlichen Zeitraum“ zu beschränken.

Verkehrsdaten sind unverzüglich zu löschen, wenn sie nicht mehr für die Erbringung des Dienstes oder die Rechnungstellung benötigt werden. Für Rechnungszwecke ist die Speicherung solange zulässig, wie ein Einspruch gegen die Rechnung möglich ist. Verkehrsdaten dürfen nur mit Zustimmung des Teilnehmers für Marketing oder Dienste mit Zusatznutzen verwendet werden (opt-in).

9.5 Ausgestaltung des Zugriffs der berechtigten Stellen

Nach der österreichischen StPO ist ein Untersuchungsrichter zuständig für die Anordnung einer Rufdatenrückerfassung bzw. Feststellung der Position des Endgeräts. Die Polizeien führen die entsprechende Anordnung aus.

Die Anordnung ergeht schriftlich. Sie muß Namen und Anschrift des Betroffenen, gegen den sie sich richtet, und die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten. In ihr sind Art, Umfang und Dauer der Maßnahmen zu bestimmen.

9.6 Kostenentschädigung

9.6.1 Rechtliche Grundlagen

In Österreich hat ein Urteil des Verfassungsgerichts im Frühjahr 2003 einige Aufmerksamkeit auf sich gezogen. Danach ist die Reduzierung der Kostenentschädigung auf die Betriebskosten – in Österreich „Mitwirkungskosten“ genannt – unzulässig.

Mit Erkenntnis vom 27.2.2003, G 37/02 u.a., hat der österreichische Verfassungsgerichtshof (VfGH) entschieden, dass § 89 Abs. 1 letzter Satz TKG-alt[50] als verfassungswidrig aufgehoben wird; die Aufhebung wäre am 31.12.2003 in Kraft getreten, wurde jedoch durch die Verabschiedung der geänderten Regelung im § 94 TKG hinfällig.

In der Sache begründete der VfGH seine Entscheidung damit, dass zwar eine Rechtfertigung der Inpflichtnahme privater Betreiber von Telekommunikationsdiensten für die Überwachungsverpflichtung bestehe; jedoch ein Verstoß der Verpflichtung zur kostenlosen Bereitstellung von Einrichtungen zur Überwachung des Fernmeldeverkehrs gegen den Gleichheitssatz mangels Berücksichtigung des Verhältnismäßigkeitsgrundsatzes durch den Gesetzgeber vorliege (RS VfGH Erkenntnis 2003/02/27 G 37/02 u.a., V 42/02 u.a.):

„Leitsatz: Zulässigkeit der Individualanträge von Mobilfunk- und Festnetzbetreibern auf Aufhebung der im Telekommunikationsgesetz normierten Verpflichtung zur kostenlosen Bereitstellung von Einrichtungen zur Überwachung des Fernmeldeverkehrs nach den Bestimmungen der StPO; sachliche Rechtfertigung der Inpflichtnahme privater Betreiber von Telekommunikationsdiensten für die Überwachungsverpflichtung; jedoch Verstoß der Kostentragungsregelung gegen den Gleichheitssatz mangels Berücksichtigung des Verhältnismäßigkeitsgrundsatzes durch den Gesetzgeber."

In Reaktion auf das Urteil wurde im Rahmen der Gesetzesnovellierung der § 94 TKG anders gefasst. Der Satz *„Diese Verpflichtung begründet keinen Anspruch auf Kostenersatz"* in § 89 Abs. 1 TKG-alt wurde ersatzlos gestrichen. § 89 Abs. 2 wurde ergänzt durch die Maßgabe, dass das Justizministerium nunmehr im Einvernehmen mit dem BMVIT, dem Finanzministerium, dem Innenministerium und dem Verteidigungsministerium einen *„angemessenen Kostenersatz vorzusehen"* habe. Dabei sei *„insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, Bedacht zu nehmen."*

Entsprechend wurde vom österreichischen Bundesministerium für Justiz eine Verordnung erlassen, die die Gebührensätze für die Kostenentschädigung enthält.

Am 12. August 2004, mit BGBl. II Nr. 322/2004 wurde die

- Verordnung der Bundesministerin für Justiz über den Ersatz der Kosten der Betreiber für die Mitwirkung an der Überwachung einer Telekommunikation (Überwachungskostenverordnung - ÜKVO)

---

50 Die Vorgängerbestimmung lautete: *Technische Einrichtungen § 89. (1) Der Betreiber ist nach Maßgabe einer gemäß Abs3 erlassenen Verordnung verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung des Fernmeldeverkehrs nach den Bestimmungen der StPO erforderlich sind. Diese Verpflichtung begründet keinen Anspruch auf Kostenersatz. (2) Der Betreiber ist verpflichtet, an der Überwachung des Fernmeldeverkehrs nach den Bestimmungen der StPO im erforderlichen Ausmaß mitzuwirken. Hiefür gebührt ihm der Ersatz der angemessenen Kosten.*

veröffentlicht, welche am 1. September 2004 in Kraft getreten ist.

Die Verordnung wurde vorab mit den Interessensgruppen, namentlich dem Fachverband der Telekommunikations- und Rundfunkunternehmungen eingehend diskutiert. Der Verband hat 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.

Nunmehr regelt die ÜKVO die Kostenentschädigung nach folgendem Prinzip:

§ 3. (1) Der Umfang des Ersatzes richtet sich nach den Kosten (Personal- und Sachaufwendungen), die dem Betreiber durch die Erfüllung des gerichtlichen Auftrags notwendigerweise entstanden sind (§ 1 Abs. 2). Er ist nach den Bestimmungen des 2. Abschnitts zu bestimmen.

9.6.2 Abwicklungsprozess

Das Abrechnungsverfahren in Österreich ist wie in Deutschland aufwändig für die Unternehmen gestaltet. Die Rechnungstellung erfolgt dezentral, d.h. jedes Unternehmen muss im Einzelfall eine Rechnung an das jeweilige Gericht, vor dem die Beweisaufnahme stattgefunden hat, stellen. Dieses entscheidet von Fall zu Fall über die Höhe der Kostenentschädigung.

Insgesamt erscheint das Verfahren sowohl den Unternehmen als auch den Gerichten zu kostenintensiv. Die Behörden und Unternehmen wünschen sich ein standardisiertes System.

9.6.3 Höhe der Kostenentschädigung

Entschädigungsfähig sind nach der ÜKVO

- Personalkosten,
- Übertragung an die Untersuchungsbehörden,
- Transportkosten für Geräte (wenn für eine Überwachungsmaßnahme eigens Geräte installiert werden müssen),
- Administrationskosten („Sekretariatspauschale“).

In der Praxis bedeutet dies, dass die Betriebskosten in Form von Personalkosten für die Dauer der Durchführung einer Überwachung geltend gemacht werden können sowie Transportkosten im Zusammenhang mit einer Überwachung. Gemeinkosten können als Pauschale pro Anordnung entschädigt werden. Nicht berücksichtigt sind Kapitalkosten.

Die Entschädigungssätze nach ÜKVO Abschnitt 2 sind in Bezug auf die Rufdatenrückerfassung wie folgt festgelegt:

Tabelle 9-2: Höhe der Entschädigungszahlungen an TK-Anbieter in Österreich für Rufdatenrückerfassungen

Art der Dienstleistung	Höhe der Entschädigung (zzgl. Umsatzsteuer, in Euro)
für eine Ermittlung von historischen Standortdaten bei zustande gekommenen Verbindungen	
a) Einrichtung (einmalig)	64,00
b) Auswertung pro überwachten Tag	06,50
für die Ermittlung von historischen Vermittlungsdaten auf Basis der Rufnummer, IMEI- Nummer oder IMSI- Nummer	
a) Einrichtung	64,00
b) Auswertung pro überwachten Tag	06,50
c) Zusätzliche Ermittlung einer verwendeten IMEI- Nummer (im Mobilnetz)	60,00
Ermittlung von Rufnummern auf Basis von IMEI- oder IMSI-Nummern (Datenrasterung)	60,00
Bekanntgabe des PUK- Codes (Ermittlung und Weiterleitung)	32,00
Sekretariatspauschale (Kosten für die Aufbereitung und Übermittlung der Daten, sofern diese nicht bereits in den vorhergehenden Tarifansätzen umfasst sind, sowie für die Herstellung sonstiger Unterlagen und Kostennoten.	
pro Beschluss	15,20
pro Ergänzungsbeschluss	05,60
Transport von Zusatzgeräten	Kosten für die Nutzung eines Kraftfahrzeuges nach § 10 Abs. 3 der Reisegebührenvorschrift 1955, BGBl. Nr. 133

Quelle: ÜKVO

Für Leistungen an Samstagen, Sonntagen und gesetzlichen Feiertagen sowie an Werktagen zwischen 22.00 und 6.00 Uhr erhält der Betreiber einen Zuschlag von 100% für die enthaltenen Personalkosten, es sei denn, dass die Leistungen ohne Nachteil für die Überwachung auch zu einem anderen Zeitpunkt hätten erbracht werden können.

Das Justizministerium hat die Pflicht, Entwicklung der Kosten nach den Bestimmungen der Verordnung in „angemessenen Abständen“ zu überprüfen und im Fall einer maßgeblichen Veränderung der Kostenstrukturen und Kostenfaktoren eine Anpassung für das folgende Kalenderjahr vorzunehmen.

9.7 Besonderheiten und aktuelle Entwicklungen

Grundsätzlich hat der im WKO (Wirtschaftskammer Österreich) organisierte Fachverband der Telekommunikations- und Rundfunkunternehmungen die Einbindung der im Fachverband vertretenen Netzbetreiber im Vorfeld der Begutachtung des ÜKVO-Entwurfs durch das Justizministerium begrüßt.

Positiv wurde außerdem angemerkt, dass sich der Entwurf in weiten Teilen an den Vorschlag des Fachverbandes für eine Überwachungskostenverordnung anlehnt hat. Trotzdem wurde massive Kritik an der Höhe der Gebührensätze und zum Teil auch an der Tarifstruktur geübt.

Immerhin konnte der Verband erreichen, dass über eine Entschädigung der Kapitalkosten gesondert mit den zuständigen Ministerien (u.a. Justiz, Innen) verhandelt wird. In welcher Form diese dann ggf. festgelegt wird (Änderung der bestehenden Verordnung bzw. neue Verordnung oder andere Regelungsart) ist noch offen.

10 USA

10.1 Gesetzliche Grundlagen

10.1.1 Gesetzliche Grundlagen für Vorratsdatenspeicherung zum Zweck der Strafverfolgung

In den USA gibt es keine gesetzliche Verpflichtung zur Vorratsdatenspeicherung. Während der Debatte um den sog. „ USA Patriot Act“ als Reaktion auf die Terrorangriffe von 2001 wurde die vollständige Vorratsdatenspeicherung mehrmals vom US Congress abgelehnt. In diese Entscheidung floss zum einen die Überlegung ein, dass durch Vorratsspeicherung die verfassungsmäßigen Bürgerrechte unverhältnismäßig eingeschränkt würden und zum anderen sollten den Unternehmen keine unnötigen Kosten auferlegt werden.[51]

Statt eine Speicherung der Daten aller Nutzer vorzuschreiben, entschied sich der Gesetzgeber aus den genannten Gründen dazu, nur die Verkehrsdaten von verdächtigen Personen auf Anordnung durch die Strafverfolgungsbehörden speichern zu lassen, d.h. eine Politik der anlassbezogenen Datenspeicherung zu verfolgen.

Zudem besitzen die Strafverfolgungsbehörden die Möglichkeit, alle in den Unternehmen gespeicherten Daten abzufragen.[52] Hierbei kommt den Behörden der Umstand zu Hilfe, dass die Privatwirtschaft in der Regel die Bestands- und Verkehrsdaten für ihre Zwecke in großem Umfang speichern darf, da sie keinen Einschränkungen durch Datenschutzgesetze unterliegt.

10.1.2 Gesetzliche Grundlagen für anlassbezogene Datenspeicherung zum Zweck der Strafverfolgung

Bei der anlassbezogenen Datenspeicherung wird in den USA unterschieden zwischen einerseits dem behördlichen Zugriff auf Daten, die bei den Netzbetreibern und Providern aus betrieblichen Gründen gespeichert werden und andererseits dem Zugriff auf Verkehrsdaten, die durch spezielle Überwachungsgeräte bzw. –prozesse im Bedarfsfall generiert werden.

Die gesetzlichen Grundlagen für ersteren Fall, also die staatliche Anforderung der vorhandenen Bestands- und Verkehrsdaten finden sich in Title 18 United States Code

---

51 Vgl. AMCHAM EU (2003): Position Paper on Data Retention in the EU, 4. Juni, S. 4.

52 Dieser Zugriff auf persönliche Daten gilt nicht nur für Telekommunikationsunternehmen, sondern wurde im Rahmen des Patriot Act für alle Unternehmen mit Kundendatenbanken ermöglicht.

(USC) („Crimes and Criminal Procedure"), im Chapter 121 („Stored Wire and Electronic Communications and Transactional Records Access), Sections 2701 bis 2712.

Die gesetzlichen Grundlagen für den zweiten Fall, also die Installation von Überwachungsgeräten bzw. –prozessen im Bedarfsfall, den sog. Pen Registers and Trap and Trace Devices (PR/TT) finden sich in Title 18 USC Chapter 206 („Pen Registers and Trap and Trace Devices"), Sections 3121 bis 3127.

Für die gezielte Überwachung der Verkehrsdaten definierte der amerikanische Gesetzgeber die Begriffe „Pen Register" und „Trap and Trace Device".

- Unter „Pen Register" wird das Gerät oder der Prozess verstanden, durch das/den die gewählten Nummern, das Routing und Addressing sowie die Signalinformationen der elektronischen Kommunikation aufgezeichnet werden. Durch ein Pen Register werden keine Inhalte der Kommunikation aufgezeichnet. Ein Pen Register umfasst nicht das Gerät oder den Prozess, durch das/den die Daten erfasst werden, die für das Billing der Dienste oder für andere unternehmensinterne Zwecke benötigt werden.[53]

- Unter „Trap and Trace Device" wird ein Gerät oder ein Prozess verstanden, durch das/den die ankommenden elektronischen oder anderen Signale erfasst werden, um Anrufernummer bzw. Absenderadresse sowie weitere Informationen, die die Kommunikationsquelle identifizieren. Auch das Trap and Trace Device darf keine Inhalte der Kommunikation erfassen.[54]

Eingeführt wurde ein Großteil dieser Gesetze im Rahmen des „Electronic Communications Privacy Act" (ECPA) im Jahre 1986 und seither durch mehrere Gesetzesänderungen verändert. Bei den Veränderungen gab es zum einen Anpassungen auf technische Innovationen und zum anderen Erleichterungen für den Zugang der Strafverfolgungsbehörden zu gespeicherten Verkehrsdaten.

Im Rahmen des USA Patriot Act wurden die Möglichkeiten der Strafverfolgungsbehörden für PR/TT-Maßnahmen deutlich ausgeweitet. Konnte ein Richter zuvor lediglich PR/TT-Maßnahmen innerhalb seines Amtsbezirks genehmigen, so kann er dies nun für die ganze USA. Zudem wurde die Aufzeichnung der Adressinformationen beim E-Mail-Verkehr inklusive der Betreffzeilen sowie die Protokollierung des Internetsurfens zugelassen.[55]

Die speziellen technischen Ausgestaltungen der Maßnahmen, die Kostenentschädigungen für vorzuhaltende technische Einrichtungen sowie weitere spezielle Vorschriften zur Durchführung sind in Title 47 USC („Telegraphs, Telephones, and Radiote-

---

53 Vgl. Title 18 USC, Section 3127 (3).
54 Vgl. Title 18 USC, Section 3127 (4).
55 Vgl. http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12263&c=206.

legraphs“) und dort speziell in Chapter 9 („Interception of digital and other communications“) geregelt.

10.1.2.1 Zugang zu Bestands- und Verkehrsdaten der Unternehmen

Title 18 USC, Part I, Chapter 121 beschäftigt sich mit dem Zugang der Strafverfolgungsbehörden zur gespeicherten elektronischen Kommunikation sowie zu Verkehrsdaten. In Section 2702 sind die Vorschriften zum Datenschutz und seine freiwilligen Ausnahmen niedergelegt („Voluntary disclosure of customer communications or records“). In Section 2703 finden sich die Regelungen der Datenweitergabe an staatliche Stellen zum Zwecke der Strafverfolgung („Required disclosure of customer communications or records“). Sec. 2703 (a) und (b) beziehen sich auf elektronisch gespeicherte Inhalte. Sec. 2703 (c) regelt den Zugriff auf Bestandsdaten , die bereits beim Dienstebetreiber gesammelt sind.

> ***18 USC § 2703 (c):*** *Records Concerning Electronic Communication Service or Remote Computing Service. -*
>
> *(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity -*
>
> *(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;*
>
> *(B) obtains a court order for such disclosure under subsection (d) of this section;*
>
> *(C) has the consent of the subscriber or customer to such disclosure;*
>
> *(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or*
>
> *(E) seeks information under paragraph (2).*
>
> *(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the -*
>
> *(A) name;*

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

In Sec. 2703 (d) werden die Anforderungen an den richterlichen Beschluss zur Datenweitergabe definiert.

18 USC § 2703 (d): *Requirements for Court Order. -*

A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Sec. 2703 (f) schließlich verpflichtet die Diensteanbieter zur fallweisen Speicherung der Verkehrsdaten und legt den Speicherungszeitraum fest.

18 USC § 2703 (f): *Requirement To Preserve Evidence. -*

(1) *In general. –*

A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) *Period of retention. –*

Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

10.1.2.2 Gezielte Überwachung von Verkehrsdaten mittels Pen Registers und Trap and Trace Devices

In Title 18 USC Chapter 206 Section 3121 bis 3127 sind die Bestimmungen zu Pen Registers und Trap and Trace Devices festgelegt.

Section 3122 regelt die Beantragung der anlassbezogenen Datenspeicherung. Der Antrag auf eine Aufzeichnung der Verkehrsdaten einer bestimmten Person kann durch einen Bundesstaatsanwalt („Attorney for the Government“) oder durch die Strafverfolgungsbehörden der Bundesstaaten („State Investigative or Law Enforcement Officer“) ausgestellt werden.

18 USC § 3122: *Application for an order for a pen register or a trap and trace device*

(a) Application. -

(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of Application. -

An application under subsection (a) of this section shall include -

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Die Genehmigung dieser Anträge erfolgt nach Title 18 USC Section 3123 durch eine richterliche Anordnung. Der Antragsteller hat dem Richter hierfür glaubhaft zu machen, dass die durch die Maßnahme gewonnenen Daten Relevanz für die Aufklärung des laufenden Strafverfahrens besitzt.

Die Anordnung zur anlassbezogenen Datenspeicherung ist befristet. Die Befristung darf nach Title 18 USC Section 3123 (c) 60 Tage nicht überschreiten. Durch einen neuerlichen Antrag kann die Maßnahme um bis zu weiter 60 Tage verlängert werden. Spätestens 30 Tage nach Ablauf der Frist, müssen dem Richter Protokolle über die Maßnahme vorgelegt werden, die Angaben zu den durchführenden Personen, den installierten Geräten, den gesammelten Daten und weiterer Details enthalten.

***18 USC Section 3123**: Issuance of an order for a pen register or a trap and trace device*

***(a)** In General. -*

***(1)** Attorney for the government. –*

Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

***(2)** State investigative or law enforcement officer. -*

Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(3)

(A) *Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify -*

(i) *any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;*

(ii) *the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;*

(iii) *the configuration of the device at the time of its installation and any subsequent modification thereof; and*

(iv) *any information which has been collected by the device.*

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

(B) *The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).*

(b) *Contents of Order. -*

An order issued under this section –

(1) *shall specify -*

(A) *the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;*

(B) *the identity, if known, of the person who is the subject of the criminal investigation;*

(C) *the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and*

(D) *a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and*

(2) *shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.*

(c) *Time Period and Extensions. -*

(1) *An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.*

(2) *Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.*

(d) *Nondisclosure of Existence of Pen Register or a Trap and Trace Device. -*

An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that -

(1) *the order be sealed until otherwise ordered by the court; and*

(2) *the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached or applied, or*

> *who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.*

In Title 18, Section 3126 ist geregelt, dass der Generalbundesstaatsanwalt („Attorney General") jährlich dem Congress die Anzahl der anlassbezogenen Datenspeicherungen berichten muss. Dabei müssen Angaben gemacht werden zur Dauer der Überwachung, zu den Vergehen, die den Anträgen zugrunde liegen, zur Anzahl der Ermittlungen, zur Art und Anzahl der betroffenen technischen Einrichtungen sowie zur Identität der beantragenden Strafverfolgungsbehörden und der Personen, die die Maßnahmen genehmigten.

10.1.2.3 Technische Einrichtungen für staatliche Überwachungsmaßnahmen

Title 47 USC Chapter 9 ist im Wesentlichen durch den Communications Assistance for Law Enforcement Act von 1994 (CALEA) entstanden. Hier werden die technischen Einrichtungen beschrieben, die Netzbetreiber vorhalten müssen, um staatliche Überwachungsmaßnahmen zu ermöglichen. Erforderlich sind beispielsweise spezielle Netzelemente wie Switches und Software. Neben der Aufzeichnung der Kommunikationsinhalte können diese Einrichtungen auch für die Erfassung der Verkehrsdaten genutzt werden.

Die Anforderungen an CALEA-konforme Technologie und Prozesse sind im Interim Standard J-STD-025-A definiert. Dieser wird seit 1995 unter der Leitung der Telecommunications Industry Association (TIA), Subcommittee TR-45.2 zusammen mit dem Committee T1 der Alliance for Telecommunications Industry Solutions entwickelt. Mittlerweile wurde dieser Standardentwurf durch den technischen Fortschritt überholt. Immer mehr Carrier setzen paketvermittelnde Dienste, insbesondere Voice-over-IP ein. Deshalb veröffentlichte das FBI im November 2001 das „Packet Surveillance Fundamental Needs Document" (PSFND) und ergänzte es im Januar 2003 mit dem Papier „Carrier Grade Voice over Packet" (CGVoP).[56]

Die technischen Anforderungen von CALEA mussten ursprünglich bis zum 30. Juni 2000 umgesetzt werden. Es können jedoch nach individueller Prüfung jeweils zweijährige Fristverlängerungen vergeben werden. Der jüngste Termin zu dem die Umsetzung nachgewiesen bzw. Fristverlängerungen beantragt werden musste war der 30. Juni 2004.

---

56 Vgl. Communications Assistance for Law Enforcement Act (CALEA), Ninth Annual Report to Congress, Prepared by Federal Bureau of Investigation (FBI) and United States Department of Justice, 30. November, S. 3f.

Die Anforderungen des FBI zu paketvermittelnder Kommunikation wurden 2003 zunächst ausgesetzt, da es auf diesem Feld noch zu keiner Standardbildung gekommen ist und die verfügbaren Lösungen nicht die Anforderungen des Gesetzes erfüllen können.[57]

10.1.3 Gesetzliche Grundlagen der Datenspeicherung für unternehmenseigene Zwecke

Es existieren keine Gesetze, die den Netzbetreibern und Providern die Speicherung von Daten für ihre unternehmerischen Zwecke einschränken. Auch bezüglich der maximalen Aufbewahrungszeit der Bestands- und Verkehrsdaten gibt es keine Einschränkungen.[58]

10.2 Praxis der Vorratsdatenspeicherung

nicht zutreffend

10.3 Praxis der anlassbezogenen Datenspeicherung

10.3.1 Behördlicher Zugriff auf im Unternehmen gespeicherte Daten

Die konkrete Abwicklung eines anlassbezogen Zugriffs auf Bestands- und Verkehrsdaten, die im Unternehmen gespeichert werden, wird von einem ISP folgendermaßen beschrieben:

a. Ein Mitarbeiter einer Strafverfolgungsbehörde kontaktiert die Rechtsabteilung des ISP, in der Regel per Fax, um die Aufzeichnung der Bestands- und/oder der Verkehrsdaten einer bestimmten Person zu ersuchen. Zu den Bestandsdaten zählen beispielsweise eigene E-Mail-Adressen, Vertragsdaten, Wohnungsadresse, Kreditkarteninformationen, zu den Verkehrsdaten zählen u.a. IP-Adressen, E-Mail-Adressen der Adressaten, Anzahl und Zeiten der Mails.

b. Daraufhin sorgt der ISP dafür, dass alle zum Zeitpunkt dieses Ersuchens bei ihm vorhandenen Daten zu dieser Person sowie die neu entstehenden Verkehrsdaten für 90 Tage nicht gelöscht werden.

---

57 Vgl. CALEA (2003), S. 8.
58 Lt. Aussage des US-Justizministeriums.

c. Der Mitarbeiter der Strafverfolgungsbehörde hat nun 90 Tage Zeit, die im Gesetz (Title 18 USC Section 3123) vorgeschriebene richterliche Anordnung einzuholen und dem ISP vorzulegen.

d. Nach Vorlage der richterlichen Anordnung übergibt der ISP die Bestands- und Verkehrsdaten an die Strafverfolgungsbehörde.

Nach Auskunft des US-Justizministeriums gibt es keine zentralen Statistiken über die Anzahl der Datenabfragen. Auf Grund der Vielzahl an Strafverfolgungsbehörden und auf Basis der Erfahrungen im eigenen Hause, schätzt das Ministerium, dass die Möglichkeiten zur Datenabfrage sehr stark genutzt werden.

10.3.2 Pen Register/Trap and Trace zur gezielten Datenspeicherung

Alle TK-Anbieter und -Anlagenbetreiber, also alle Netzbetreiber und Service Provider, sind generell verpflichtet, die berechtigten Stellen bei der Durchführung von PR/TT-Maßnahmen zu unterstützen.

> *Auszug aus **Title 18 USC, Sec. 3123 (a) (1)**:*
>
> *(…) The order, upon service of that order, shall apply to any person or entitiy providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. (…)*

10.3.3 Bereitschaft von technischem Personal

CALEA verpflichtet die TK-Netzbetreiber, technische Einrichtungen permanent mit einer ständigen Verfügbarkeit von Personal („24x7“) zur Verfügung zu stellen. ISP mit eigener Netztechnik, z.B. eigenen Einwählknoten, aber ohne eigenes Netz, müssen dies nur fallweise gewährleisten.

10.4 Praxis der Datenspeicherung für unternehmenseigene Zwecke

Netzbetreiber und Internet Service Provider sind nicht gesetzlich verpflichtet, Daten zu löschen. Soweit es für die Unternehmen wirtschaftlich erscheint, werden Daten für Abrechnungs-, Marketing- oder Sicherheitszwecke gespeichert. Die maximale Speicherdauer obliegt ausschließlich den Unternehmen. Alle freiwillig durch die Unternehmen gespeicherten Daten müssen im Falle einer Datenabfrage den Strafverfolgungsbehörden ausgehändigt werden.

10.5 Ausgestaltung des Zugriffs der berechtigten Stellen

Die Bereitstellung von im Unternehmen gespeicherten Daten bedarf einem Antrag einer staatlichen Stelle („governmental entity“), der durch einen richterlichen Beschluss bestätigt werden muss (Title 18 USC Section 2703).

Um eine gezielte Überwachungsmaßnahme (PR/TT) einzurichten ist ein Antrag durch einen Bundesstaatsanwalt („Attorney for the Government“) oder durch die Strafverfolgungsbehörden der Bundesstaaten („State Investigative or Law Enforcement officer (Title 18 USC Section 3122) erforderlich. Die Genehmigung dieser Anträge erfolgt nach 18 USC Section 3123 durch eine richterliche Anordnung. Der Antragsteller hat dem Richter hierfür glaubhaft zu machen, dass die durch die Maßnahme gewonnenen Daten Relevanz für die Aufklärung des laufenden Strafverfahrens besitzen.

10.6 Kostenentschädigung

10.6.1 Rechtliche Grundlagen

Regelungen zur Kostenentschädigung bei staatlichen Zugriff auf Unternehmensdaten finden sich in Title 18 USC Section 2706.

Grundsätzlich sollen die Unternehmen für Kosten, die in direktem Zusammenhang mit der angeordneten Maßnahme stehen und einen angemessenen Rahmen nicht übersteigen entschädigt werden. Allerdings besteht für die Herausgabe von Daten, die der Netzbetreiber bzw. Serviceanbieter für eigene Zwecken gespeichert hat kein Kostenentschädigungsanspruch. Eine Ausnahmeregelung besteht für Fälle in denen der Aufwand übermäßig hoch bzw. das Datenvolumen ungewöhnlich groß ist. In diesem Fall entscheidet der Richter, der die Maßnahme genehmigt hat über die Höhe der Entschädigung.

> ***18 USC Section 2706**: Cost reimbursement*
>
> *(a) Payment. -*
>
> *Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal opera-*

tions of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount. -

The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception. –

The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

Die rechtlichen Grundlagen zur Entschädigung der Kosten, die im Zusammenhang mit PR/TT-Maßnahmen entstehen, sind in Title 18 USC Section 3124 zu finden.

***18 USC Section 3124**: Assistance in installation and use of a pen register or a trap and trace device*

(c) Compensation. -

A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

Für die Abwicklung eines einzelnen Überwachungsfalls erhalten die Anbieter demnach nur Entschädigungen für entstandene Betriebskosten. Im Rahmen der Verpflichtungen nach CALEA werden jedoch auch einmalige Entschädigungszahlungen für Kapitalkosten geleistet.

In Title 47 USC Section 1008 ist eine Kostenentschädigung in angemessener Höhe („reasonable costs“) für Investitionen vorgesehen, um vorhandene Anlagen für die gesetzlich vorgeschriebene Datenspeicherung aufzurüsten.

Dies gilt allerdings grundsätzlich nur für Ausrüstungen, Anlagen und Dienste, die vor dem 1. Januar 1995 installiert bzw. eingesetzt wurden und nicht ersetzt oder wesentlich aufgerüstet oder modifiziert wurden. Um Kostenentschädigungen auch für Ausrüstungen, Anlagen und Dienste, die nach diesem Termin installiert bzw. eingesetzt wurden, zu erhalten, sind begründete Anträge bei der Regulierungsbehörde FCC einzureichen.

10.6.2 Abwicklungsprozess

Das Abrechungsverfahren der einzelnen Überwachungen ist dezentral organisiert. Die Rechnung wird jeweils an die Gerichte gestellt, die die Maßnahmen genehmigt haben.

Die Kostenentschädigung für Netzkomponenten zur Echtzeit-Überwachung, die die Netzbetreiber entsprechend CALEA installieren müssen, erfolgt zum Teil auf indirektem Weg. Das FBI, das mit diesen Zahlungen vertraut wurde, schließt Rahmenabkommen mit den Herstellern von Software ab, die ihre Produkte kostenlos an die Netzbetreiber abgeben. Auch die Entschädigungen für Hardware erfolgt direkt an die Hersteller.

10.6.3 Höhe der Kostenentschädigung

Nach Aussage der US ISP Association (ISPA) liegt es an den Unternehmen, die durch eine gezielte Überwachungsmaßnahme (PR/TT) entstandenen Kosten zu beziffern und beim zuständigen Gericht einzufordern. Die Provider stellen in der Regel entweder geschätzte fallbezogene Kosten in Rechnung oder sie berechnen den zeitlichen Aufwand ihrer Mitarbeiter für die angeordneten Maßnahmen.

Konkrete Kostensätze sind nicht öffentlich bekannt.

10.7 Besonderheiten und aktuelle Entwicklungen

Die USA verfügen nicht über Bestimmungen zu Vorratsdatenspeicherung, sondern setzen bei der Strafverfolgung auf Data Preservation. Dies wird insbesondere von den TK-Anbietern begrüßt, da dieses Regime nach ihrer Auffassung weitaus kostengünstiger zu realisieren ist.